

## **Oracle® Fusion Middleware**

Upgrade Guide for Oracle Identity and Access Management

11g Release 2 (11.1.2.3.0)

**E51062-07**

March 2018

Documentation for Oracle Fusion Middleware administrators who wish to upgrade Oracle Identity and Access Management components to 11g Release 2 (11.1.2.3.0).

Oracle Fusion Middleware Upgrade Guide for Oracle Identity and Access Management, 11g Release 2 (11.1.2.3.0)

E51062-07

Copyright © 2015, 2018, Oracle and/or its affiliates. All rights reserved.

Primary Author: Shynitha K S

Contributors: Allison Sparshott, Arun Singla, Aruna Vempaty, Ashwini Singhvi, Astha Gupta, Ballaji Sahoo, Basavaraj Hungund, Bhavik Sankesara, Brad Donnison, Bruce Xie, Charles Wesley, Deepak Ramakrishnan, Derick Leo, Gaurav Johar, Gururaj B S, Kavita Tippanna, Kishor Negi, Kumar Dhanagopal, Lixin Zheng, Lokesh Gupta, Madhu Martin, Mark Karlstrand, Mark Wilcox, Mrudul Uchil, Nagasravani Akula, Neelanand Sharma, Neeraj Goel, Niranjana Ananthapadmanabha, Pallavi Rao, Peter Laquerre, Raminder Deep Kaler, Ramya Subramanya, Ravi Thirumalasetty, Rubis Chowallur, Sandeep Dongare, Sanjay Sadarangani, Sanjeev Sharma, Semyon Shulman, Shruthi Chikkanna, Sitaraman Swaminathan, Sree Chitturi, Srinivas Nagandla, Stephen Mathew, Steven Frehe, Stuart Duggan, Svetlana Kolomeyskaya, Tushar Wagh, Umesh Waghode, Vadim Lander, Vishal Mishra, Venu Shastri, William Cai, Wortimla Rs, Yongqing Jiang

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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.

---

---

# Contents

<b>Preface</b> .....	xix
Audience .....	xix
Documentation Accessibility .....	xix
Related Documents .....	xix
Conventions .....	xx
<b>What's New In This Guide</b> .....	xxi
New and Changed Features for 11g Release 2 (11.1.2.3.0) .....	xxi
Other Significant Changes in this Document for 11g Release 2 (11.1.2.3.0) .....	xxii
<b>Part I Understanding the Oracle Identity and Access Management Upgrade</b>	
<b>1 Introduction to Oracle Identity and Access Management Upgrade</b>	
1.1 Introduction to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) .....	1-1
1.2 Oracle Identity and Access Management Upgrade Overview .....	1-2
1.3 Migration and Coexistence Scenarios .....	1-2
<b>2 Understanding the Oracle Identity and Access Management Automated Upgrade</b>	
2.1 Introduction to Automated Upgrade .....	2-1
2.2 Deployment Topologies Supported for Automated Upgrade .....	2-2
2.3 Isolated Upgrade Overview .....	2-3
2.4 Supported Starting Points for Automated Upgrade .....	2-3
2.5 Documentation Roadmap .....	2-4
<b>3 Understanding the Oracle Identity and Access Management Manual Upgrade</b>	
3.1 Introduction to Manual Upgrade .....	3-1
3.2 Scenarios Supported for Manual Upgrade .....	3-1
3.2.1 Upgrading Oracle Identity and Access Management Components on a Single Node .....	3-2
3.2.2 Upgrading Oracle Identity and Access Management Highly Available Environments .....	3-3
3.2.3 Upgrading Oracle Access Management Multi-Data Center Environments .....	3-3

3.2.4	Upgrading Oracle Identity Manager, Oracle Access Management, and Oracle Adaptive Access Manager Integrated Highly Available Environments	3-3
3.3	Supported Starting Points for Oracle Identity and Access Management Manual Upgrade ...	3-3
3.4	Documentation Roadmap .....	3-7

## **Part II Upgrading Oracle Identity and Access Management Environments Deployed Using Life Cycle Management (LCM) Tools**

### **4 Upgrading Oracle Identity and Access Management Environments Deployed Using Life Cycle Management (LCM) Tools on a Single Node**

4.1	Variables Used in This Chapter .....	4-2
4.2	Upgrade Scenarios Covered in this Chapter.....	4-2
4.3	Upgrading Oracle Identity Manager (OIM) Only Topology on a Single Node .....	4-3
4.3.1	Completing the Prerequisites.....	4-4
4.3.2	Obtaining the Software .....	4-4
4.3.3	Setting the Environment Variables .....	4-4
4.3.4	Updating the Properties File .....	4-4
4.3.5	Performing Pre-Validation Checks on OIMHOST.....	4-5
4.3.6	Creating BIP Schema for OIM Upgrade (Only on Solaris, IBM AIX, and HP Itanium Platforms) 4-5	
4.3.7	Stopping All Servers on OIMHOST .....	4-5
4.3.8	Backing Up Database and WebLogic Domain .....	4-5
4.3.9	Upgrading Binaries and Configuration on OIMHOST .....	4-5
4.3.10	Performing Post-Validation Checks on OIMHOST .....	4-6
4.3.11	Verifying the Upgrade .....	4-6
4.4	Upgrading Oracle Access Manager (OAM) Suite Only Topology on a Single Node.....	4-6
4.4.1	Completing the Prerequisites.....	4-7
4.4.2	Obtaining the Software .....	4-8
4.4.3	Setting the Environment Variables .....	4-8
4.4.4	Updating the Properties File .....	4-8
4.4.5	Performing Pre-Validation Checks on OAMHOST.....	4-8
4.4.6	Stopping All Servers on OAMHOST .....	4-8
4.4.7	Backing Up Database and WebLogic Domain .....	4-9
4.4.8	Upgrading Binaries and Configuration on OAMHOST .....	4-9
4.4.9	Performing Post-Validation Checks on OAMHOST .....	4-9
4.4.10	Verifying the Upgrade .....	4-10
4.5	Upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Single Node 4-10	
4.5.1	Completing the Prerequisites.....	4-11
4.5.2	Obtaining the Software .....	4-11
4.5.3	Setting the Environment Variables .....	4-12
4.5.4	Updating the Properties File .....	4-12
4.5.5	Performing Pre-Validation Checks on IDMHOST.....	4-12
4.5.6	Creating BIP Schema for OIM Upgrade (Only on Solaris, IBM AIX, and HP Itanium Platforms) 4-13	
4.5.7	Stopping All Servers on IDMHOST .....	4-13
4.5.8	Backing Up Database and WebLogic Domain .....	4-13

4.5.9	Upgrading Binaries and Configuration on IDMHOST .....	4-13
4.5.10	Performing Post-Validation Checks on IDMHOST .....	4-14
4.5.11	Performing the Required Post-Upgrade Tasks .....	4-15
4.5.11.1	Adding the JAVA System Property if you have Configured OAAM.....	4-15
4.5.12	Verifying the Upgrade .....	4-15
4.6	Performing Isolated Upgrade for OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Single Node	4-15
4.7	Troubleshooting .....	4-19

## **5 Upgrading Oracle Identity and Access Management Highly Available Environments Deployed Using Life Cycle Management (LCM) Tools**

5.1	Variables Used in This Chapter .....	5-2
5.2	Upgrade Scenario Covered in this Chapter .....	5-2
5.3	Upgrading Oracle Identity Manager (OIM) Only on Multiple Nodes .....	5-3
5.3.1	Completing the Prerequisites.....	5-3
5.3.2	Obtaining the Software .....	5-4
5.3.3	Setting the Environment Variables .....	5-4
5.3.4	Updating the Properties File .....	5-4
5.3.5	Performing Pre-Validation Checks on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2	5-4
5.3.6	Creating BIP Schema for OIM Upgrade (Only on Solaris, IBM AIX, and HP Itanium Platforms)	5-5
5.3.7	Stopping All Servers.....	5-5
5.3.8	Backing Up Database and WebLogic Domain .....	5-6
5.3.9	Upgrading Binaries and Configuration on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2	5-6
5.3.10	Performing Post-Validation Checks on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2	5-7
5.3.11	Verifying the Upgrade .....	5-7
5.4	Upgrading Oracle Access Manager Suite (OAM) Only on Multiple Nodes.....	5-8
5.4.1	Completing the Prerequisites.....	5-8
5.4.2	Obtaining the Software .....	5-8
5.4.3	Setting the Environment Variables .....	5-9
5.4.4	Updating the Properties File .....	5-9
5.4.5	Performing Pre-Validation Checks on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2	5-9
5.4.6	Stopping All Servers.....	5-9
5.4.7	Backing Up Database and WebLogic Domain .....	5-10
5.4.8	Upgrading Binaries and Configuration on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2	5-10
5.4.9	Performing Post-Validation Checks on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2	5-11
5.4.10	Verifying the Upgrade .....	5-12
5.5	Upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Highly Available (HA) setup	5-12
5.5.1	Completing the Prerequisites.....	5-13
5.5.2	Obtaining the Software .....	5-13
5.5.3	Setting the Environment Variables .....	5-13

5.5.4	Updating the Properties File .....	5-14
5.5.5	Performing Pre-Validation Checks all of the Hosts.....	5-14
5.5.6	Creating BIP Schema for OIM Upgrade (Only on Solaris, IBM AIX, and HP Itanium Platforms) 5-15	
5.5.7	Stopping All Servers.....	5-15
5.5.8	Backing Up Database and WebLogic Domain .....	5-16
5.5.9	Upgrading Binaries and Configuration on all of the Hosts.....	5-16
5.5.10	Performing Post-Validation Checks on all of the Hosts.....	5-18
5.5.11	Performing the Required Post-Upgrade Tasks .....	5-18
5.5.11.1	Upgrading Oracle Access Management Identity Federation and Oracle Access Management Security Token Service 5-19	
5.5.11.2	Upgrading Server Keystore Certificate if you have Configured Oracle Adaptive Access Manager 5-19	
5.5.11.3	Configuring Reverse Proxy Settings.....	5-19
5.5.11.4	Adding the JAVA System Property if you have Configured OAAM.....	5-19
5.5.12	Verifying the Upgrade .....	5-19
5.6	Troubleshooting .....	5-19

## 6 Tasks Common to Various Automated Upgrade Scenarios

6.1	Variables Used in This Chapter .....	6-1
6.2	Reviewing System Requirements and Certifications.....	6-2
6.3	Backing up the Existing Environment .....	6-2
6.4	Setting the Required Environment Variables Necessary for Upgrade .....	6-3
6.5	Verifying Hostnames in the Hosts File .....	6-4
6.6	Obtaining the Automated Upgrade Tool .....	6-4
6.7	Updating the upgrade.properties File .....	6-5
6.8	Performing Pre-Validation Checks Using preValidate.pl Script .....	6-7
6.9	Creating BIP Schema for Oracle Identity Manager Upgrade on Solaris, IBM AIX, and HP Itanium Platforms 6-8	
6.9.1	Obtaining Repository Creation Utility .....	6-8
6.9.2	Starting Repository Creation Utility .....	6-8
6.9.3	Creating Schemas.....	6-8
6.10	Upgrading Oracle Identity and Access Management Binaries and Configuration Using idmUpgrade.pl script 6-9	
6.11	Performing Post-Validation Checks Using postValidate.pl Script .....	6-9
6.12	Stopping All Servers Using stopall.sh Script.....	6-10
6.13	Post-Upgrade Tasks.....	6-11
6.13.1	Adding the Java System Property for Oracle Adaptive Access Manager .....	6-11
6.14	Troubleshooting .....	6-11
6.14.1	IDM URL Access Issues When Performing Pre-Validation and Post-Validation Checks on HP-UX Itanium 6-11	
6.14.2	Autologin to OIM Console Fails After Resetting User Password Post OIM/OAM Isolated Upgrade on AIX 6-11	
6.14.3	Perl Undefined Symbol Error While Running preValidate.pl Script.....	6-12
6.14.4	/xmlpsrver and /access URLs not Accessible via OHS Port After Isolated Upgrade ... 6-12	

## Part III Upgrading Oracle Identity and Access Management 11g Release 2

## (11.1.2.x.x) Environments

### 7 Upgrading Oracle Privileged Account Manager 11g Release 2 (11.1.2.x.x) Environments

7.1	Upgrade Roadmap for Oracle Privileged Account Manager.....	7-2
7.2	Performing the Required Pre-Upgrade Tasks .....	7-3
7.3	Exporting the Pre-Upgrade Data.....	7-3
7.4	Stopping the Administration Servers and the Managed Server(s).....	7-4
7.5	Upgrading Oracle WebLogic Server to 10.3.6.....	7-5
7.6	Updating Oracle Privileged Account Manager Binaries to 11.1.2.3.0 .....	7-5
7.7	Upgrading the Database Schemas.....	7-5
7.8	Start the Administration Server and the Managed Server(s) .....	7-5
7.9	Redeploying the Applications.....	7-6
7.9.1	Redeploying Oracle Privileged Account Manager Console Application.....	7-6
7.9.2	Redeploying Oracle Privileged Account Manager Application.....	7-7
7.9.3	Redeploying Oracle Privileged Account Manager Session Manager Application ....	7-8
7.10	Enabling TDE or Non-TDE Mode in OPAM Data Store .....	7-9
7.10.1	Configuring TDE Mode in Data Store .....	7-9
7.10.1.1	Enabling TDE in the Database .....	7-9
7.10.1.2	Enabling Encryption in OPAM Schema.....	7-9
7.10.2	Configuring Non-TDE Mode in Data Store .....	7-9
7.11	Importing the Pre-Upgrade Data.....	7-10
7.12	Clearing Pre-Upgrade OPSS Artifacts .....	7-10
7.13	Optional: Configuring the Oracle Privileged Account Manager 11.1.2.3.0 Session Manager . 7-11	
7.14	Optional: Configuring Oracle Privileged Account Manager Console Application on OPAM Managed Server 7-11	
7.15	Verifying the Oracle Privileged Account Manager Upgrade.....	7-12

### 8 Upgrading Oracle Access Management 11g Release 2 (11.1.2.x.x) Environments

8.1	Upgrade Roadmap for Oracle Access Management.....	8-2
8.2	Performing the Required Pre-Upgrade Tasks .....	8-3
8.3	Upgrading Oracle Home .....	8-6
8.3.1	Upgrading Oracle WebLogic Server to 10.3.6 .....	8-6
8.3.2	Applying Mandatory Patches for Oracle WebLogic Server .....	8-6
8.3.3	Upgrading Oracle Access Management Binaries to 11.1.2.3.0 .....	8-6
8.4	Creating OMSM Schema.....	8-7
8.5	Upgrading the Database Schemas.....	8-7
8.6	Upgrading Oracle Platform Security Services .....	8-7
8.7	Copying Modified System mbean Configurations .....	8-7
8.8	Undeploying coherence#3.7.1.1 Library .....	8-8
8.9	Restarting the Servers.....	8-9
8.10	Upgrading System Configuration .....	8-9
8.11	Extending the Oracle Access Management Domain to Include Mobile Security Suite and Policy Manager 8-11	

8.12	Starting the Servers.....	8-11
8.13	Performing the Required Post-Upgrade Tasks.....	8-11
8.13.1	Optional: Enabling Oracle Mobile Security Suite .....	8-11
8.13.2	Optional: Upgrading Oracle Access Management Mobile and Service .....	8-12
8.13.3	Optional: Upgrading Oracle Access Management Identity Federation .....	8-12
8.13.4	Assigning Necessary Roles to Admin.....	8-12
8.14	Verifying the Oracle Access Management Upgrade.....	8-12
8.15	Troubleshooting .....	8-12

## **9 Upgrading Oracle Adaptive Access Manager 11g Release 2 (11.1.2.x.x) Environments**

9.1	Upgrade Roadmap for Oracle Adaptive Access Manager .....	9-2
9.2	Performing the Required Pre-Upgrade Tasks .....	9-2
9.3	Shutting Down Administration Server and Managed Servers .....	9-3
9.4	Backing Up Oracle Adaptive Access Manager 11.1.2.x.x.....	9-3
9.5	Optional: Upgrading Oracle WebLogic Server .....	9-3
9.6	Updating Oracle Adaptive Access Manager Binaries to 11.1.2.3.0.....	9-4
9.7	Upgrading OAAM, MDS, IAU, and OPSS Schemas .....	9-4
9.8	Upgrading Oracle Platform Security Services .....	9-4
9.9	Starting the Servers.....	9-5
9.10	Redeploying Oracle Adaptive Access Manager Applications .....	9-5
9.11	Restarting the Servers.....	9-6
9.12	Verifying the Oracle Adaptive Access Manager Upgrade .....	9-7
9.13	Troubleshooting .....	9-8

## **10 Upgrading Oracle Identity Manager 11g Release 2 (11.1.2.x.x) Environments**

10.1	Upgrade Roadmap for Oracle Identity Manager .....	10-1
10.2	Performing the Required Pre-Upgrade Tasks .....	10-3
10.2.1	Feature Comparison .....	10-3
10.2.2	Reviewing System Requirements and Certification .....	10-5
10.2.3	Ensuring that you are Using a Certified JDK Version.....	10-6
10.2.4	Reviewing the Customizations that are Lost or Overwritten as Part of Upgrade..	10-6
10.2.5	Generating and Analyzing the Pre-Upgrade Report.....	10-7
10.2.6	Shutting Down Node Manager, Administration Server and Managed Server(s)...	10-7
10.2.7	Backing Up Oracle Identity Manager 11.1.2.x.x Environment.....	10-7
10.2.8	Disabling OIM Materialized-View Creation.....	10-8
10.3	Upgrading Oracle Home .....	10-8
10.3.1	Upgrading Oracle WebLogic Server to 10.3.6 .....	10-9
10.3.2	Upgrading Oracle SOA Suite to 11.1.1.9.0 .....	10-9
10.3.3	Upgrading Oracle Identity Manager Binaries to 11.1.2.3.0.....	10-9
10.4	Creating Necessary Schemas and Upgrading Existing Schemas.....	10-10
10.4.1	Creating Oracle BI Publisher Schema .....	10-10
10.4.2	Upgrading Existing Schemas .....	10-10
10.5	Upgrading Oracle Identity Manager Middle Tier.....	10-11
10.6	Upgrading Other Oracle Identity Manager Installed Components .....	10-11
10.7	Performing the Required Post-Upgrade Tasks.....	10-12
10.8	Verifying the Oracle Identity Manager Upgrade .....	10-12

10.9	Troubleshooting .....	10-13
------	-----------------------	-------

## **11 Upgrading Oracle Entitlements Server 11g Release 2 (11.1.2.x.x) Environments**

11.1	Upgrading Oracle Entitlements Server 11.1.2.x.x Administration Server .....	11-1
11.1.1	Upgrade Roadmap for Oracle Entitlements Server Administration Server .....	11-2
11.1.2	Performing the Required Pre-Upgrade Tasks .....	11-3
11.1.3	Shutting Down Administration Server and Oracle Entitlements Server Managed Servers 11-3	
11.1.4	Upgrading Oracle WebLogic Server .....	11-3
11.1.5	Updating Oracle Entitlements Server Binaries to 11.1.2.3.0 .....	11-4
11.1.6	Deleting all py.class Files.....	11-4
11.1.7	Upgrading Oracle Platform Security Services Schema .....	11-4
11.1.8	Upgrading Oracle Platform Security Services.....	11-4
11.1.9	Deleting Certain Directories From the Domain .....	11-4
11.1.10	Starting the Administration Server and the Managed Servers .....	11-4
11.1.11	Verifying the Oracle Entitlements Server Administration Server Upgrade .....	11-5
11.2	Upgrading Oracle Entitlements Server 11.1.2.x.x Client.....	11-5
11.2.1	Upgrade Roadmap for Oracle Entitlements Server Client .....	11-5
11.2.2	Stopping all Security Module Instances .....	11-6
11.2.3	Upgrade Oracle Entitlements Server Client to 11.1.2.3.0.....	11-6
11.2.3.1	Prerequisites .....	11-6
11.2.3.2	Obtaining the Software .....	11-6
11.2.3.3	Installing Oracle Entitlements Server Client 11g Release 2 (11.1.2.3.0) .....	11-6
11.2.3.4	Verifying the Installation.....	11-7
11.2.4	Deleting all py.class Files.....	11-7
11.2.5	Starting the Security Modules.....	11-7
11.2.6	Verifying Oracle Entitlements Server Client Upgrade.....	11-7

## **Part IV Upgrading Oracle Identity and Access Management 11g Release 1 (11.1.1.x.x) and 9.x Environments**

### **12 Upgrading Oracle Access Manager 11g Release 1 (11.1.1.x.x) Environments**

12.1	Upgrade Roadmap for Oracle Access Manager .....	12-2
12.2	Performing the Required Pre-Upgrade Tasks .....	12-3
12.3	Upgrading Oracle Home .....	12-6
12.3.1	Upgrading Oracle WebLogic Server to 10.3.6 .....	12-6
12.3.2	Applying Mandatory Patches for Oracle WebLogic Server .....	12-6
12.3.3	Upgrading Oracle Access Manager Binaries to 11.1.2.3.0.....	12-7
12.4	Creating Necessary Schemas.....	12-7
12.5	Extending Oracle Access Manager 11.1.1.x.x Domain with Oracle Platform Security Services Template 12-7	
12.6	Upgrading Oracle Platform Security Services .....	12-8
12.7	Configuring Oracle Platform Security Services Security Store .....	12-9
12.8	Exporting Access Data .....	12-9
12.9	Importing Access Data.....	12-14

12.10	Copying Modified System mbean Configurations .....	12-16
12.11	Ensuring that the Newly Created OAM Policy Schema is in Use .....	12-16
12.12	Starting the Administration Server and Access Manager Managed Servers .....	12-17
12.13	Redeploying Access Manager Server Applications and Shared Libraries .....	12-17
12.14	Stopping the Administration Server and Access Manager Managed Servers .....	12-20
12.15	Deleting Folders .....	12-20
12.16	Upgrading System Configuration .....	12-20
12.17	Starting the Servers .....	12-21
12.18	Extending the Oracle Access Management Domain to Include Mobile Security Suite and Policy Manager	12-22
12.19	Performing the Required Post-Upgrade Tasks.....	12-22
12.19.1	Optional: Enabling Oracle Mobile Security Suite .....	12-22
12.19.2	Assigning Necessary Roles to Admin.....	12-22
12.20	Verifying the Oracle Access Management Upgrade.....	12-22
12.21	Troubleshooting .....	12-23

### **13 Upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x) Environments**

13.1	Upgrade Roadmap for Oracle Adaptive Access Manager .....	13-2
13.2	Performing the Required Pre-Upgrade Tasks .....	13-3
13.3	Shutting Down Administration Server and Managed Servers .....	13-3
13.4	Backing Up Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x).....	13-3
13.5	Optional: Upgrading Oracle WebLogic Server .....	13-4
13.6	Upgrading Oracle Adaptive Access Manager Binaries to 11g Release 2 (11.1.2.3.0) .....	13-4
13.7	Upgrading OAAM, MDS, IAU, and OPSS Schemas .....	13-4
13.8	Extending Oracle Adaptive Access Manager 11.1.1.x.x Component Domains with OPSS Template	13-5
13.9	Upgrading Oracle Platform Security Services .....	13-6
13.10	Configuring OPSS Security Store .....	13-6
13.11	Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers	13-6
13.12	Redeploying the Applications.....	13-7
13.13	Deleting Folders .....	13-9
13.14	Restarting the Servers.....	13-9
13.15	Verifying the Upgrade .....	13-10

### **14 Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.x.x) Environments**

14.1	Upgrade Roadmap for Oracle Identity Manager .....	14-2
14.2	Performing the Required Pre-Upgrade Tasks .....	14-4
14.2.1	Comparing the Features of Oracle Identity Manager 11.1.1.x.x and 11.1.2.3.0.....	14-4
14.2.2	Reviewing System Requirements and Certification .....	14-7
14.2.3	Ensuring that you are Using a Certified JDK Version.....	14-7
14.2.4	Reviewing the Customizations that are Lost or Overwritten as Part of Upgrade ..	14-7
14.2.5	Generating and Analyzing the Pre-Upgrade Report.....	14-8
14.2.6	Ensuring That getPlatformTransactionManager() Method is Not Used in Custom Code	14-9
14.2.7	Emptying the oimProcessQueue JMS Queue .....	14-9

14.2.8	Other Prerequisites .....	14-9
14.2.9	Creating Reconciliation Field of Type IT Resource .....	14-10
14.2.10	Shutting Down Node Manager, Administration Server and Managed Servers ...	14-11
14.2.11	Backing Up Oracle Identity Manager 11g Release 1 (11.1.1.x.x).....	14-11
14.3	Upgrading Oracle Home .....	14-12
14.3.1	Upgrading Oracle WebLogic Server to 10.3.6 .....	14-12
14.3.2	Upgrading Oracle SOA Suite to 11.1.1.9.0 .....	14-12
14.3.3	Upgrading Oracle Identity Manager Binaries to 11.1.2.3.0.....	14-13
14.4	Creating Necessary Schemas and Upgrading the Existing Schemas .....	14-13
14.4.1	Creating Necessary Database Schemas .....	14-13
14.4.2	Upgrading Existing Schemas .....	14-14
14.4.2.1	Version Numbers After Upgrading Schemas.....	14-14
14.5	Upgrading Oracle Identity Manager Middle Tier.....	14-14
14.6	Upgrade Other Oracle Identity Manager Installed Components .....	14-15
14.7	Performing the Required Post-Upgrade Tasks.....	14-15
14.8	Verifying the Oracle Identity Manager Upgrade .....	14-16
14.9	Troubleshooting .....	14-16

## **15 Upgrading Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) Environment**

15.1	Upgrading Oracle Entitlements Server Administration Server .....	15-1
15.1.1	Upgrade Roadmap for Oracle Entitlements Server Administration Server .....	15-2
15.1.2	Performing the Required Pre-Upgrade Tasks .....	15-3
15.1.3	Shutting Down Administration Server and Managed Servers .....	15-3
15.1.4	Backing Up Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) .....	15-3
15.1.5	Upgrading Oracle WebLogic Server to 10.3.6 .....	15-4
15.1.6	Upgrading Oracle Entitlements Server Administration Server 11g Release 2 (11.1.2.3.0) 15-4	
15.1.7	Creating Oracle Platform Security Service Schema .....	15-5
15.1.8	Executing R2_Upgrade.sql .....	15-5
15.1.9	Creating New Oracle Entitlements Server Domain.....	15-5
15.1.10	Exporting Encryption Key .....	15-5
15.1.11	Re-Associating Policy Stores .....	15-6
15.1.11.1	Policy Store is DB.....	15-6
15.1.11.2	Policy Store is OID.....	15-8
15.1.12	Deleting all py.class Files.....	15-10
15.1.13	Upgrading Oracle Platform Security Services.....	15-10
15.1.14	Starting the Administration Server and Oracle Entitlements Server Managed Servers ... 15-10	
15.1.15	Redeploying APM .....	15-10
15.1.16	Verifying the Upgrade .....	15-11
15.2	Upgrading Oracle Entitlements Server Client Server.....	15-12
15.2.1	Upgrade Roadmap for Oracle Entitlements Server Client Server .....	15-12
15.2.2	Stopping all Security Module Instances .....	15-12
15.2.3	Upgrading Oracle Entitlements Server Client 11g Release 2 (11.1.2.3.0).....	15-13
15.2.3.1	Prerequisites .....	15-13
15.2.3.2	Obtaining the Software .....	15-13

15.2.3.3	Installing Oracle Entitlements Server Client Server 11g Release 2 (11.1.2.3.0)	15-13
15.2.3.4	Verifying the Installation.....	15-13
15.2.4	Changing Username and Password for the New Schemas .....	15-13
15.2.5	Starting the Security Modules.....	15-15
15.2.6	Verifying the Upgrade .....	15-15

## 16 Upgrading Oracle Identity Manager 9.1.x.x Environments

16.1	Upgrade Roadmap for Oracle Identity Manager .....	16-1
16.2	Feature Comparison .....	16-2
16.3	Reviewing System Requirements and Certification .....	16-4
16.4	Upgrading Oracle Identity Manager 9.1.x.x to 11.1.2.2.0.....	16-4
16.5	Upgrading Oracle Identity Manager 11.1.2.2.0 to 11.1.2.3.0.....	16-4

## Part V Upgrading Oracle Identity and Access Management High Availability Environments

### 17 Upgrading Oracle Access Management Highly Available Environments

17.1	Understanding Oracle Access Management High Availability Upgrade Topology .....	17-2
17.2	Upgrade Roadmap.....	17-2
17.3	Shutting Down Administration Server and Managed Servers on OAMHOST1 and OAMHOST2	17-3
17.4	Backing Up the Existing Environment .....	17-4
17.5	Upgrading OAMHOST1 to 11.1.2.3.0 .....	17-4
17.6	Updating Component Versions on OAMHOST1 .....	17-4
17.7	Updating Binaries of WebLogic Server and Access Manager on OAMHOST2 .....	17-5
17.8	Replicating Domain Configuration on OAMHOST2 .....	17-6
17.9	Redeploying Access Manager Server Applications and Shared Libraries on OAMHOST1....	17-6
17.10	Starting Administration Server and Managed Servers on OAMHOST1 and OAMHOST2....	17-7

### 18 Upgrading Oracle Access Management Multi-Data Center Environments

18.1	Understanding Oracle Access Management Multi-Data Center Topology .....	18-2
18.2	Upgrade Roadmap.....	18-2
18.3	Backing Up the Existing Environment .....	18-3
18.4	Enabling Write Permission to Master and Clones (if Necessary).....	18-3
18.5	Disabling and Deleting All Replication Agreements Between Master and Clone.....	18-3
18.6	Redirecting Traffic to Clone Data Center .....	18-4
18.7	Upgrading OAM on Master Data Center .....	18-4
18.8	Redirecting Traffic to Master Data Center .....	18-4
18.9	Upgrading OAM on Clone Data Center.....	18-4
18.10	Freezing all Changes to Master and Clones (if Necessary).....	18-4
18.11	Syncing Access Metadata.....	18-4
18.12	Creating Replication Agreement .....	18-5
18.13	Bringing up the Master and Clone Data Centers Online .....	18-5
18.14	Troubleshooting .....	18-5

18.14.1	Multi-Data Centre Feature Not Working After Upgrade .....	18-6
---------	---	------

## **19 Upgrading Oracle Adaptive Access Manager Highly Available Environments**

19.1	Understanding Oracle Adaptive Access Manager High Availability Upgrade Topology .....	19-2
19.2	Upgrade Roadmap.....	19-3
19.3	Shutting Down Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2	19-3
19.4	Backing Up the Existing Environment .....	19-4
19.5	Updating Binaries of WebLogic Server and Oracle Adaptive Access Manager on OAAMHOST2	19-4
19.6	Upgrading OAAMHOST1 to 11.1.2.3.0 .....	19-4
19.7	Updating Component Versions on OAAMHOST1 .....	19-5
19.8	Replicating Domain Configuration on OAAMHOST2 .....	19-6
19.9	Starting Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2	19-7

## **20 Upgrading Oracle Identity Manager Highly Available Environments**

20.1	Upgrade Roadmap.....	20-2
20.2	Understanding Oracle Identity Manager High Availability Upgrade Topology .....	20-2
20.3	Performing the Pre-Upgrade Tasks.....	20-3
20.4	Upgrading Oracle Home on OIMHOST1 and OIMHOST2.....	20-4
20.5	Upgrading Database Schemas on OIMHOST1.....	20-4
20.6	Performing OIM Middle Tier Upgrade Offline on OIMHOST1 .....	20-4
20.7	Replicating Domain Configuration on OIMHOST2 .....	20-4
20.8	Performing OIM Middle Tier Upgrade Online on OIMHOST1 .....	20-5
20.9	Scaling out Oracle BI Publisher.....	20-6
20.9.1	Creating a new BIP Server on OIMHOST2.....	20-6
20.9.2	Setting the Location of the Shared BI Publisher Configuration Folder .....	20-7
20.9.3	Setting Scheduler Configuration Options .....	20-8
20.9.4	Configuring JMS for BI Publisher .....	20-8
20.9.5	Verifying the BIP Server Scale Out.....	20-10
20.10	Upgrading Other OIM Installed Components on OIMHOST1.....	20-10
20.11	Performing Post-Upgrade Tasks.....	20-10
20.12	Verifying the Upgrade .....	20-10
20.13	Troubleshooting .....	20-11

## **21 Upgrading Oracle Entitlements Server Highly Available Environments**

21.1	Understanding Oracle Entitlements Server High Availability Upgrade Topology.....	21-2
21.2	Upgrade Roadmap.....	21-2
21.3	Shutting Down Administration Server and Managed Servers on OESHOST1 and OESHOST2	21-3
21.4	Backing Up the Existing Environment .....	21-3
21.5	Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST1 .....	21-4
21.6	Upgrading Oracle Platform Security Services Schema on OESHOST1 .....	21-4
21.7	Upgrading Oracle Platform Security Services on OESHOST1 and OESHOST2 .....	21-4

21.8	Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST2 .....	21-4
21.9	Redeploying APM Applications on OESHOST1 and OESHOST2 .....	21-5
21.10	Starting Administration Server and Managed Servers on OESHOST1 and OESHOST2.....	21-6

## **22 Upgrading Oracle Privileged Account Manager Highly Available Environments**

22.1	Understanding Oracle Privileged Account Manager High Availability Upgrade Topology .	22-2
22.2	Upgrade Roadmap.....	22-2
22.3	Shutting Down all Servers on OPAMHOST1 and OPAMHOST2.....	22-3
22.4	Backing Up the Existing Environment .....	22-4
22.5	Updating Binaries of WebLogic Server and Oracle Privileged Account Manager on OPAMHOST1 and OPAMHOST2	22-4
22.6	Upgrading Database Schemas on OPAMHOST1 .....	22-4
22.7	Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2	22-5
22.8	Redeploying Applications on OPAMHOST1 .....	22-5
22.9	Verifying the Domain Upgrade .....	22-5
22.10	Optional: Configuring Oracle Privileged Account Manager Session Manager.....	22-5
22.11	Optional: Configuring Oracle Privileged Account Manager Console Application on WLS_OPAM1 and WLS_OPAM2	22-6

## **23 Upgrading OIM-OAM Integrated Highly Available Environments**

23.1	Understanding the Integrated HA Upgrade Topology.....	23-2
23.2	Upgrade Overview .....	23-4
23.3	Supported Starting Points for an Integrated, HA Upgrade.....	23-5
23.4	Roadmap for Upgrading OIM/OAM/OAAM Integrated Highly Available Environments .	23-6
23.5	Performing the Required Pre-Upgrade Tasks .....	23-6
23.6	Upgrading Oracle Home .....	23-8
23.7	Creating Necessary Schemas and Upgrading the Existing Schemas .....	23-8
23.8	Upgrading Oracle Identity Manager Domain .....	23-9
23.9	Upgrading Oracle Access Management Domain Which Also Contains Oracle Adaptive Access Manager	23-11
23.10	Seeding the Oracle Identity Manager 11.1.2.3.0 Resources in Oracle Access Management ....	23-12
23.11	Verifying the Upgraded Environment.....	23-13
23.12	Troubleshooting .....	23-13

## **Part VI Common Upgrade Tasks and Troubleshooting**

### **24 Tasks Common to Various Manual Upgrade Scenarios**

24.1	Generic Topics .....	24-1
24.1.1	Verifying Certification, System Requirements, and Interoperability .....	24-2
24.1.2	Backing up the Existing Environment .....	24-2

24.1.3	Creating Database Schemas Using Repository Creation Utility.....	24-2
24.1.3.1	Obtaining Repository Creation Utility .....	24-3
24.1.3.2	Starting Repository Creation Utility .....	24-3
24.1.3.3	Creating Schemas .....	24-3
24.1.4	Upgrading Schemas Using Patch Set Assistant .....	24-3
24.1.4.1	Checking Your Database and Schemas .....	24-3
24.1.4.2	Starting Patch Set Assistant .....	24-4
24.1.4.3	Using the Patch Set Assistant Graphical Interface to Upgrade Schemas .....	24-4
24.1.4.4	Verifying Schema Upgrade .....	24-5
24.1.5	Upgrading Oracle WebLogic Server to 11g Release 1 (10.3.6) .....	24-5
24.1.6	Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.3.0) 24-6	
24.1.6.1	Obtaining the Software .....	24-6
24.1.6.2	Starting the Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) Installer 24-6	
24.1.6.3	Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0). 24-7	
24.1.7	Upgrading Oracle Platform Security Services.....	24-8
24.1.8	Starting the Servers.....	24-11
24.1.8.1	Starting the Node Manager.....	24-11
24.1.8.2	Starting the WebLogic Administration Server .....	24-12
24.1.8.3	Starting the Managed Server(s) .....	24-12
24.1.9	Stopping the Servers.....	24-13
24.1.9.1	Stopping the Managed Server(s).....	24-13
24.1.9.2	Stopping the WebLogic Administration Server .....	24-14
24.1.9.3	Stopping the Node Manager.....	24-14
24.2	Oracle Identity Manager Specific Topics.....	24-14
24.2.1	Protected Metadata Files for Which Customization will be Retained After Upgrade .....	24-15
24.2.2	Generating and Analyzing Pre-Upgrade Report for Oracle Identity Manager.....	24-18
24.2.2.1	Obtaining Pre-Upgrade Report Utility .....	24-18
24.2.2.2	Generating the Pre-Upgrade Report.....	24-18
24.2.2.3	Analyzing the Pre-Upgrade Report.....	24-20
24.2.3	Upgrading Oracle SOA Suite to 11g Release 1 (11.1.1.9.0).....	24-32
24.2.4	Upgrading Oracle Identity Manager Middle Tier .....	24-34
24.2.4.1	Additional Task for Windows 64-Bit Users Before Upgrading Middle Tier ..	24-34
24.2.4.2	Creating a Truststore for Upgrading SSL Enabled Middleware .....	24-34
24.2.4.3	Updating the Properties File .....	24-35
24.2.4.4	Performing Oracle Identity Manager Middle Tier Upgrade Offline .....	24-42
24.2.4.5	Starting Administration Server and SOA Managed Server(s).....	24-44
24.2.4.6	Performing Oracle Identity Manager Middle Tier Upgrade Online.....	24-45
24.2.4.7	Starting the Oracle Identity Manager Managed Server(s) and the BIP Server.....	24-46
24.2.4.8	Changing the Deployment Order of Oracle Identity Manager EAR.....	24-46
24.2.5	Upgrading Other Oracle Identity Manager Installed Components .....	24-47
24.2.5.1	Upgrading Oracle Identity Manager Design Console .....	24-47
24.2.5.2	Upgrading Oracle Identity Manager Remote Manager.....	24-48
24.2.6	Performing Oracle Identity Manager Post-Upgrade Tasks .....	24-49
24.2.6.1	After You Upgrade .....	24-51

24.2.6.2	Enabling Oracle BI Publisher .....	24-51
24.2.6.3	Reviewing Performance Tuning Recommendations.....	24-53
24.2.6.4	Creating PeopleSoft Enterprise HRMS Reconciliation Profile.....	24-53
24.2.6.5	Reviewing OIM Data Purge Job Parameters .....	24-53
24.2.6.6	Reconfiguring Lookup Based UDF Field .....	24-54
24.2.6.7	Reviewing Connector Certification.....	24-56
24.2.6.8	Verifying the Functionality of Connectors .....	24-56
24.2.6.9	Validating the Database Objects.....	24-56
24.2.6.10	Impact of Removing Approver-Only Attribute in Request Data Set.....	24-57
24.2.6.11	Changes to Request API After Upgrading to Oracle Identity Manager 11g Release 2 (11.1.2.3.0) .....	24-59
24.2.6.12	Verifying the Compatibility of Oracle Identity Manager Integrated with Oracle Access Manager .....	24-63
24.2.6.13	Running the Entitlement List Schedule.....	24-65
24.2.6.14	Running the Evaluate User Policies Scheduled Task.....	24-66
24.2.6.15	Running Catalog Synchronization.....	24-66
24.2.6.16	UMS Notification Provider .....	24-66
24.2.6.17	Upgrading User UDF.....	24-68
24.2.6.18	Upgrading Application Instances .....	24-71
24.2.6.19	Re XIMDD .....	24-72
24.2.6.20	Re SPML-DSML.....	24-73
24.2.6.21	Customizing Event Handlers.....	24-73
24.2.6.22	Upgrading SOA Composites .....	24-74
24.2.6.23	Authorization Policy Changes.....	24-75
24.2.6.24	Creating Password Policies.....	24-76
24.2.6.25	Migrating Customized Oracle Identity Manager Reports Built on BI Publisher 10g to BI Publisher 11g .....	24-76
24.2.6.26	Updating the Provider URL For ForeignJNDIPProvider-SOA.....	24-77
24.2.6.27	Rebuilding the Indexes of Oracle Identity Manager Table to Change to Reverse Type .....	24-77
24.2.6.28	Reviewing System Property.....	24-78
24.2.6.29	Updating Message Buffer Size for UMSJMServer .....	24-78
24.2.6.30	Changing the Authentication Scheme to TAPScheme After Upgrading Oracle Identity Manager in an OIM-OAM Integrated Environment .....	24-78
24.2.6.31	Updating the URI of the Human Task Service Component with Oracle HTTP Server Details .....	24-78
24.2.6.32	Migrating Approval Policies to Approval Workflow Rules .....	24-79
24.2.6.33	Disabling Oracle SOA Suite Server.....	24-79
24.2.6.34	Adjusting the Width of UDF Components .....	24-79
24.2.6.35	Enabling Certification Using the System Property <code>OIG.IsIdentityAuditorEnabled</code> ..	24-80
24.2.6.36	Updating the OHS Configuration File After Upgrading OIM 11.1.1.x.x Highly Available Environments .....	24-80
24.2.6.37	Observing the UI Changes in the Catalog Page.....	24-81
24.2.6.38	<code>oimclient.jar</code> Needs Update and <code>ipf.jar</code> for Some passwordmgmt VOs.....	24-81
24.3	Oracle Access Management Specific Topics .....	24-81
24.3.1	Extending the 11.1.2.3.0 Access Manager Domain to Include Mobile Security Suite and Policy Manager .....	24-81
24.3.2	Enabling Oracle Mobile Security Suite .....	24-83

24.3.3	Upgrading Oracle Access Management Identity Federation.....	24-85
--------	---	-------

## 25 Troubleshooting Upgrade Issues

25.1	Troubleshooting Oracle Identity Manager Upgrade Issues .....	25-1
25.1.1	Pre-Upgrade Report Generation Fails .....	25-2
25.1.1.1	Validation Failure While Generating Pre-Upgrade Report.....	25-2
25.1.1.2	Plugin Failure While Generating Pre-Upgrade Report.....	25-2
25.1.2	Pre-Upgrade Utility Reports Invalid Objects in OIM Schema .....	25-3
25.1.3	Oracle Identity Manager Binary Upgrade Fails .....	25-4
25.1.4	Patch Set Assistant (PSA) Fails .....	25-4
25.1.5	Upgrade Assistant (UA) Fails .....	25-4
25.1.6	Backups Taken by OIM Middle Tier Upgrade Utility.....	25-4
25.1.7	Errors or Warnings During Oracle Identity Manager Middle Tier Offline Upgrade.....	25-5
25.1.7.1	Validation Failures During OIM Middle Tier Offline Upgrade .....	25-5
25.1.7.2	Plugin Failures During OIM Middle Tier Offline Upgrade .....	25-7
25.1.7.3	Other Failures During OIM Middle Tier Offline Upgrade .....	25-11
25.1.8	Reviewing Autodiscovery.properties File Created During the OIM Middle Tier Upgrade	25-15
25.1.9	Errors or Warning During Oracle Identity Manager Middle Tier Online Upgrade.....	25-16
25.1.9.1	Validation Failures During OIM Middle Tier Online Upgrade .....	25-16
25.1.9.2	Plugin Failures During OIM Middle Tier Online Upgrade .....	25-17
25.1.10	MDS Patching Issues.....	25-18
25.1.11	Some MDS Documents not Merged Correctly .....	25-18
25.1.12	JDBC Errors .....	25-18
25.1.13	Exception in Log When Creating Users .....	25-18
25.1.14	All Features not Upgraded During Oracle Identity Manager Middle Tier Upgrade.....	25-19
25.1.15	Oracle Identity Manager Upgrade Control Points .....	25-19
25.1.16	Performing Basic Sanity Checks .....	25-20
25.1.16.1	Checking New Data Source Added .....	25-20
25.1.16.2	Checking for SOA Foreign JNDI Provider.....	25-20
25.1.16.3	Checking the Order of EARs.....	25-21
25.1.17	Exception While Starting Administration Server After OIM Middle Tier Upgrade in an OIM-OAM-OAAM Integrated Environment	25-22
25.1.18	OIM Incremental Reconciliation Not Working After Upgrading OIM in an OIM-OAM-OAAM Integrated Environment	25-22
25.1.19	Unable to Access Pending Approvals After OIM Middle Tier Online Upgrade ..	25-23
25.1.20	Exception While Running upgradeOpss Command .....	25-23
25.1.21	OIM Middle Tier Online Upgrade Fails in Examine Phase in SSL Environment .	25-24
25.1.22	OIM Schema Upgrade Fails When Upgrading OIM 11.1.2.2.0 .....	25-24
25.1.23	OPSS Authorization Fails After Upgrading to OIM 11.1.2.3.....	25-24
25.2	Troubleshooting Oracle Access Management Upgrade Issues.....	25-25
25.2.1	Exception While Running ImportAccessData Command .....	25-25
25.2.2	Exception While Accessing OAM Console Before Upgrading System Configuration .....	25-25
25.2.3	Exception While Deploying Application .....	25-26

25.2.4	PolicyValidationException While Restarting Administration Server.....	25-27
25.2.5	Exception While Restarting Managed Server .....	25-28
25.2.6	Component Version Shows 11.1.1.5.0 After Upgrade.....	25-28
25.2.7	Errors While Starting the Administration Server After Upgrade.....	25-29
25.2.8	Memory Issues While Running upgradeConfig() Command.....	25-30
25.2.9	Null Exception While Creating IDS Profile .....	25-30
25.2.10	Post Authentication Rules Tab is Disabled on Oracle Access Management Console After Upgrade	25-31
25.2.11	Exception While Running importAccessData Command .....	25-31
25.2.12	.oamkeystore File Size Reduced to 0 Byte After Extending the OAM Domain.....	25-31
25.2.13	upgradeConfig Fails with NullPointerException .....	25-32

---

---

# Preface

This document describes how to upgrade Oracle Identity and Access Management components to 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server.

## Audience

This document is intended for system administrators who are responsible for upgrading existing Oracle Identity and Access Management environments to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

## 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.

## Related Documents

For more information, see the following documents in the Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) documentation library:

- *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Migration Guide for Oracle Identity and Access Management*
- *Oracle Fusion Middleware Administering Oracle Identity Manager*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*
- *Oracle Fusion Middleware Administering Oracle Adaptive Access Manager*
- *Oracle Fusion Middleware Administering Oracle Entitlements Server*
- *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Navigator*
- *Oracle Fusion Middleware Administering Oracle Privileged Account Manager*
- *Oracle Fusion Middleware High Availability Guide*
- *Oracle Fusion Middleware Release Notes*

## Conventions

The following text conventions are used in this document:

<b>Convention</b>	<b>Meaning</b>
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

---

---

# What's New In This Guide

This section summarizes the new features and significant product changes for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) and provides pointers to additional information.

- [New and Changed Features for 11g Release 2 \(11.1.2.3.0\)](#)
- [Other Significant Changes in this Document for 11g Release 2 \(11.1.2.3.0\)](#)

## New and Changed Features for 11g Release 2 (11.1.2.3.0)

The Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) suite includes the following components:

- Oracle Access Management  
For information about new features and enhancements for Oracle Access Management 11.1.2.3.0, see "Product Enhancements for Oracle Access Management 11.1.2.3.0" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.
- Oracle Adaptive Access Manager  
For information about new features and enhancements for Oracle Adaptive Access Manager 11.1.2.3.0, see "New Features and Enhancements for 11g Release 2 (11.1.2.3)" in the *Oracle Fusion Middleware Administering Oracle Adaptive Access Manager*.
- Oracle Identity Manager  
For information about new features and enhancements for Oracle Identity Manager 11.1.2.3.0, see "New and Changed Features for 11g Release 2 (11.1.2.3.0)" in the *Oracle Fusion Middleware Administering Oracle Identity Manager*.
- Oracle Privileged Account Manager  
For information about new features and enhancements for Oracle Privileged Account Manager 11.1.2.3.0, see "New and Changed Features for 11g Release 2 (11.1.2.3.0)" in the *Oracle Fusion Middleware Administering Oracle Privileged Account Manager*.
- Oracle Entitlements Server  
For information about new features and enhancements for Oracle Entitlements Server 11.1.2.3.0, see "Features of Oracle Entitlements Server 11gR2" in the *Oracle Fusion Middleware Administering Oracle Entitlements Server*.

## Other Significant Changes in this Document for 11g Release 2 (11.1.2.3.0)

This document has undergone many changes for 11g Release 2 (11.1.2.3.0). The major updates made to this document includes:

- The automated upgrade procedure for upgrading Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) environments deployed using the Life Cycle Management (LCM) Tools has been added.

For more information about automated upgrade, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

- The procedure for upgrading Oracle Identity Manager, Oracle Access Management, and Oracle Adaptive Access Manager integrated highly available environments to 11g Release 2 (11.1.2.3.0) has been included.

For more information, see [Chapter 23, "Upgrading OIM-OAM Integrated Highly Available Environments"](#).

- The Oracle Identity Navigator chapters have been removed from the guide, as Oracle Identity Navigator is deprecated in 11g Release 2 (11.1.2.3.0).

# Part I

---

## Understanding the Oracle Identity and Access Management Upgrade

This part includes the following chapters:

- [Chapter 1, "Introduction to Oracle Identity and Access Management Upgrade"](#)
- [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#)
- [Chapter 3, "Understanding the Oracle Identity and Access Management Manual Upgrade"](#)



---

---

# Introduction to Oracle Identity and Access Management Upgrade

This chapter provides an overview of the upgrade process for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

This chapter includes the following topics:

- [Section 1.1, "Introduction to Oracle Identity and Access Management 11g Release 2 \(11.1.2.3.0\)"](#)
- [Section 1.2, "Oracle Identity and Access Management Upgrade Overview"](#)
- [Section 1.3, "Migration and Coexistence Scenarios"](#)

## 1.1 Introduction to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)

Oracle Identity and Access Management components enable enterprises to manage the end-to-end lifecycle of user identities across all enterprise resources - both within and beyond the firewall. With Oracle Identity and Access Management, you can deploy applications faster, apply the most granular protection to enterprise resources, automatically eliminate latent access privileges, and much more.

Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) includes the following products:

- Oracle Access Management, which includes the following components:
  - Oracle Access Management Access Manager
  - Oracle Access Management Identity Federation
  - Oracle Access Management Mobile and Social
  - Oracle Access Management Security Token Service
- Oracle Adaptive Access Manager
- Oracle Identity Manager
- Oracle Entitlements Server
- Oracle Privileged Account Manager

For information about new features and enhancements for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0), see [New and Changed Features for 11g Release 2 \(11.1.2.3.0\)](#).

## 1.2 Oracle Identity and Access Management Upgrade Overview

This guide describes how to upgrade Oracle Identity and Access Management 11g Release 1 (11.1.1.x.x) and 11g Release 2 (11.1.2.x.x) to 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server.

---

---

**Note:** ■11.1.1.x.x refers to 11.1.1.7.0 and 11.1.1.5.0.

- 11.1.2.x.x refers to 11.1.2.2.0, 11.1.2.1.0, and 11.1.2.0.0.

Moving from 10g or previous versions to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0), and migrating from Sun product to Oracle Identity and Access Management are considered as migration scenarios, and are covered in *Oracle Fusion Middleware Migration Guide for Oracle Identity and Access Management*.

---

---

If you have deployed Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) using the Life Cycle Management (LCM) Tools, then you must use the automated upgrade tool to upgrade your existing Oracle Identity and Access Management environment to 11g Release 2 (11.1.2.3.0).

For information about the automated upgrade process, topologies supported for upgrade, and the documentation roadmap, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

If you have configured Oracle Identity and Access Management using the Oracle Identity and Access Management Oracle Universal Installer and Fusion Middleware Configuration Wizard, then you must use the manual upgrade procedure to upgrade your existing Oracle Identity and Access Management environment to 11g Release 2 (11.1.2.3.0).

For information about the manual upgrade process and the supported starting points, see [Chapter 3, "Understanding the Oracle Identity and Access Management Manual Upgrade"](#).

## 1.3 Migration and Coexistence Scenarios

The term **Migration** refers to migrating 10g version of Oracle Identity and Access Management components, or Sun products to Oracle Identity and Access Management 11.1.2.3.0. During migration, you must install a new 11g Release 2 (11.1.2.3.0) Oracle Home (*IAM\_HOME*) and then migrate your configuration data from your previous installation to the new 11g Release 2 (11.1.2.3.0) Oracle Home.

The following are migration scenarios supported for 11g Release 2 (11.1.2.3.0):

- Migrating Oracle Access Manager 10g to Oracle Access Management 11.1.2.3.0
- Migrating Oracle Adaptive Access Manager 10g to Oracle Adaptive Access Manager 11.1.2.3.0
- Migrating Oracle Single Sign-On 10g to Oracle Access Management 11.1.2.3.0
- Migrating Sun OpenSSO Enterprise 8.0 to Oracle Access Management 11.1.2.3.0
- Migrating Sun Java System Access Manager 7.1 to Oracle Access Management 11.1.2.3.0
- Migrating Oracle Identity Federation to Oracle Access Management 11.1.2.3.0

- Migrating the certifications of Oracle Identity Analytics to Oracle Identity Manager 11.1.2.3.0

During migration, you can have both the old and the new deployments coexisting, such that some applications are protected by the old server, and the others are protected by the new server. The coexistence mode allows you to have seamless single sign-on experience when you navigate between applications protected by different servers.

For example, Sun OpenSSO Enterprise 8.0 and Oracle Access Management Access Manager 11.1.2.3.0 servers can coexist and work together, so that you have seamless single sign-on experience when you navigate between applications protected by Sun OpenSSO Enterprise 8.0 and Oracle Access Management Access Manager 11.1.2.3.0 Servers.

The following are the coexistence scenarios supported in 11g Release 2 (11.1.2.3.0):

- Coexistence of Oracle Access Manager 10g with Oracle Access Management Access Manager 11.1.2.3.0
- Coexistence of Sun OpenSSO Enterprise 8.0 with Oracle Access Management Access Manager 11.1.2.3.0
- Coexistence of Sun Java System Access Manager 7.1 with Oracle Access Management Access Manager 11.1.2.3.0

---

---

**Note:** This guide does not cover the migration and coexistence scenarios.

For information about the migration and coexistence scenarios supported for 11g Release 2 (11.1.2.3.0), see *Oracle Fusion Middleware Migration Guide for Oracle Identity and Access Management*.

---

---



---

---

# Understanding the Oracle Identity and Access Management Automated Upgrade

This chapter provides an overview of the automated upgrade process for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

This chapter includes the following sections:

- [Section 2.1, "Introduction to Automated Upgrade"](#)
- [Section 2.2, "Deployment Topologies Supported for Automated Upgrade"](#)
- [Section 2.3, "Isolated Upgrade Overview"](#)
- [Section 2.4, "Supported Starting Points for Automated Upgrade"](#)
- [Section 2.5, "Documentation Roadmap"](#)

## 2.1 Introduction to Automated Upgrade

The Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) environments deployed using the Life Cycle Management (LCM) Tool can be upgraded to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) using the automated upgrade process.

---

---

**Note:** For information about the Life Cycle Management (LCM) tool used for deploying Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0), see *Oracle Fusion Middleware Deployment Guide for Oracle Identity and Access Management* in the for 11g Release 2 (11.1.2.2.0).

---

---

The automated upgrade process involves the following high level tasks:

- Performing the pre-validation checks using `preValidate.pl` script
- Upgrading binaries and configurations using `idmUpgrade.pl` script
- Performing post-validation checks using `postValidate.pl` script

---

---

**Note:** The automated upgrade procedure cannot be used for upgrading the Oracle Identity and Access Management environment that is installed and configured manually using the Oracle Identity and Access Management Oracle Universal Installer and Fusion Middleware Configuration tool.

For information about upgrading manually configured Oracle Identity and Access Management environments, see [Chapter 1, "Introduction to Oracle Identity and Access Management Upgrade"](#).

---

---

## 2.2 Deployment Topologies Supported for Automated Upgrade

The following topologies are supported for upgrading using the automated upgrade tool:

### Single Node Setup

- Oracle Identity Manager (OIM) Only Topology  
This topology contains an `OIMHOST` that hosts Oracle Identity Manager and Oracle HTTP Server (OHS).
- Oracle Access Manager (OAM) Suite Only Topology  
This topology contains an `OAMHOST` that hosts Oracle Access Manager and Oracle HTTP Server. This topology can also contain Oracle Adaptive Access Manager if you had extended Oracle Access Manager domain to include Oracle Adaptive Access Manager during 11g Release 2 (11.1.2.2.0) deployment.
- OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology  
This topology contains `IDMHOST` that hosts Oracle Identity Manager, Oracle Access Manager, Oracle Unified Directory, and Oracle HTTP Server.
- Isolated upgrade for OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology  
For more information about isolated upgrade, see [Section 2.3, "Isolated Upgrade Overview"](#).

### Highly Available (HA) Setup

- Oracle Identity Manager (OIM) Only Topology  
This topology contains an `OIMHOST1` and `OIMHOST2` that host Oracle Identity Manager, and `WEBHOST1` and `WEBHOST2` that host Oracle HTTP Server (OHS).
- Oracle Access Manager (OAM) Suite Only Topology  
This topology contains an `OAMHOST1` and `OAMHOST2` that host Oracle Access Manager, and `WEBHOST1` and `WEBHOST2` that host Oracle HTTP Server (OHS).
- OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology  
This topology contains `OIMHOST1` and `OIMHOST2` that host Oracle Identity Manager, `OAMHOST1` and `OAMHOST2` that host Oracle Access Manager, `LDAPHOST1` and `LDAPHOST2` that host Oracle Unified Directory, and `WEBHOST1` and `WEBHOST2` that host Oracle HTTP Server.

---



---

**Note:** The following use cases are supported in Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) Bundle Patch 2:

- Oracle Identity Manager (OIM) Only Highly Available (HA) Topology  
This is a topology with OIMHOST1 and OIMHOST2 hosting Oracle Identity Manager, and WEBHOST1 and WEBHOST2 hosting Oracle HTTP Server.
  - Oracle Access Manager (OAM) Suite Only Highly Available (HA) Topology  
This is a topology with OAMHOST1 and OAMHOST2 hosting Oracle Access Manager, and WEBHOST1 and WEBHOST2 hosting Oracle HTTP Server.
- 
- 

## 2.3 Isolated Upgrade Overview

Isolated upgrade refers to upgrading one of the tiers in OIM-OAM Integrated with Oracle Unified Directory (OUD) topology setup, using the automated upgrade tool, without upgrading the full suite.

For example, you can upgrade only OIM to 11.1.2.3.0, and the rest of the components (OAM, OUD, and OHS) which are on 11.1.2.2.0 will continue to work with the upgraded version of OIM.

### Isolated Upgrade Scenarios Supported for OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a single node

For OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a single node, the following isolated upgrade scenarios are supported:

- Upgrade Oracle Identity Manager (OIM) only
- Upgrade Oracle Access Manager (OAM) only
- Upgrade Oracle Unified Directory (OUD) only
- Upgrade Oracle HTTP Server (OHS) only

---



---

**Note:** Isolated upgrade for OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology is supported on a single node Linux platform only.

Isolated upgrade for OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a highly available (HA) setup is NOT supported.

---



---

## 2.4 Supported Starting Points for Automated Upgrade

Life Cycle Management (LCM) Tools was introduced in Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) to install, configure, and deploy the components of Oracle Identity and Access Management. Therefore, Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) environments deployed using the LCM tool is the only supported starting point for automated upgrade.

## 2.5 Documentation Roadmap

Table 2–1 lists the scenarios supported for automated upgrade, and points to the respective chapters that describe the upgrade procedure.

---



---

**Note:** For the list of topologies supported for automated upgrade, see [Deployment Topologies Supported for Automated Upgrade](#).

---



---

**Table 2–1 Automated Upgrade Roadmap**

Scenario	For the Upgrade Procedure, see
<b>Single Node Setup</b>	
Upgrading Oracle Identity Manager (OIM) Only Topology	<a href="#">Section 4.3, "Upgrading Oracle Identity Manager (OIM) Only Topology on a Single Node"</a>
Upgrading Oracle Access Manager (OAM) Suite Only Topology	<a href="#">Section 4.4, "Upgrading Oracle Access Manager (OAM) Suite Only Topology on a Single Node"</a>
Upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology	<a href="#">Section 4.5, "Upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Single Node"</a>
<b>Highly Available (HA) Setup</b>	
Upgrading Oracle Identity Manager (OIM) Only Topology	<a href="#">Section 5.3, "Upgrading Oracle Identity Manager (OIM) Only on Multiple Nodes"</a>
Upgrading Oracle Access Manager (OAM) Suite Only Topology	<a href="#">Section 5.4, "Upgrading Oracle Access Manager Suite (OAM) Only on Multiple Nodes"</a>
Upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology	<a href="#">Section 5.5, "Upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Highly Available (HA) setup"</a>

---

---

# Understanding the Oracle Identity and Access Management Manual Upgrade

This chapter provides an overview of the manual upgrade process for Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

This chapter includes the following topics:

- [Section 3.1, "Introduction to Manual Upgrade"](#)
- [Section 3.2, "Scenarios Supported for Manual Upgrade"](#)
- [Section 3.3, "Supported Starting Points for Oracle Identity and Access Management Manual Upgrade"](#)
- [Section 3.4, "Documentation Roadmap"](#)

## 3.1 Introduction to Manual Upgrade

The Oracle Identity and Access Management environment configured using the Oracle Identity and Access Management Oracle Universal Installer and the Fusion Middleware Configuration Wizard can be upgraded to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment is deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade your environment to 11g Release 2 (11.1.2.3.0).

For more information about automated upgrade, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

The manual upgrade process involves high level tasks like upgrading *ORACLE\_HOME*, upgrading the Database schemas, and performing any necessary post-upgrade steps.

This guide covers various manual upgrade scenarios. Use the documentation roadmap to navigate to the chapter based on your upgrade scenario.

## 3.2 Scenarios Supported for Manual Upgrade

The following scenarios are supported for manual upgrade:

- [Upgrading Oracle Identity and Access Management Components on a Single Node](#)

- [Upgrading Oracle Identity and Access Management Highly Available Environments](#)
- [Upgrading Oracle Access Management Multi-Data Center Environments](#)
- [Upgrading Oracle Identity Manager, Oracle Access Management, and Oracle Adaptive Access Manager Integrated Highly Available Environments](#)

### 3.2.1 Upgrading Oracle Identity and Access Management Components on a Single Node

You can upgrade the following Oracle Identity and Access Management components to 11.1.2.3.0, on a single node using the manual upgrade procedure:

- Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) Components
  - Oracle Access Manager 11.1.2.2.0
  - Oracle Adaptive Access Manager 11.1.2.2.0
  - Oracle Identity Manager 11.1.2.2.0
  - Oracle Entitlements Server 11.1.2.2.0
  - Oracle Privileged Account Manager 11.1.2.2.0
- Oracle Identity and Access Management 11g Release 2 (11.1.2.1.0) Components
  - Oracle Access Manager 11.1.2.1.0
  - Oracle Adaptive Access Manager 11.1.2.1.0
  - Oracle Identity Manager 11.1.2.1.0
  - Oracle Entitlements Server 11.1.2.1.0
  - Oracle Privileged Account Manager 11.1.2.1.0
- Oracle Identity and Access Management 11g Release 2 (11.1.2) Components
  - Oracle Access Manager 11.1.2
  - Oracle Adaptive Access Manager 11.1.2
  - Oracle Identity Manager 11.1.2
  - Oracle Entitlements Server 11.1.2
  - Oracle Privileged Account Manager 11.1.2
- Oracle Identity and Access Management 11g Release 1 (11.1.1.7.0) Components
  - Oracle Access Manager 11.1.1.7.0
  - Oracle Adaptive Access Manager 11.1.1.7.0
  - Oracle Identity Manager 11.1.1.7.0
- Oracle Identity and Access Management 11g Release 1 (11.1.1.5.0) Components
  - Oracle Access Manager 11.1.1.5.0
  - Oracle Adaptive Access Manager 11.1.1.5.0
  - Oracle Identity Manager 11.1.1.5.0
  - Oracle Entitlements Server 11.1.1.5.0
- Oracle Identity Manager 9.1.x.x

### 3.2.2 Upgrading Oracle Identity and Access Management Highly Available Environments

You can upgrade the following Oracle Identity and Access Management highly available environments to 11.1.2.3.0, using the manual upgrade procedure

- Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) Components
  - Oracle Access Manager 11.1.2.2.0
  - Oracle Adaptive Access Manager 11.1.2.2.0
  - Oracle Identity Manager 11.1.2.2.0
  - Oracle Entitlements Server 11.1.2.2.0
  - Oracle Privileged Account Manager 11.1.2.2.0
- Oracle Identity and Access Management 11g Release 2 (11.1.2.1.0) Components
  - Oracle Access Manager 11.1.2.1.0
  - Oracle Adaptive Access Manager 11.1.2.1.0
  - Oracle Identity Manager 11.1.2.1.0
  - Oracle Entitlements Server 11.1.2.1.0
  - Oracle Privileged Account Manager 11.1.2.1.0
- Oracle Identity and Access Management 11g Release 1 (11.1.1.5.0) Components
  - Oracle Access Manager 11.1.1.5.0
  - Oracle Adaptive Access Manager 11.1.1.5.0
  - Oracle Identity Manager 11.1.1.5.0
  - Oracle Entitlements Server 11.1.1.5.0

### 3.2.3 Upgrading Oracle Access Management Multi-Data Center Environments

You can upgrade the Oracle Access Management multi-data center environment using the manual procedure.

### 3.2.4 Upgrading Oracle Identity Manager, Oracle Access Management, and Oracle Adaptive Access Manager Integrated Highly Available Environments

You can upgrade the integrated highly available environment with the following components to 11.1.2.3.0, using the manual upgrade procedure.

- Oracle Access Manager 11.1.2.2.0
- Oracle Adaptive Access Manager 11.1.2.2.0
- Oracle Identity Manager 11.1.2.2.0

## 3.3 Supported Starting Points for Oracle Identity and Access Management Manual Upgrade

This section describes the supported starting points for Oracle Identity and Access Management upgrade on a single node, on a highly available setup, and on an integrated environment setup.

Table 3–1 lists the supported starting points for Oracle Identity and Access Management manual upgrade.

**Table 3–1 Supported Starting Points for Oracle Identity and Access Management Manual Upgrade**

<b>Component</b>	<b>Supported Starting Points for Single Node Upgrade</b>	<b>Supported Starting Points for Highly Available Environment Upgrade</b>	<b>Supported Starting Points for Integrated Environment Upgrade</b>
Oracle Access Management	<ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ Bundle Patch 11.1.2.1.1</li> <li>■ 11g Release 2 (11.1.2)</li> <li>■ Bundle Patch 11.1.2.0.3</li> <li>■ Bundle Patch 11.1.2.0.2</li> <li>■ Bundle Patch 11.1.2.0.1</li> <li>■ 11g Release 1 (11.1.1.7.0)</li> <li>■ Bundle Patch 11.1.1.7.0 OAM-FAREL8-BP</li> <li>■ Bundle Patch 11.1.1.7.0 OAM-FAREL7-BP</li> <li>■ 11g Release 1 (11.1.1.5.0)</li> <li>■ Bundle Patch 11.1.1.5.5</li> <li>■ Bundle Patch 11.1.1.5.4</li> <li>■ Bundle Patch 11.1.1.5.3</li> <li>■ Bundle Patch 11.1.1.5.2</li> <li>■ Bundle Patch 11.1.1.5.1</li> </ul>	<ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ 11g Release 1 (11.1.1.5.0)</li> </ul>	<ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> </ul>

**Table 3–1 (Cont.) Supported Starting Points for Oracle Identity and Access Management Manual Upgrade**

<b>Component</b>	<b>Supported Starting Points for Single Node Upgrade</b>	<b>Supported Starting Points for Highly Available Environment Upgrade</b>	<b>Supported Starting Points for Integrated Environment Upgrade</b>
Oracle Adaptive Access Manager	<ul style="list-style-type: none"> <li>▪ 11g Release 2 (11.1.2.2.0)</li> <li>▪ 11g Release 2 (11.1.2.1.0)</li> <li>▪ All Bundle Patches are supported</li> <li>▪ 11g Release 2 (11.1.2)</li> <li>▪ All Bundle Patches are supported</li> <li>▪ 11g Release 1 (11.1.1.7.0)</li> <li>▪ All Bundle Patches are supported</li> <li>▪ 11g Release 1 (11.1.1.5.0)</li> <li>▪ Bundle Patch 11.1.1.5.1</li> <li>▪ Bundle Patch 11.1.1.5.2</li> </ul>	<ul style="list-style-type: none"> <li>▪ 11g Release 2 (11.1.2.2.0)</li> <li>▪ 11g Release 2 (11.1.2.1.0)</li> <li>▪ 11g Release 1 (11.1.1.5.0)</li> </ul>	<ul style="list-style-type: none"> <li>▪ 11g Release 2 (11.1.2.2.0)</li> </ul>

**Table 3–1 (Cont.) Supported Starting Points for Oracle Identity and Access Management Manual Upgrade**

<b>Component</b>	<b>Supported Starting Points for Single Node Upgrade</b>	<b>Supported Starting Points for Highly Available Environment Upgrade</b>	<b>Supported Starting Points for Integrated Environment Upgrade</b>
Oracle Identity Manager	<ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0) All Bundle Patches are supported</li> <li>■ 11g Release 2 (11.1.2) All Bundle Patches are supported</li> <li>■ 11g Release 1 (11.1.1.7.0) All Bundle Patches are supported</li> <li>■ 11g Release 1 (11.1.1.5.0) All Bundle Patches are supported</li> <li>■ 9.1.x.x Bundle Patches 9.1.0.1 and higher  If your starting point is Oracle Identity Manager 9.1.x.x, you must first upgrade to Oracle Identity Manager 11g Release 2 (11.1.2.2.0) and then to 11g Release 2 (11.1.2.3.0).  Direct upgrade from Oracle Identity Manager 9.1.x.x to 11.1.2.3.0 is not supported.</li> </ul>	<ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ 11g Release 1 (11.1.1.5.0)</li> </ul>	<ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> </ul>

**Table 3–1 (Cont.) Supported Starting Points for Oracle Identity and Access Management Manual Upgrade**

Component	Supported Starting Points for Single Node Upgrade	Supported Starting Points for Highly Available Environment Upgrade	Supported Starting Points for Integrated Environment Upgrade
Oracle Entitlements Server	<ul style="list-style-type: none"> <li>▪ 11g Release 2 (11.1.2.2.0)</li> <li>▪ 11g Release 2 (11.1.2.1.0) All Bundle Patches are supported</li> <li>▪ 11g Release 2 (11.1.2) All Bundle Patches are supported</li> <li>▪ 11g Release 1 (11.1.1.5.0) Bundle Patch 11.1.1.5.1</li> </ul>	<ul style="list-style-type: none"> <li>▪ 11g Release 2 (11.1.2.2.0)</li> </ul>	NA
Oracle Privileged Account Manager	<ul style="list-style-type: none"> <li>▪ 11g Release 2 (11.1.2.2.0)</li> <li>▪ 11g Release 2 (11.1.2.1.0) All Bundle Patches are supported</li> <li>▪ 11g Release 2 (11.1.2) All Bundle Patches are supported</li> </ul>	<ul style="list-style-type: none"> <li>▪ 11g Release 2 (11.1.2.2.0)</li> <li>▪ 11g Release 2 (11.1.2.1.0)</li> </ul>	NA

### 3.4 Documentation Roadmap

[Table 3–2](#) provides the documentation roadmap for all of the manual upgrade scenarios for Oracle Identity and Access Management.

**Table 3–2 Documentation Roadmap for Oracle Identity and Access Management Upgrade**

Manual Upgrade Scenario	Chapter
<b>Oracle Identity and Access Management 11.1.2.x.x Upgrade on a Single Node</b>  Upgrading the following versions of Oracle Access Management to 11.1.2.3.0 on a single node: <ul style="list-style-type: none"> <li>▪ 11g Release 2 (11.1.2.2.0)</li> <li>▪ 11g Release 2 (11.1.2.1.0)</li> <li>▪ 11g Release 2 (11.1.2)</li> </ul>	<a href="#">Chapter 8, "Upgrading Oracle Access Management 11g Release 2 (11.1.2.x.x) Environments"</a>

**Table 3–2 (Cont.) Documentation Roadmap for Oracle Identity and Access Management Upgrade**

Manual Upgrade Scenario	Chapter
Upgrading the following versions of Oracle Adaptive Access Manager to 11.1.2.3.0 on a single node: <ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ 11g Release 2 (11.1.2)</li> </ul>	<a href="#">Chapter 9, "Upgrading Oracle Adaptive Access Manager 11g Release 2 (11.1.2.x.x) Environments"</a>
Upgrading the following versions of Oracle Identity Manager to 11.1.2.3.0 on a single node: <ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ 11g Release 2 (11.1.2)</li> </ul>	<a href="#">Chapter 10, "Upgrading Oracle Identity Manager 11g Release 2 (11.1.2.x.x) Environments"</a>
Upgrading the following versions of Oracle Entitlements Server to 11.1.2.3.0 on a single node: <ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ 11g Release 2 (11.1.2)</li> </ul>	<a href="#">Chapter 11, "Upgrading Oracle Entitlements Server 11g Release 2 (11.1.2.x.x) Environments"</a>
Upgrading the following versions of Oracle Privileged Account Manager to 11.1.2.3.0 on a single node: <ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ 11g Release 2 (11.1.2)</li> </ul>	<a href="#">Chapter 7, "Upgrading Oracle Privileged Account Manager 11g Release 2 (11.1.2.x.x) Environments"</a>
<b>Oracle Identity and Access Management 11.1.1.x.x and 9.x Upgrade on a Single Node</b>	
Upgrading the following versions of Oracle Access Manager to 11.1.2.3.0 on a single node: <ul style="list-style-type: none"> <li>■ 11g Release 1 (11.1.1.7.0)</li> <li>■ 11g Release 1 (11.1.1.5.0)</li> </ul>	<a href="#">Chapter 12, "Upgrading Oracle Access Manager 11g Release 1 (11.1.1.x.x) Environments"</a>
Upgrading the following versions of Oracle Adaptive Access Manager to 11.1.2.3.0 on a single node: <ul style="list-style-type: none"> <li>■ 11g Release 1 (11.1.1.7.0)</li> <li>■ 11g Release 1 (11.1.1.5.0)</li> </ul>	<a href="#">Chapter 13, "Upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x) Environments"</a>
Upgrading the following versions of Oracle Identity Manager to 11.1.2.3.0 on a single node: <ul style="list-style-type: none"> <li>■ 11g Release 1 (11.1.1.7.0)</li> <li>■ 11g Release 1 (11.1.1.5.0)</li> <li>■ 9.1.x.x</li> </ul>	<a href="#">Chapter 14, "Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.x.x) Environments"</a>  <a href="#">Chapter 16, "Upgrading Oracle Identity Manager 9.1.x.x Environments"</a>

**Table 3–2 (Cont.) Documentation Roadmap for Oracle Identity and Access Management Upgrade**

<b>Manual Upgrade Scenario</b>	<b>Chapter</b>
Upgrading the following version of Oracle Entitlements Server to 11.1.2.3.0 on a single node: <ul style="list-style-type: none"> <li>■ 11g Release 1 (11.1.1.5.0)</li> </ul>	Chapter 15, "Upgrading Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) Environment"
<b>Oracle Identity and Access Management High Availability Upgrade</b>	
Upgrading the following Oracle Access Management High Availability Environments: <ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ 11g Release 1 (11.1.1.5.0)</li> </ul>	Chapter 17, "Upgrading Oracle Access Management Highly Available Environments"
Upgrading Oracle Access Management multi-data center environments.	Chapter 18, "Upgrading Oracle Access Management Multi-Data Center Environments"
Upgrading the following Oracle Adaptive Access Manager High Availability Environments: <ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ 11g Release 1 (11.1.1.5.0)</li> </ul>	Chapter 19, "Upgrading Oracle Adaptive Access Manager Highly Available Environments"
Upgrading the following Oracle Identity Manager High Availability Environments: <ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ 11g Release 1 (11.1.1.5.0)</li> </ul>	Chapter 20, "Upgrading Oracle Identity Manager Highly Available Environments"
Upgrading the following Oracle Entitlements Server High Availability Environments: <ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> <li>■ 11g Release 1 (11.1.1.5.0)</li> </ul>	Chapter 21, "Upgrading Oracle Entitlements Server Highly Available Environments"
Upgrading the following Oracle Privileged Account Manager High Availability Environments: <ul style="list-style-type: none"> <li>■ 11g Release 2 (11.1.2.2.0)</li> <li>■ 11g Release 2 (11.1.2.1.0)</li> </ul>	Chapter 22, "Upgrading Oracle Privileged Account Manager Highly Available Environments"
<b>Upgrading Oracle Identity and Access Management Integrated Highly Available Environments</b>	
Upgrading Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager Integrated Highly Available Environments	Chapter 23, "Upgrading OIM-OAM Integrated Highly Available Environments"



# Part II

---

## Upgrading Oracle Identity and Access Management Environments Deployed Using Life Cycle Management (LCM) Tools

This part includes the following chapters:

- [Chapter 4, "Upgrading Oracle Identity and Access Management Environments Deployed Using Life Cycle Management \(LCM\) Tools on a Single Node"](#)
- [Chapter 5, "Upgrading Oracle Identity and Access Management Highly Available Environments Deployed Using Life Cycle Management \(LCM\) Tools"](#)
- [Chapter 6, "Tasks Common to Various Automated Upgrade Scenarios"](#)



---

---

# Upgrading Oracle Identity and Access Management Environments Deployed Using Life Cycle Management (LCM) Tools on a Single Node

This chapter describes how to upgrade Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) environments that are deployed using the Life Cycle Management (LCM) Tools on a single node, to 11g Release 2 (11.1.2.3.0) using the automated upgrade procedure.

If you wish to upgrade Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) highly available (HA) environments that are deployed using the Life Cycle Management (LCM) Tools, see [Chapter 5, "Upgrading Oracle Identity and Access Management Highly Available Environments Deployed Using Life Cycle Management \(LCM\) Tools"](#).

---

---

**Note:** The upgrade procedure described in this chapter cannot be used to upgrade the Oracle Identity and Access Management environments that are configured manually, using the Oracle Universal Installer and Fusion Middleware Configuration wizard.

For information about upgrading Oracle Identity and Access Management environments that configured manually, see [Chapter 1, "Introduction to Oracle Identity and Access Management Upgrade"](#).

---

---

Before you proceed, review the automated upgrade overview, deployment topologies supported for automated upgrade, and the supported starting points described in [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

**Note:** For information about any latest patches, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Release Notes for Identity Management*.

---

---

This chapter includes the following sections:

- [Section 4.1, "Variables Used in This Chapter"](#)
- [Section 4.2, "Upgrade Scenarios Covered in this Chapter"](#)

- [Section 4.3, "Upgrading Oracle Identity Manager \(OIM\) Only Topology on a Single Node"](#)
- [Section 4.4, "Upgrading Oracle Access Manager \(OAM\) Suite Only Topology on a Single Node"](#)
- [Section 4.5, "Upgrading OIM-OAM Integrated with Oracle Unified Directory \(OUD\) Topology on a Single Node"](#)
- [Section 4.6, "Performing Isolated Upgrade for OIM-OAM Integrated with Oracle Unified Directory \(OUD\) Topology on a Single Node"](#)
- [Section 4.7, "Troubleshooting"](#)

## 4.1 Variables Used in This Chapter

Table 4–1 lists the variables used in this chapter.

**Table 4–1 Variables Used in This Chapter and Their Descriptions**

Variable	Description
<code>SCRIPT_FILE_LOCATION</code>	This is the location where you copied the upgrade tool <code>idmUpgrade.zip</code> , and extracted the files.
<code>OIMHOST</code>	This is the host on which Oracle Identity Manager (OIM) Suite Only topology is deployed. The following components are installed on this host: <ul style="list-style-type: none"> <li>■ Oracle Identity Manager</li> <li>■ Oracle HTTP Server</li> </ul>
<code>OAMHOST</code>	This is the host on which Oracle Access Manager (OAM) Suite Only topology is deployed. The following components are installed on this host: <ul style="list-style-type: none"> <li>■ Oracle Access Manager</li> <li>■ Oracle HTTP Server</li> </ul>
<code>IDMHOST</code>	This is the host on which OIM-OAM Integrated with Oracle Unified Directory (OUD) topology is deployed. The following components are installed on this host: <ul style="list-style-type: none"> <li>■ Oracle Identity Manager</li> <li>■ Oracle Access Manager</li> <li>■ Oracle Unified Directory</li> <li>■ Oracle HTTP Server</li> </ul>

## 4.2 Upgrade Scenarios Covered in this Chapter

This chapter describes how to upgrade the following Oracle Identity and Access Management topologies deployed using the Life Cycle Management (LCM) Tools:

- Oracle Identity Manager (OIM) Only Topology on a Single Node  
For information about upgrading Oracle Identity Manager (OIM) Only topology on a single node, see [Section 4.3, "Upgrading Oracle Identity Manager \(OIM\) Only Topology on a Single Node"](#).
- Oracle Access Manager (OAM) Suite Only Topology on a Single Node

For information about upgrading Oracle Access Manager (OAM) Suite Only topology on a single node, see [Section 4.4, "Upgrading Oracle Access Manager \(OAM\) Suite Only Topology on a Single Node"](#).

- OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Single Node

For information about upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) topology on a single node, see [Section 4.5, "Upgrading OIM-OAM Integrated with Oracle Unified Directory \(OUD\) Topology on a Single Node"](#).

- Isolated Upgrade for OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Single Node

For information about performing isolated upgrade for OIM-OAM Integrated with Oracle Unified Directory (OUD) topology on a single node, see [Section 4.6, "Performing Isolated Upgrade for OIM-OAM Integrated with Oracle Unified Directory \(OUD\) Topology on a Single Node"](#).

---

**Note:** For more information about isolated upgrade, see [Section 2.3, "Isolated Upgrade Overview"](#).

For the list of scenarios supported for automated upgrade, see [Section 2.2, "Deployment Topologies Supported for Automated Upgrade"](#).

---

## 4.3 Upgrading Oracle Identity Manager (OIM) Only Topology on a Single Node

This section describes how to upgrade Oracle Identity Manager (OIM) Only topology on a single node deployed using LCM tool, from 11g Release 2 (11.1.2.2.0) to 11g Release 2 (11.1.2.3.0).

This topology contains OIMHOST that hosts Oracle Identity Manager and Oracle HTTP Server (OHS).

As part of the Oracle Identity Manager upgrade, the embedded Oracle BI Publisher (BIP) will be installed and configured with Oracle Identity Manager. Therefore, after upgrading to Oracle Identity Manager 11.1.2.3.0, you can choose to either use the embedded BI Publisher or continue to use the standalone Oracle BI Publisher. If you choose to use the embedded BI Publisher and discontinue using the standalone BIP, then you must migrate the existing BIP reports to embedded BIP.

To upgrade Oracle Identity Manager (OIM) Only topology on a single node, perform the following tasks:

1. [Completing the Prerequisites](#)
2. [Obtaining the Software](#)
3. [Setting the Environment Variables](#)
4. [Updating the Properties File](#)
5. [Performing Pre-Validation Checks on OIMHOST](#)
6. [Creating BIP Schema for OIM Upgrade \(Only on Solaris, IBM AIX, and HP Itanium Platforms\)](#)
7. [Stopping All Servers on OIMHOST](#)

8. [Backing Up Database and WebLogic Domain](#)
9. [Upgrading Binaries and Configuration on OIMHOST](#)
10. [Performing Post-Validation Checks on OIMHOST](#)
11. [Verifying the Upgrade](#)

### 4.3.1 Completing the Prerequisites

Before you start with the upgrade process, you must complete the following prerequisites:

1. Review the system requirements and certification document and make sure that your existing environment meets all hardware and software requirements necessary for 11g Release 2 (11.1.2.3.0) software. For more information, see [Section 6.2, "Reviewing System Requirements and Certifications"](#).
2. On OIMHOST, ensure that the `/etc/hosts` file contains both canonical hostnames (fully qualified host names) along with the hostname entry. For more information, see ["Section 6.5, "Verifying Hostnames in the Hosts File"](#).

### 4.3.2 Obtaining the Software

Obtain the file `idmUpgrade.zip` that contains the upgrade scripts. Copy the zip file to any accessible location on OIMHOST and extract the contents of the zip file. For more information about obtaining the zip file, and extracting the contents, see [Section 6.6, "Obtaining the Automated Upgrade Tool"](#).

---

---

**Note:** The instructions for performing an automated upgrade of Oracle Identity and Access Management to 11g Release 2 (11.1.2.3.0) assume you have applied the Oracle Identity and Access Management Automated Upgrade Tool Bundle Patch 2 (11.1.2.3.2). To download this patch, go to the following URL:

<https://updates.oracle.com/download/21419345.html>

---

---

### 4.3.3 Setting the Environment Variables

Before you start with the upgrade process, you must set the required environment variables on OIMHOST depending on the platform on which you are upgrading Oracle Identity and Access Management. For more information, see [Section 6.4, "Setting the Required Environment Variables Necessary for Upgrade"](#).

### 4.3.4 Updating the Properties File

You must update the `upgrade.properties` file located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties` on OIMHOST with the values for the required properties.

For information about the properties that you must update for upgrading Oracle Identity Manager (OIM) Only topology, see [Section 6.7, "Updating the upgrade.properties File"](#).

### 4.3.5 Performing Pre-Validation Checks on OIMHOST

After you update the properties file, you must perform pre-validation checks on OIMHOST for both Oracle Identity Manager and Oracle HTTP Server. To do this, complete the following steps:

1. Run the `preValidate.pl` script for Oracle Identity Manager by specifying OIM for the argument `-node`.
2. Run the `preValidate.pl` script for Oracle HTTP Server by specifying WEBTIER for the argument `-node`.

For general syntax of the `preValidate.pl` script and for information about running the script, see [Section 6.8, "Performing Pre-Validation Checks Using preValidate.pl Script"](#).

### 4.3.6 Creating BIP Schema for OIM Upgrade (Only on Solaris, IBM AIX, and HP Itanium Platforms)

If you are upgrading Oracle Identity Manager on platforms such as Solaris, IBM AIX, and HP Itanium using the automated upgrade tool, you must create the Oracle BI Publisher (BIPLATFORM) schema manually using the Repository Creation Utility (RCU) 11.1.2.3.0 from the machine that is running Linux or Windows operating system.

For more information about creating schema using RCU, see [Section 6.9, "Creating BIP Schema for Oracle Identity Manager Upgrade on Solaris, IBM AIX, and HP Itanium Platforms"](#).

---



---

**Note:** If you are upgrading Oracle Identity Manager on Linux, skip this step, as the automated upgrade tool creates the BIPLATFORM schema on Linux.

---



---

### 4.3.7 Stopping All Servers on OIMHOST

You must stop the following servers on OIMHOST:

1. Oracle HTTP Server
2. Oracle Identity Manager Managed Server(s)
3. Oracle SOA Suite Managed Server(s)
4. WebLogic Administration Server

To stop all of the servers on a host, run the following command script from the location `SHARED_CONFIG_DIR/config/scripts`:

```
./stopall.sh
```

### 4.3.8 Backing Up Database and WebLogic Domain

Before you run the upgrade script, you must backup your Database schemas and the WebLogic domain on OIMHOST. For more information, see [Section 6.3, "Backing up the Existing Environment"](#).

### 4.3.9 Upgrading Binaries and Configuration on OIMHOST

You must upgrade binaries and configuration of both Oracle Identity Manager and Oracle HTTP Server on OIMHOST using the `idmUpgrade.pl` script.

Both binary upgrade and configuration upgrade can be performed together by specifying the value `both` for the argument `-mode` while running the script. When you do so, the upgrade script performs the binary upgrade first followed by the configuration upgrade. If you do not specify any value for the argument `-mode`, the value will be taken as `both`, as it is the default value. Therefore, `-mode` is an optional argument when you upgrade Oracle Identity Manager on a single node.

---

---

**Note:** Make sure that the Database services are up and running before you run the upgrade script.

---

---

To upgrade the binaries and configurations of Oracle Identity Manager and Oracle HTTP Server on `OIMHOST`, complete the following steps:

1. Run the `idmUpgrade.pl` script on `OIMHOST` for upgrading the binaries and configurations of Oracle Identity Manager by specifying `OIM` for the argument `-node` and `both` for the argument `-mode`.
2. Run the `idmUpgrade.pl` script on `OIMHOST` for upgrading the binaries and configurations of Oracle HTTP Server by specifying `WEBTIER` for the argument `-node` and `both` for the argument `-mode`.

For general syntax of the `idmUpgrade.pl` script and for information about running the script, see [Section 6.10, "Upgrading Oracle Identity and Access Management Binaries and Configuration Using `idmUpgrade.pl` script"](#).

#### 4.3.10 Performing Post-Validation Checks on OIMHOST

After you upgrade binaries and configuration, you must perform post-validation checks on `OIMHOST` for both Oracle Identity Manager and Oracle HTTP Server using the `postValidate.pl` script.

To perform the post-validation checks on `OIMHOST`, complete the following steps:

1. Run the `postValidate.pl` script for Oracle Identity Manager by specifying `OIM` for the argument `-node`.
2. Run the `postValidate.pl` script for Oracle HTTP Server by specifying `WEBTIER` for the argument `-node`.

For general syntax of the `postValidate.pl` script and for information about running the script, see [Section 6.11, "Performing Post-Validation Checks Using `postValidate.pl` Script"](#).

#### 4.3.11 Verifying the Upgrade

After you perform the post-validation checks, verify the Oracle Identity Manager upgrade by checking the log files on `OIMHOST`. Log files are created at the location you specified for `LOG_DIR` parameter in the `upgrade.properties` file.

### 4.4 Upgrading Oracle Access Manager (OAM) Suite Only Topology on a Single Node

This section describes how to upgrade Oracle Access Manager (OAM) Suite Only topology on a single node deployed using LCM tool, from 11g Release 2 (11.1.2.2.0) to 11g Release 2 (11.1.2.3.0).

This topology contains OAMHOST that hosts Oracle Access Manager and Oracle HTTP Server (OHS). This topology can also include Oracle Adaptive Access Manager if you had extended your Oracle Access Manager 11g Release 2 (11.1.2.2.0) domain to Oracle Adaptive Access Manager post-deployment.

Oracle Access Manager 11g Release 2 (11.1.2.3.0) has a new feature called Oracle Mobile Security Suite. You can enable Oracle Mobile Security Suite post-upgrade. For an introduction to Oracle Mobile Security Suite, see "Understanding Oracle Mobile Security Suite" in *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*.

---

**Note:** Upgrade is supported on OAM only environment with non-embedded LDAP - Oracle Unified Directory (OUD), Oracle Internet Directory (OID), and Microsoft Active Directory (AD). Upgrading OAM only environment with embedded LDAP is NOT supported.

---

To upgrade Oracle Access Manager (OAM) Suite Only topology on a single node, perform the following tasks:

1. [Completing the Prerequisites](#)
2. [Obtaining the Software](#)
3. [Setting the Environment Variables](#)
4. [Updating the Properties File](#)
5. [Performing Pre-Validation Checks on OAMHOST](#)
6. [Stopping All Servers on OAMHOST](#)
7. [Backing Up Database and WebLogic Domain](#)
8. [Upgrading Binaries and Configuration on OAMHOST](#)
9. [Performing Post-Validation Checks on OAMHOST](#)
10. [Verifying the Upgrade](#)

#### 4.4.1 Completing the Prerequisites

Before you start with the upgrade process, you must complete the following prerequisites:

1. Review the system requirements and certification document and make sure that your existing environment meets all hardware and software requirements necessary for 11g Release 2 (11.1.2.3.0) software. For more information, see [Section 6.2, "Reviewing System Requirements and Certifications"](#).
2. On OAMHOST, ensure that the `/etc/hosts` file contains both canonical hostnames (fully qualified host names) along with the hostname entry. For more information, see ["Section 6.5, "Verifying Hostnames in the Hosts File"](#).
3. Verify that the Oracle Adaptive Access Manager (OAAM) Administration Server is accessible at the following URL:

```
http://OAM_HOST:OAAM_ADMIN_PORT/oaam_admin
```

Use the OAAM admin username and OAAM admin password to access the OAAM Administration Server.

For example:

`http://identity.example.com:14200/oaam_admin`

Username: oaamadminuser

Password: welcome1

## 4.4.2 Obtaining the Software

Obtain the file `idmUpgrade.zip` that contains the upgrade scripts. Copy the zip file to any accessible location on `OAMHOST` and extract the contents of the zip file on both the hosts. For more information about obtaining the zip file, and extracting the contents, see [Section 6.6, "Obtaining the Automated Upgrade Tool"](#).

---

---

**Note:** The instructions for performing an automated upgrade of Oracle Identity and Access Management to 11g Release 2 (11.1.2.3.0) assume you have applied the Oracle Identity and Access Management Automated Upgrade Tool Bundle Patch 2 (11.1.2.3.2). To download this patch, go to the following URL:

<https://updates.oracle.com/download/21419345.html>

---

---

## 4.4.3 Setting the Environment Variables

Before you start with the upgrade process, you must set the required environment variables on `OAMHOST` depending on the platform on which you are upgrading Oracle Identity and Access Management. For more information, see [Section 6.4, "Setting the Required Environment Variables Necessary for Upgrade"](#).

## 4.4.4 Updating the Properties File

You must update the `upgrade.properties` file located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties` on `OAMHOST` with the values for the required properties.

For information about the properties that you must update for upgrading Oracle Access Manager (OAM) Only topology, see [Section 6.7, "Updating the upgrade.properties File"](#).

## 4.4.5 Performing Pre-Validation Checks on OAMHOST

After you update the properties file, you must perform pre-validation checks for both Oracle Access Manager and Oracle HTTP Server on `OAMHOST`, using the `preValidate.pl` script. To perform pre-validation checks, complete the following steps:

1. Run the `preValidate.pl` script for Oracle Access Manager by specifying `OAM` for the argument `-node`.
2. Run the `preValidate.pl` script for Oracle HTTP Server by specifying `WEBTIER` for the argument `-node`.

For general syntax of the `preValidate.pl` script and for information about running the script, see [Section 6.8, "Performing Pre-Validation Checks Using preValidate.pl Script"](#).

## 4.4.6 Stopping All Servers on OAMHOST

You must stop the following server(s) on `OAMHOST`:

1. Oracle HTTP Server

2. Oracle Access Manager Managed Server(s)
3. WebLogic Administration Server

To stop all of the servers on a host, run the following command script from the location `SHARED_CONFIG_DIR/config/scripts`:

```
./stopall.sh
```

#### 4.4.7 Backing Up Database and WebLogic Domain

Before you run the upgrade script, you must backup your Database schemas and the WebLogic domain on OAMHOST. For more information, see [Section 6.3, "Backing up the Existing Environment"](#).

#### 4.4.8 Upgrading Binaries and Configuration on OAMHOST

You must upgrade binaries and configuration of both Oracle Access Manager and Oracle HTTP Server on OAMHOST using the `idmUpgrade.pl` script.

Both binary upgrade and configuration upgrade can be performed together by specifying the value `both` for the argument `-mode` while running the script. When you do so, the upgrade script performs the binary upgrade first followed by the configuration upgrade. If you do not specify any value for the argument `-mode`, the value will be taken as `both`, as it is the default value. Therefore, `-mode` is an optional argument when you upgrade Oracle Identity Manager on a single node.

---



---

**Note:** Make sure that the Database services are up and running before you run the upgrade script.

---



---

To upgrade the binaries and configurations of Oracle Access Manager and Oracle HTTP Server on OAMHOST, complete the following steps:

1. Run the `idmUpgrade.pl` script on OAMHOST for upgrading the binaries and configurations of Oracle Access Manager by specifying `OAM` for the argument `-node` and `both` for the argument `-mode`.
2. Run the `idmUpgrade.pl` script on OAMHOST for upgrading the binaries and configurations of Oracle HTTP Server by specifying `WEBTIER` for the argument `-node` and `both` for the argument `-mode`.

For general syntax of the `idmUpgrade.pl` script and for information about running the script, see [Section 6.10, "Upgrading Oracle Identity and Access Management Binaries and Configuration Using `idmUpgrade.pl` script"](#).

#### 4.4.9 Performing Post-Validation Checks on OAMHOST

After you upgrade binaries and configuration, you must perform post-validation checks on OAMHOST for both Oracle Access Manager and Oracle HTTP Server using the `postValidate.pl` script.

To perform the post-validation checks on OAMHOST, complete the following steps:

1. Run the `postValidate.pl` script for Oracle Access Manager by specifying `OAM` for the argument `-node`.
2. Run the `postValidate.pl` script for Oracle HTTP Server by specifying `WEBTIER` for the argument `-node`.

For general syntax of the `postValidate.pl` script and for information about running the script, see [Section 6.11, "Performing Post-Validation Checks Using `postValidate.pl` Script"](#).

#### 4.4.10 Verifying the Upgrade

After you perform the post-validation checks, verify the Oracle Access Manager upgrade by checking the log files on `OAMHOST`. Log files are created at the location you specified for `LOG_DIR` parameter in the `upgrade.properties` file.

### 4.5 Upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Single Node

This section describes how to upgrade OIM-OAM Integrated with Oracle Unified Directory (OUD) topology on a single node deployed using LCM tool, from 11g Release 2 (11.1.2.2.0) to 11g Release 2 (11.1.2.3.0).

This topology contains `IDMHOST` that hosts Oracle Identity Manager, Oracle Access Manager, and Oracle Unified Directory, and Oracle HTTP Server.

As part of the Oracle Identity Manager upgrade, the embedded Oracle BI Publisher (BIP) will be installed and configured with Oracle Identity Manager. Therefore, after upgrading to Oracle Identity Manager 11.1.2.3.0, you can choose to either use the embedded BI Publisher or continue to use the standalone Oracle BI Publisher. If you choose to use the embedded BI Publisher and discontinue using the standalone BIP, then you must migrate the existing BIP reports to embedded BIP.

Oracle Access Manager 11g Release 2 (11.1.2.3.0) has a new feature called Oracle Mobile Security Suite. You can enable Oracle Mobile Security Suite post-upgrade. For an introduction to Oracle Mobile Security Suite, see "Understanding Oracle Mobile Security Suite" in *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*.

---

---

**Note:** Isolated upgrade is supported on Linux. It implies that you can choose to upgrade only one of the tiers in OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology to 11.1.2.3.0. The upgraded tier should function properly with the rest of the tiers which are still at 11g Release 2 (11.1.2.2.0).

For more information about isolated upgrade, see [Section 2.3, "Isolated Upgrade Overview"](#).

For information about performing isolated upgrade, see [Section 4.6, "Performing Isolated Upgrade for OIM-OAM Integrated with Oracle Unified Directory \(OUD\) Topology on a Single Node"](#).

---

---

To upgrade OIM-OAM Integrated with Oracle Unified Directory (OUD) topology on a single node, perform the following tasks:

1. [Completing the Prerequisites](#)
2. [Obtaining the Software](#)
3. [Setting the Environment Variables](#)
4. [Updating the Properties File](#)
5. [Performing Pre-Validation Checks on `IDMHOST`](#)

6. [Creating BIP Schema for OIM Upgrade \(Only on Solaris, IBM AIX, and HP Itanium Platforms\)](#)
7. [Stopping All Servers on IDMHOST](#)
8. [Backing Up Database and WebLogic Domain](#)
9. [Upgrading Binaries and Configuration on IDMHOST](#)
10. [Performing Post-Validation Checks on IDMHOST](#)
11. [Performing the Required Post-Upgrade Tasks](#)
12. [Verifying the Upgrade](#)

### 4.5.1 Completing the Prerequisites

Before you start with the upgrade process, you must complete the following prerequisites:

1. Review the system requirements and certification document and make sure that your existing environment meets all hardware and software requirements necessary for 11g Release 2 (11.1.2.3.0) software. For more information, see [Section 6.2, "Reviewing System Requirements and Certifications"](#).
2. On IDMHOST, ensure that the `/etc/hosts` file contains both canonical hostnames (fully qualified host names) along with the hostname entry. For more information, see ["Section 6.5, "Verifying Hostnames in the Hosts File"](#).
3. Verify that the Oracle Adaptive Access Manager (OAAM) Administration Server is accessible at the following URL:

`http://OAM_HOST:OAAM_ADMIN_PORT/oaam_admin`

Use the OAAM admin username and OAAM admin password to access the OAAM Administration Server.

For example:

`http://identity.example.com:14200/oaam_admin`

Username: oaamadminuser

Password: Welcome1

### 4.5.2 Obtaining the Software

Obtain the file `idmUpgrade.zip` that contains the upgrade scripts. Copy the zip file to any accessible location on IDMHOST, and extract the contents of the zip file. For more information about obtaining the zip file, and extracting the contents, see [Section 6.6, "Obtaining the Automated Upgrade Tool"](#).

---

---

**Note:** The instructions for performing an automated upgrade of Oracle Identity and Access Management to 11g Release 2 (11.1.2.3.0) assume you have applied the Oracle Identity and Access Management Automated Upgrade Tool Bundle Patch 2 (11.1.2.3.2). To download this patch, go to the following URL:

<https://updates.oracle.com/download/21419345.html>

---

---

### 4.5.3 Setting the Environment Variables

Before you start with the upgrade process, you must set the required environment variables depending on the platform on which you are upgrading Oracle Identity and Access Management. For more information, see [Section 6.4, "Setting the Required Environment Variables Necessary for Upgrade"](#).

### 4.5.4 Updating the Properties File

You must update the `upgrade.properties` file located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties` on `IDMHOST`, with the values for the required properties.

For information about the properties that you must update for upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) topology, see [Section 6.7, "Updating the upgrade.properties File"](#).

### 4.5.5 Performing Pre-Validation Checks on IDMHOST

After you update the properties file, you must perform pre-validation checks on `IDMHOST` for Oracle Identity Manager, Oracle Access Manager, and Oracle Unified Directory, and Oracle HTTP Server, using the `preValidate.pl` script.

To perform the pre-validation checks, complete the following tasks on `IDMHOST`:

1. Run the `preValidate.pl` script for Oracle Access Manager by specifying `OAM` for the argument `-node`.
2. Run the `preValidate.pl` script for Oracle Identity Manager by specifying `OIM` for the argument `-node`.
3. Run the `preValidate.pl` script for Oracle HTTP Server by specifying `WEBTIER` for the argument `-node`.
4. Run the `preValidate.pl` script for Oracle Unified Directory by specifying `DIRECTORY` for the argument `-node`.

For general syntax of the `preValidate.pl` script and for information about running the script, see [Section 6.8, "Performing Pre-Validation Checks Using preValidate.pl Script"](#).

---

---

**Note:** If you wish to perform the pre-validation checks for Oracle Unified Directory first, you must copy the files `libnntz11.so` and `libcIntsh.so.11.1` to the folder `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/lib` on `LDAPHOST` from one of the following locations:

- `IAD_WL_HOME/server/adr`
- `IGD_WL_HOME/server/adr`
- `Web_Tier_ORACLE_HOME/lib`

`IAD_WL_HOME` refers to the **IAMAccessDomain** and `IGD_WL_HOME` refers to the **IAMGovernanceDomain**.

After you copy the files, you can perform the pre-validation checks for Oracle Unified Directory.

---

---

## 4.5.6 Creating BIP Schema for OIM Upgrade (Only on Solaris, IBM AIX, and HP Itanium Platforms)

If you are upgrading Oracle Identity Manager on platforms such as Solaris, IBM AIX, and HP Itanium using the automated upgrade tool, you must create the Oracle BI Publisher (BIPLATFORM) schema manually using the Repository Creation Utility (RCU) 11.1.2.3.0 from the machine that is running Linux or Windows operating system.

For more information about creating schema using RCU, see [Section 6.9, "Creating BIP Schema for Oracle Identity Manager Upgrade on Solaris, IBM AIX, and HP Itanium Platforms"](#).

---

---

**Note:** If you are upgrading Oracle Identity Manager on Linux, skip this step, as the automated upgrade tool creates the BIPLATFORM schema on Linux.

---

---

## 4.5.7 Stopping All Servers on IDMHOST

You must stop the following server(s) on `IDMHOST`:

1. Oracle HTTP Server.
2. Oracle Access Manager Managed Server(s)
3. Oracle Identity Manager Managed Server(s)
4. Oracle SOA Suite Managed Server(s)
5. WebLogic Administration Server.
6. Oracle Unified Directory

To stop all of the servers on a host, run the following command script from the location `SHARED_CONFIG_DIR/config/scripts`:

```
./stopall.sh
```

## 4.5.8 Backing Up Database and WebLogic Domain

Before you run the upgrade script, you must backup your Database schemas and the WebLogic domain. For more information, see [Section 6.3, "Backing up the Existing Environment"](#).

## 4.5.9 Upgrading Binaries and Configuration on IDMHOST

You must upgrade binaries and configuration of Oracle Identity Manager, Oracle Access Manager, and Oracle Unified Directory, and Oracle HTTP Server, using the `idmUpgrade.pl` script.

Both binary upgrade and configuration upgrade can be performed together by specifying the value `both` for the argument `-mode` while running the script. When you do so, the upgrade script performs the binary upgrade first followed by the configuration upgrade. If you do not specify any value for the argument `-mode`, the value will be taken as `both`, as it is the default value. Therefore, `-mode` is an optional argument when you upgrade Oracle Identity Manager on a single node.

---

---

**Note:** Make sure that the Database services are up and running before you run the upgrade script.

---

---

To upgrade the binaries and configurations on `IDMHOST`, complete the following steps:

1. Run the `idmUpgrade.pl` script to upgrade the binaries and configurations of Oracle Unified Directory by specifying `DIRECTORY` for the argument `-node` and both for the argument `-mode`.

---

---

**Note:** Before you upgrade the binaries and configuration of Oracle Unified Directory (OUD), ensure that you have stopped the Oracle Identity Manager and Oracle Access Manager Managed Servers.

---

---

2. Run the `idmUpgrade.pl` script to upgrade the binaries and configurations of Oracle Access Manager by specifying `OAM` for the argument `-node` and both for the argument `-mode`.
3. Run the `idmUpgrade.pl` script to upgrade the binaries and configurations of Oracle Identity Manager by specifying `OIM` for the argument `-node` and both for the argument `-mode`.

---

---

**Note:** Before you upgrade the binaries and configuration of Oracle Identity Manager, ensure that you have stopped the Oracle Access Manager Managed Server(s).

---

---

4. Run the `idmUpgrade.pl` script to upgrade the binaries and configurations of Oracle HTTP Server by specifying `WEBTIER` for the argument `-node` and both for the argument `-mode`.

For general syntax of the `idmUpgrade.pl` script and for information about running the script, see [Section 6.10, "Upgrading Oracle Identity and Access Management Binaries and Configuration Using `idmUpgrade.pl` script"](#).

#### 4.5.10 Performing Post-Validation Checks on `IDMHOST`

After you update the properties file, you must perform post-validation checks on `IDMHOST` for Oracle Identity Manager, Oracle Access Manager, and Oracle Unified Directory, and Oracle HTTP Server, using the `postValidate.pl` script.

To perform the post-validation checks, complete the following tasks on `IDMHOST`:

1. Run the `postValidate.pl` script for Oracle Access Manager by specifying `OAM` for the argument `-node`.
2. Run the `postValidate.pl` script for Oracle Identity Manager by specifying `OIM` for the argument `-node`.
3. Run the `postValidate.pl` script for Oracle HTTP Server by specifying `WEBTIER` for the argument `-node`.
4. Run the `postValidate.pl` script for Oracle Unified Directory by specifying `DIRECTORY` for the argument `-node`.

For general syntax of the `postValidate.pl` script and for information about running the script, see [Section 6.11, "Performing Post-Validation Checks Using `postValidate.pl` Script"](#).

## 4.5.11 Performing the Required Post-Upgrade Tasks

This section lists the post-upgrade tasks required for some of the features to work post-upgrade. Perform the post-upgrade tasks based on your requirement.

This section includes the following topics:

- [Adding the JAVA System Property if you have Configured OAM](#)

### 4.5.11.1 Adding the JAVA System Property if you have Configured OAM

If you have configured Oracle Adaptive Access Manager in OIM-OAM Integrated with Oracle Unified Directory (OUD) topology, you must add the JAVA system property `-Djava.security.auth.login.config` to the `setDomainEnv.sh` script located in the `IAMAccessDomain`. For more information, see [Section 6.13.1, "Adding the Java System Property for Oracle Adaptive Access Manager"](#).

## 4.5.12 Verifying the Upgrade

After you perform the post-validation checks, verify the upgrade by checking the log files on `IDMHOST`. Log files are created at the location you specified for `LOG_DIR` parameter in the `upgrade.properties` file.

## 4.6 Performing Isolated Upgrade for OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Single Node

If you have deployed OIM-OAM Integrated with Oracle Unified Directory (OUD) topology on a single node using the LCM tool 11g Release 2 (11.1.2.2.0), you can choose to upgrade only one of the components without upgrading the entire suite.

In this section, `IDMHOST` refers to the host on which OIM-OAM Integrated with Oracle Unified Directory (OUD) topology is deployed.

---



---

**Note:** Isolated upgrade for OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology is supported on a single node Linux platform only.

---



---

For more information about isolated upgrade, see [Section 2.3, "Isolated Upgrade Overview"](#).

---



---

**Note:** If you wish to upgrade the full suite, that is the OIM-OAM Integrated with Oracle Unified Directory (OUD) topology on a single node, follow the instructions described in the section [Section 4.5, "Upgrading OIM-OAM Integrated with Oracle Unified Directory \(OUD\) Topology on a Single Node"](#).

---



---

For an OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a single node, the following isolated upgrade scenarios are supported:

- Upgrade only Oracle Identity Manager (OIM)
- Upgrade only Oracle Access Manager (OAM)
- Upgrade only Oracle Unified Directory (OUD)
- Upgrade only Oracle HTTP Server (OHS)

## Instructions for Performing Isolated Upgrade

To perform isolated upgrade, complete the following steps:

1. Complete the following prerequisites:
  - a. Review the system requirements and certification document and make sure that your existing environment meets all hardware and software requirements necessary for 11g Release 2 (11.1.2.3.0) software. For more information, see [Section 6.2, "Reviewing System Requirements and Certifications"](#).
  - b. On `IDMHOST`, ensure that the `/etc/hosts` file contains both canonical hostnames (fully qualified host names) along with the hostname entry. For more information, see ["Section 6.5, "Verifying Hostnames in the Hosts File"](#).
2. Obtain the file `idmUpgrade.zip` that contains the upgrade scripts. Copy the zip file to any accessible location on `IDMHOST` and extract the contents of the zip file. For more information about obtaining the zip file, and extracting the contents, see [Section 6.6, "Obtaining the Automated Upgrade Tool"](#).

---

---

**Note:** The instructions for performing an automated upgrade of Oracle Identity and Access Management to 11g Release 2 (11.1.2.3.0) assume you have applied the Oracle Identity and Access Management Automated Upgrade Tool Bundle Patch 2 (11.1.2.3.2). To download this patch, go to the following URL:

<https://updates.oracle.com/download/21419345.html>

---

---

3. Set the required environment variables depending on the platform on which you are upgrading Oracle Unified Directory. For more information, see [Section 6.4, "Setting the Required Environment Variables Necessary for Upgrade"](#).
4. Update the `upgrade.properties` file located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties` on `IDMHOST` with the values for the required parameters depending on the component that you wish to upgrade.  
  
For information about updating the `upgrade.properties` file, and for the descriptions of these parameters, see [Section 6.7, "Updating the upgrade.properties File"](#).
5. Perform the pre-validation checks using the `preValidate.pl` script for the component that you wish to upgrade.
  - If you are upgrading only Oracle Identity Manager, run the `preValidate.pl` script for performing pre-validation checks for Oracle Identity Manager on `IDMHOST`, by specifying `OIM` for the argument `-node`.
  - If you are upgrading only Oracle Access Manager, run the `preValidate.pl` script for performing pre-validation checks for Oracle Access Manager on `IDMHOST`, by specifying `OAM` for the argument `-node`.
  - If you are upgrading only Oracle Unified Directory, run the `preValidate.pl` script for performing pre-validation checks for Oracle Unified Directory on `IDMHOST`, by specifying `DIRECTORY` for the argument `-node`.
  - If you are upgrading only Oracle HTTP Server, run the `preValidate.pl` script for performing pre-validation checks for Oracle HTTP Server on `IDMHOST`, by specifying `WEBTIER` for the argument `-node`.

---

**Note:** Before you perform the pre-validation checks for Oracle Unified Directory, copy the files `libnzn11.so` and `libclntsh.so.11.1` to the folder `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/lib` on LDAPHOST from one of the following locations:

- `IAD_WL_HOME/server/adr`
- `IGD_WL_HOME/server/adr`
- `Web_Tier_ORACLE_HOME/lib`

`IAD_WL_HOME` refers to the **IAMAccessDomain** and `IGD_WL_HOME` refers to the **IAMGovernanceDomain**.

After you copy the files, you can perform the pre-validation checks for Oracle Unified Directory.

---

For general syntax of the `preValidate.pl` script and for information about running the script, see [Section 6.8, "Performing Pre-Validation Checks Using preValidate.pl Script"](#).

6. If you are upgrading only Oracle Identity Manager on platforms such as Solaris, IBM AIX, and HP Itanium using the automated upgrade tool, you must create the Oracle BI Publisher (BIPLATFORM) schema manually using the Repository Creation Utility (RCU) 11.1.2.3.0 from the machine that is running Linux or Windows operating system.

For more information about creating schema using RCU, see [Section 6.9, "Creating BIP Schema for Oracle Identity Manager Upgrade on Solaris, IBM AIX, and HP Itanium Platforms"](#).

---

**Note:** If you are upgrading Oracle Identity Manager on Linux, skip this step, as the automated upgrade tool creates the BIPLATFORM schema on Linux.

---

7. Stop the following servers on IDMHOST.
  - a. Oracle HTTP Server.
  - b. Oracle Access Manager Managed Server(s)
  - c. Oracle Identity Manager Managed Server(s)
  - d. Oracle SOA Suite Managed Server(s)
  - e. WebLogic Administration Server.
  - f. Oracle Unified Directory

To stop all of the servers on a host, run the following command script from the location `SHARED_CONFIG_DIR/config/scripts`:

```
./stopall.sh
```

8. Backup your Database schemas and the WebLogic domain. For more information, see [Section 6.3, "Backing up the Existing Environment"](#).
9. Upgrade the binaries and configurations of the component that you wish to upgrade, using the `idmUpgrade.pl` script.

- If you are upgrading only Oracle Unified Directory, run the `idmUpgrade.pl` script by for upgrading the binaries and configurations of Oracle Unified Directory, by specifying `DIRECTORY` for the argument `-node` and both for the argument `-mode`.

---

**Note:** Before you upgrade the binaries and configuration of Oracle Unified Directory (OUD), ensure that you have stopped the Oracle Identity Manager and Oracle Access Manager Managed Servers.

---

- If you are upgrading only Oracle Access Manager, run the `idmUpgrade.pl` script by for upgrading the binaries and configurations of Oracle Access Manager, by specifying `OAM` for the argument `-node` and both for the argument `-mode`.
- If you are upgrading only Oracle Identity Manager, run the `idmUpgrade.pl` script by for upgrading the binaries and configurations of Oracle Identity Manager, by specifying `OIM` for the argument `-node` and both for the argument `-mode`.

---

**Note:** Before you upgrade the binaries and configuration of Oracle Identity Manager, ensure that you have stopped the Oracle Access Manager Managed Server(s).

---

- If you are upgrading only Oracle HTTP Server, run the `idmUpgrade.pl` script by for upgrading the binaries and configurations of Oracle HTTP Server, by specifying `WEBTIER` for the argument `-node` and both for the argument `-mode`.
10. Perform the post-validation checks using the `postValidate.pl` script for the component that you wish to upgrade.
    - If you are upgrading only Oracle Identity Manager, run the `postValidate.pl` script for performing post-validation checks for Oracle Identity Manager on `IDMHOST`, by specifying `OIM` for the argument `-node`.
    - If you are upgrading only Oracle Access Manager, run the `postValidate.pl` script for performing post-validation checks for Oracle Access Manager on `IDMHOST`, by specifying `OAM` for the argument `-node`.
    - If you are upgrading only Oracle Unified Directory, run the `postValidate.pl` script for performing post-validation checks for Oracle Unified Directory on `IDMHOST`, by specifying `DIRECTORY` for the argument `-node`.
    - If you are upgrading only Oracle HTTP Server, run the `postValidate.pl` script for performing post-validation checks for Oracle HTTP Server on `IDMHOST`, by specifying `WEBTIER` for the argument `-node`.

For general syntax of the `postValidate.pl` script and for information about running the script, see [Section 6.11, "Performing Post-Validation Checks Using `postValidate.pl` Script"](#).

11. Perform the necessary post-upgrade tasks described in [Section 6.13, "Post-Upgrade Tasks"](#) depending on the component you upgraded.
12. Verify the upgrade by checking the log files on `IDMHOST`. Log files are created at the location you specified for `LOG_DIR` parameter in the `upgrade.properties` file.

## 4.7 Troubleshooting

For any issues that you may encounter during the upgrade process, refer to [Section 6.14, "Troubleshooting"](#) for workaround.

For the list of known issues related to automated upgrade and their workaround, see "Upgrade and Migration Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes for Identity Management*.



---

---

# Upgrading Oracle Identity and Access Management Highly Available Environments Deployed Using Life Cycle Management (LCM) Tools

This chapter describes how to upgrade Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) highly available (HA) environments that are deployed using the Life Cycle Management (LCM) Tools, to 11g Release 2 (11.1.2.3.0) using the automated upgrade procedure.

If you wish to upgrade Oracle Identity and Access Management 11g Release 2 (11.1.2.2.0) environments that are deployed using the Life Cycle Management (LCM) Tools on a single node, see [Chapter 4, "Upgrading Oracle Identity and Access Management Environments Deployed Using Life Cycle Management \(LCM\) Tools on a Single Node"](#).

---

---

**Note:** The upgrade procedure described in this chapter cannot be used to upgrade the Oracle Identity and Access Management environments that are configured manually, using the Oracle Universal Installer and Fusion Middleware Configuration wizard.

For information about upgrading Oracle Identity and Access Management environments that configured manually, see [Chapter 1, "Introduction to Oracle Identity and Access Management Upgrade"](#).

---

---

Before you proceed, review the automated upgrade overview, deployment topologies supported for automated upgrade, and the supported starting points described in [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

**Note:** For information about any latest patches, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Release Notes for Identity Management*.

---

---

This chapter includes the following sections:

- [Section 5.1, "Variables Used in This Chapter"](#)
- [Section 5.2, "Upgrade Scenario Covered in this Chapter"](#)
- [Section 5.3, "Upgrading Oracle Identity Manager \(OIM\) Only on Multiple Nodes"](#)

- [Section 5.4, "Upgrading Oracle Access Manager Suite \(OAM\) Only on Multiple Nodes"](#)
- [Section 5.5, "Upgrading OIM-OAM Integrated with Oracle Unified Directory \(OUD\) Topology on a Highly Available \(HA\) setup"](#)
- [Section 5.6, "Troubleshooting"](#)

## 5.1 Variables Used in This Chapter

Table 5–1 lists the variables used in this chapter.

**Table 5–1 Variables Used in This Chapter With Their Descriptions**

Variable	Description
<code>SCRIPT_FILE_LOCATION</code>	This is the location where you copied the upgrade tool <code>idmUpgrade.zip</code> , and extracted the files.
<code>OAMHOST1</code> <code>OAMHOST2</code>	This is the host on which Oracle Access Manager is configured.
<code>OIMHOST1</code> <code>OIMHOST2</code>	This is the host on which Oracle Identity Manager is configured.
<code>LDAPHOST1</code> <code>LDAPHOST2</code>	This is the host on which Oracle Unified Directory is configured.
<code>WEBHOST1</code> <code>WEBHOST2</code>	This is the host on which Oracle HTTP Server is configured.

## 5.2 Upgrade Scenario Covered in this Chapter

This chapter describes how to upgrade the following Oracle Identity and Access Management topologies deployed using the Life Cycle Management (LCM) Tools:

- **Oracle Identity Manager (OIM) Only Topology on a Highly Available (HA) Setup**  
For information about upgrading Oracle Identity Manager (OIM) Only topology on a highly available (HA) setup, see [Section 5.3, "Upgrading Oracle Identity Manager \(OIM\) Only on Multiple Nodes"](#).
- **Oracle Access Manager (OAM) Suite Only Topology on a Highly Available (HA) Setup**  
For information about upgrading Oracle Access Manager (OAM) Suite Only topology on a highly available (HA) setup, see [Section 5.4, "Upgrading Oracle Access Manager Suite \(OAM\) Only on Multiple Nodes"](#).
- **OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Highly Available (HA) Setup**  
For information about upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) topology on a highly available (HA) setup, see [Section 5.5, "Upgrading OIM-OAM Integrated with Oracle Unified Directory \(OUD\) Topology on a Highly Available \(HA\) setup"](#).

---

**Note:** Isolated upgrade is not supported for OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a highly available (HA) setup. For information about isolated upgrade, [Section 2.3, "Isolated Upgrade Overview"](#).

For the list of scenarios supported for automated upgrade, see [Section 2.2, "Deployment Topologies Supported for Automated Upgrade"](#).

---

## 5.3 Upgrading Oracle Identity Manager (OIM) Only on Multiple Nodes

This section describes how to upgrade Oracle Identity Manager only 11g Release 2 (11.1.2.2.0) highly available environments to 11.1.2.3.0. As part of the Oracle Identity Manager upgrade, Oracle BI Publisher will be installed and configured with Oracle Identity Manager. Therefore, after upgrading to Oracle Identity Manager 11.1.2.3.0, you do not have to use an external standalone Oracle BI Publisher to publish reports.

To upgrade Oracle Identity Manager highly available environments, perform the following tasks:

1. [Completing the Prerequisites](#)
2. [Obtaining the Software](#)
3. [Setting the Environment Variables](#)
4. [Updating the Properties File](#)
5. [Performing Pre-Validation Checks on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2](#)
6. [Creating BIP Schema for OIM Upgrade \(Only on Solaris, IBM AIX, and HP Itanium Platforms\)](#)
7. [Stopping All Servers](#)
8. [Backing Up Database and WebLogic Domain](#)
9. [Upgrading Binaries and Configuration on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2](#)
10. [Performing Post-Validation Checks on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2](#)
11. [Verifying the Upgrade](#)

### 5.3.1 Completing the Prerequisites

Before you start with the upgrade process, you must complete the following prerequisites:

1. Review the system requirements and certification document and make sure that your existing environment meets all hardware and software requirements necessary for 11g Release 2 (11.1.2.3.0) software. For more information, see [Section 6.2, "Reviewing System Requirements and Certifications"](#).
2. On OIMHOST1 and OIMHOST2, ensure that the `/etc/hosts` file contains both canonical hostnames (fully qualified host names) along with the hostname entry. For more information, see [Section 6.5, "Verifying Hostnames in the Hosts File"](#).
3. If you are using the following RAC datasources, then make they are enabled before you start the upgrade:

- ApplicationDB
- soaOIMLookupDB
- opss-dbds
- bip\_datasource

To enable the RAC databases, see *Converting Single-Instance Oracle Databases to Oracle RAC and Oracle RAC One Node in the Real Application Clusters Administration and Deployment Guide*.

## 5.3.2 Obtaining the Software

Obtain the file `idmUpgrade.zip` that contains the upgrade scripts. Copy the script to `OIMHOST1`, `OIMHOST2`, `WEBHOST1`, and `WEBHOST2`. Extract the contents of the zip file on all of the hosts. For more information about obtaining the zip file, and extracting the contents, see [Section 6.6, "Obtaining the Automated Upgrade Tool"](#).

---

---

**Note:** The instructions for performing an automated upgrade of Oracle Identity and Access Management to 11g Release 2 (11.1.2.3.0) assume you have applied the Oracle Identity and Access Management Automated Upgrade Tool Bundle Patch 2 (11.1.2.3.2). To download this patch, go to the following URL:

<https://updates.oracle.com/download/21419345.html>

---

---

## 5.3.3 Setting the Environment Variables

Before you start with the upgrade process, you must set the required environment variables depending on the platform on which you are upgrading Oracle Identity and Access Management. For more information, see [Section 6.4, "Setting the Required Environment Variables Necessary for Upgrade"](#).

## 5.3.4 Updating the Properties File

You must update the `upgrade.properties` file located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties` on `OIMHOST1` and `OIMHOST2` with the values for the required properties.

For information about the properties that you must update for upgrading Oracle Identity Manager (OIM) Only topology on multiple nodes, see [Section 6.7, "Updating the upgrade.properties File"](#).

## 5.3.5 Performing Pre-Validation Checks on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2

After you update the properties file, you must perform pre-validation checks on `OIMHOST1`, `OIMHOST2`, `WEBHOST1`, and `WEBHOST2`. To perform the pre-validation checks, you must run the `preValidate.pl` script.

To perform the pre-validation checks, do the following:

- On `OIMHOST1`, run the `preValidate.pl` script to perform pre-validation checks. While running the command, specify `OIM` as the value for `-node` argument.
- On `OIMHOST2`, run the `preValidate.pl` script to perform pre-validation checks. While running the command, specify `OIM` as the value for `-node` argument.

- On `WEBHOST1`, run the `preValidate.pl` script to perform pre-validation checks. While running the command, specify `WEBTIER` as the value for `-node` argument.
- On `WEBHOST2`, run the `preValidate.pl` script to perform pre-validation checks. While running the command, specify `WEBTIER` as the value for `-node` argument.

For general syntax of the `preValidate.pl` script and for information about running the script, see [Section 6.8, "Performing Pre-Validation Checks Using `preValidate.pl` Script"](#).

### 5.3.6 Creating BIP Schema for OIM Upgrade (Only on Solaris, IBM AIX, and HP Itanium Platforms)

If you are upgrading Oracle Identity Manager on platforms such as Solaris, IBM AIX, and HP Itanium using the automated upgrade tool, you must create the Oracle BI Publisher (BIPLATFORM) schema manually using the Repository Creation Utility (RCU) 11.1.2.3.0 from the machine that is running Linux or Windows operating system.

For more information about creating schema using RCU, see [Section 6.9, "Creating BIP Schema for Oracle Identity Manager Upgrade on Solaris, IBM AIX, and HP Itanium Platforms"](#).

---



---

**Note:** If you are upgrading Oracle Identity Manager on Linux, skip this step, as the automated upgrade tool creates the BIPLATFORM schema on Linux.

---



---

### 5.3.7 Stopping All Servers

You must stop the following server(s):

1. Oracle HTTP Server on `WEBHOST2`.
2. Oracle HTTP Server on `WEBHOST1`.
3. Oracle Identity Manager Managed Server(s) on `OIMHOST2`.
4. Oracle SOA Suite Managed Server(s) on `OIMHOST2`.
5. Oracle Identity Manager Managed Server(s) on `OIMHOST1`.
6. Oracle SOA Suite Managed Server(s) on `OIMHOST1`.
7. WebLogic Administration Server on `OIMHOST1`.

To stop all servers on a host, you must run `stopall.sh` script on that host.

Complete the following steps to stop all of the servers:

1. On `WEBHOST2`, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:
 

```
./stopall.sh
```
2. On `WEBHOST1`, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:
 

```
./stopall.sh
```
3. On `OIMHOST2`, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:
 

```
./stopall.sh
```

4. On OIMHOST1, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:  

```
./stopall.sh
```

For more information about running the `stopall.sh` script to stop the servers, see [Section 6.12, "Stopping All Servers Using stopall.sh Script"](#).

### 5.3.8 Backing Up Database and WebLogic Domain

Before you run the upgrade script, you must backup your Database schemas and the WebLogic domain(s). For more information, see [Section 6.3, "Backing up the Existing Environment"](#).

### 5.3.9 Upgrading Binaries and Configuration on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2

You must upgrade binaries and configuration on OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2 by running the `idmUpgrade.pl` script.

The `idmUpgrade.pl` script must be used for upgrading both binaries and configuration. The argument `-mode` represents the type of upgrade. You must perform binary upgrade on each of the nodes followed by the configuration upgrade.

---

---

**Note:** Make sure that the Database services are up and running before you run the upgrade script.

If you do not specify any value for the argument `-mode`, the value will be taken as `both`, which is the default value of the `-mode` argument. In this case, the script performs the binary upgrade first followed by the configuration upgrade. For more information about running the `idmUpgrade.pl` command, see [Section 6.10, "Upgrading Oracle Identity and Access Management Binaries and Configuration Using idmUpgrade.pl script"](#).

If you have shared binaries, you must perform binary upgrade on one node only. For example, if Oracle Identity Manager binaries are shared between OIMHOST1 and OIMHOST2, you can perform binary upgrade on either of these hosts. Binary upgrade on both the hosts is not required.

---

---

To upgrade binaries and configuration, complete the following tasks:

1. On OIMHOST1, run `idmUpgrade.pl` script to upgrade binaries. While running this command, specify `binary` as the value for the `-mode` argument, and `OIM` as the value for the `-node` argument.
2. On OIMHOST2, run `idmUpgrade.pl` script to upgrade binaries. While running this command, specify `binary` as the value for the `-mode` argument, and `OIM` as the value for the `-node` argument.

This step is required only if binaries are not shared between OIMHOST1 and OIMHOST2.

3. On WEBHOST1, run `idmUpgrade.pl` script to upgrade binaries. While running this command, specify `binary` as the value for the `-mode` argument, and `WEBTIER` as the value for the `-node` argument.

4. On `WEBHOST2`, run `idmUpgrade.pl` script to upgrade binaries. While running this command, specify `binary` as the value for the `-mode` argument, and `WEBTIER` as the value for the `-node` argument.

This step is required only if binaries are not shared between `WEBHOST1` and `WEBHOST2`.

5. On `OIMHOST1`, run `idmUpgrade.pl` script to upgrade configuration. While running this command, specify `config` as the value for the `-mode` argument, and `OIM` as the value for the `-node` argument.
6. On `OIMHOST2`, run `idmUpgrade.pl` script to upgrade configuration. While running this command, specify `config` as the value for the `-mode` argument, and `OIM` as the value for the `-node` argument.
7. On `WEBHOST1`, run `idmUpgrade.pl` script to upgrade configuration. While running this command, specify `config` as the value for the `-mode` argument, and `WEBTIER` as the value for the `-node` argument.
8. On `WEBHOST2`, run `idmUpgrade.pl` script to upgrade configuration. While running this command, specify `config` as the value for the `-mode` argument, and `WEBTIER` as the value for the `-node` argument.

For general syntax of the `idmUpgrade.pl` script and for information about running the script, see [Section 6.10, "Upgrading Oracle Identity and Access Management Binaries and Configuration Using `idmUpgrade.pl` script"](#).

### 5.3.10 Performing Post-Validation Checks on `OIMHOST1`, `OIMHOST2`, `WEBHOST1`, and `WEBHOST2`

After you upgrade binaries and configuration, you must perform post-validation checks on `OIMHOST1`, `OIMHOST2`, `WEBHOST1`, and `WEBHOST2`. To perform the post-validation checks, you must run the `postValidate.pl` script.

To perform the post-validation checks, do the following:

- On `OIMHOST1`, run the `postValidate.pl` script to perform post-validation checks. While running the command, specify `OIM` as the value for `-node` argument.
- On `OIMHOST2`, run the `postValidate.pl` script to perform post-validation checks. While running the command, specify `OIM` as the value for `-node` argument.
- On `WEBHOST1`, run the `postValidate.pl` script to perform post-validation checks. While running the command, specify `WEBTIER` as the value for `-node` argument.
- On `WEBHOST2`, run the `postValidate.pl` script to perform post-validation checks. While running the command, specify `WEBTIER` as the value for `-node` argument.

For general syntax of the `postValidate.pl` script and for information about running the script, see [Section 6.11, "Performing Post-Validation Checks Using `postValidate.pl` Script"](#).

### 5.3.11 Verifying the Upgrade

After you perform the post-validation checks, verify the Oracle Identity Manager upgrade by checking the log files on each of the nodes. Log files are created at the location you specified for `LOG_DIR` parameter in the `upgrade.properties` file.

## 5.4 Upgrading Oracle Access Manager Suite (OAM) Only on Multiple Nodes

This section describes how to upgrade Oracle Access Manager only 11g Release 2 (11.1.2.2.0) highly available environments to 11.1.2.3.0. If your OAM 11.1.2.2.0 domain contains Oracle Adaptive Access Manager, then the upgrade script upgrades Oracle Adaptive Access Manager to 11.1.2.3.0 along with Oracle Access Manager.

---

---

**Note:** Upgrade is supported on OAM only environment with non-embedded LDAP -OUD. Upgrading OAM only environment with embedded LDAP is NOT supported.

---

---

To upgrade Oracle Access Manager and Oracle Adaptive Access Manager on multiple nodes, perform the following tasks:

1. [Completing the Prerequisites](#)
2. [Obtaining the Software](#)
3. [Setting the Environment Variables](#)
4. [Updating the Properties File](#)
5. [Performing Pre-Validation Checks on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2](#)
6. [Stopping All Servers](#)
7. [Backing Up Database and WebLogic Domain](#)
8. [Upgrading Binaries and Configuration on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2](#)
9. [Performing Post-Validation Checks on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2](#)
10. [Verifying the Upgrade](#)

### 5.4.1 Completing the Prerequisites

Before you start with the upgrade process, you must complete the following prerequisites:

1. Review the system requirements and certification document and make sure that your existing environment meets all hardware and software requirements necessary for 11g Release 2 (11.1.2.3.0) software. For more information, see [Section 6.2, "Reviewing System Requirements and Certifications"](#).
2. On OAMHOST1 and OAMHOST2, ensure that the `/etc/hosts` file contains both canonical hostnames (fully qualified host names) along with the hostname entry. For more information, see ["Section 6.5, "Verifying Hostnames in the Hosts File"](#).

### 5.4.2 Obtaining the Software

Obtain the file `idmUpgrade.zip` that contains the upgrade scripts. Copy the script to OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2. Extract the contents of the zip file on all of the hosts. For more information about obtaining the zip file, and extracting the contents, see [Section 6.6, "Obtaining the Automated Upgrade Tool"](#).

---

---

**Note:** The instructions for performing an automated upgrade of Oracle Identity and Access Management to 11g Release 2 (11.1.2.3.0) assume you have applied the Oracle Identity and Access Management Automated Upgrade Tool Bundle Patch 2 (11.1.2.3.2). To download this patch, go to the following URL:

<https://updates.oracle.com/download/21419345.html>

---

---

### 5.4.3 Setting the Environment Variables

Before you start with the upgrade process, you must set the required environment variables depending on the platform on which you are upgrading Oracle Identity and Access Management. For more information, see [Section 6.4, "Setting the Required Environment Variables Necessary for Upgrade"](#).

### 5.4.4 Updating the Properties File

You must update the `upgrade.properties` file located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties` on `OAMHOST1` and `OAMHOST2` with the values for the required properties.

For information about the properties that you must update for upgrading Oracle Access Manager (OAM) Only topology on multiple nodes, see [Section 6.7, "Updating the upgrade.properties File"](#).

### 5.4.5 Performing Pre-Validation Checks on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2

After you update the properties file, you must perform pre-validation checks on `OAMHOST1`, `OAMHOST2`, `WEBHOST1`, and `WEBHOST2`. To perform the pre-validation checks, you must run the `preValidate.pl` script.

To perform the pre-validation checks, do the following:

- On `OAMHOST1`, run the `preValidate.pl` script to perform pre-validation checks. While running the command, specify `OAM` as the value for `-node` argument.
- On `OAMHOST2`, run the `preValidate.pl` script to perform pre-validation checks. While running the command, specify `OAM` as the value for `-node` argument.
- On `WEBHOST1`, run the `preValidate.pl` script to perform pre-validation checks. While running the command, specify `WEBTIER` as the value for `-node` argument.
- On `WEBHOST2`, run the `preValidate.pl` script to perform pre-validation checks. While running the command, specify `WEBTIER` as the value for `-node` argument.

For general syntax of the `preValidate.pl` script and for information about running the script, see [Section 6.8, "Performing Pre-Validation Checks Using preValidate.pl Script"](#).

### 5.4.6 Stopping All Servers

You must stop the following server(s):

1. Oracle HTTP Server on `WEBHOST2`.
2. Oracle HTTP Server on `WEBHOST1`.
3. Oracle Access Manager Managed Server(s) on `OAMHOST2`.
4. Oracle Access Manager Managed Server(s) on `OAMHOST1`.

#### 5. WebLogic Administration Server on OAMHOST1.

To stop all servers on a host, you must run `stopall.sh` script on that host.

Complete the following steps to stop all of the servers:

1. On `WEBHOST2`, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:  

```
./stopall.sh
```
2. On `WEBHOST1`, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:  

```
./stopall.sh
```
3. On `OAMHOST2`, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:  

```
./stopall.sh
```
4. On `OAMHOST1`, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:  

```
./stopall.sh
```

For more information about running the `stopall.sh` script to stop the servers, see [Section 6.12, "Stopping All Servers Using stopall.sh Script"](#).

### 5.4.7 Backing Up Database and WebLogic Domain

Before you run the upgrade script, you must backup your Database schemas and the WebLogic domain(s). For more information, see [Section 6.3, "Backing up the Existing Environment"](#).

### 5.4.8 Upgrading Binaries and Configuration on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2

You must upgrade binaries and configuration on `OAMHOST1`, `OAMHOST2`, `WEBHOST1`, and `WEBHOST2` by running the `idmUpgrade.pl` script.

The `idmUpgrade.pl` script must be used for upgrading both binaries and configuration. The argument `-mode` represents the type of upgrade. You must perform binary upgrade on each of the nodes followed by the configuration upgrade.

---

---

**Note:** Make sure that the Database services are up and running before you run the upgrade script.

If you have shared binaries, you must perform binary upgrade on one node only. For example, if Oracle Identity Manager binaries are shared between `OAMHOST1` and `OAMHOST2`, you can perform binary upgrade on either of these hosts. Binary upgrade on both the hosts is not required.

---

---

To upgrade binaries and configuration, complete the following tasks:

1. On `OAMHOST1`, run `idmUpgrade.pl` script to upgrade binaries. While running this command, specify `binary` as the value for the `-mode` argument, and `OAM` as the value for the `-node` argument.

2. On OAMHOST2, run `idmUpgrade.pl` script to upgrade binaries. While running this command, specify `binary` as the value for the `-mode` argument, and `OAM` as the value for the `-node` argument.

This step is required only if binaries are not shared between OAMHOST1 and OAMHOST2.

3. On WEBHOST1, run `idmUpgrade.pl` script to upgrade binaries. While running this command, specify `binary` as the value for the `-mode` argument, and `WEBTIER` as the value for the `-node` argument.

4. On WEBHOST2, run `idmUpgrade.pl` script to upgrade binaries. While running this command, specify `binary` as the value for the `-mode` argument, and `WEBTIER` as the value for the `-node` argument.

This step is required only if binaries are not shared between WEBHOST1 and WEBHOST2.

5. On OAMHOST1, run `idmUpgrade.pl` script to upgrade configuration. While running this command, specify `config` as the value for the `-mode` argument, and `OAM` as the value for the `-node` argument.
6. On OAMHOST2, run `idmUpgrade.pl` script to upgrade configuration. While running this command, specify `config` as the value for the `-mode` argument, and `OAM` as the value for the `-node` argument.
7. On WEBHOST1, run `idmUpgrade.pl` script to upgrade configuration. While running this command, specify `config` as the value for the `-mode` argument, and `WEBTIER` as the value for the `-node` argument.
8. On WEBHOST2, run `idmUpgrade.pl` script to upgrade configuration. While running this command, specify `config` as the value for the `-mode` argument, and `WEBTIER` as the value for the `-node` argument.

For general syntax of the `idmUpgrade.pl` script and for information about running the script, see [Section 6.10, "Upgrading Oracle Identity and Access Management Binaries and Configuration Using `idmUpgrade.pl` script"](#).

### 5.4.9 Performing Post-Validation Checks on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2

After you upgrade binaries and configuration, you must perform post-validation checks on OAMHOST1, OAMHOST2, WEBHOST1, and WEBHOST2. To perform the post-validation checks, you must run the `postValidate.pl` script.

To perform the post-validation checks, do the following:

- Restart the Oracle HTTP Servers on both WEBHOST1 and WEBHOST2.
- On OAMHOST1, run the `postValidate.pl` script to perform post-validation checks. While running the command, specify `OAM` as the value for `-node` argument.
- On OAMHOST2, run the `postValidate.pl` script to perform post-validation checks. While running the command, specify `OAM` as the value for `-node` argument.
- On WEBHOST1, run the `postValidate.pl` script to perform post-validation checks. While running the command, specify `WEBTIER` as the value for `-node` argument.
- On WEBHOST2, run the `postValidate.pl` script to perform post-validation checks. While running the command, specify `WEBTIER` as the value for `-node` argument.

For general syntax of the `postValidate.pl` script and for information about running the script, see [Section 6.11, "Performing Post-Validation Checks Using `postValidate.pl` Script"](#).

### 5.4.10 Verifying the Upgrade

After you perform the post-validation checks, verify the Oracle Access Manager upgrade by checking the log files on each of the nodes. Log files are created at the location you specified for `LOG_DIR` parameter in the `upgrade.properties` file.

## 5.5 Upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) Topology on a Highly Available (HA) setup

This section describes how to upgrade OIM-OAM Integrated with Oracle Unified Directory (OUD) topology on a highly available (HA) setup deployed using LCM tool, from 11g Release 2 (11.1.2.2.0) to 11g Release 2 (11.1.2.3.0).

This topology contains the following hosts:

- `OIMHOST1` and `OIMHOST2` - These are the hosts on which Oracle Identity Manager is configured.
- `OAMHOST1` and `OAMHOST2` - These are the hosts on which Oracle Access Manager is configured.
- `LDAPHOST1` and `LDAPHOST2` - These are the hosts on which Oracle Unified Directory is configured.
- `WEBHOST1` and `WEBHOST2` - These are the hosts on which Oracle HTTP Server is configured.

As part of the Oracle Identity Manager upgrade, the embedded Oracle BI Publisher (BIP) will be installed and configured with Oracle Identity Manager. Therefore, after upgrading to Oracle Identity Manager 11.1.2.3.0, you can choose to either use the embedded BI Publisher or continue to use the standalone Oracle BI Publisher. If you choose to use the embedded BI Publisher and discontinue using the standalone BIP, then you must migrate the existing BIP reports to embedded BIP.

Oracle Access Manager 11g Release 2 (11.1.2.3.0) has a new feature called Oracle Mobile Security Suite. You can enable Oracle Mobile Security Suite post-upgrade. For an introduction to Oracle Mobile Security Suite, see "Understanding Oracle Mobile Security Suite" in *Oracle Fusion Middleware Administering Oracle Mobile Security Suite*.

To upgrade OIM-OAM Integrated with Oracle Unified Directory (OUD) topology on a highly available (HA) setup, from 11g Release 2 (11.1.2.2.0) to 11g Release 2 (11.1.2.3.0), perform the following tasks:

1. [Completing the Prerequisites](#)
2. [Obtaining the Software](#)
3. [Setting the Environment Variables](#)
4. [Updating the Properties File](#)
5. [Performing Pre-Validation Checks all of the Hosts](#)
6. [Creating BIP Schema for OIM Upgrade \(Only on Solaris, IBM AIX, and HP Itanium Platforms\)](#)
7. [Stopping All Servers](#)

8. [Backing Up Database and WebLogic Domain](#)
9. [Upgrading Binaries and Configuration on all of the Hosts](#)
10. [Performing Post-Validation Checks on all of the Hosts](#)
11. [Performing the Required Post-Upgrade Tasks](#)
12. [Verifying the Upgrade](#)

### 5.5.1 Completing the Prerequisites

Before you start with the upgrade process, you must complete the following prerequisites:

1. Review the system requirements and certification document and make sure that your existing environment meets all hardware and software requirements necessary for 11g Release 2 (11.1.2.3.0) software. For more information, see [Section 6.2, "Reviewing System Requirements and Certifications"](#).
2. On LDAPHOST1, LDAPHOST2, OAMHOST1, OAMHOST2, OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2, ensure that the `/etc/hosts` file contains both canonical hostnames (fully qualified host names) along with the hostname entry. For more information, see ["Section 6.5, "Verifying Hostnames in the Hosts File"](#).
3. Verify that the Oracle Adaptive Access Manager (OAAM) Administration Server is accessible at the following URL:

```
http://OAM_HOST:OAM_ADMIN_PORT/oaam_admin
```

Use the OAAM admin username and OAAM admin password to access the OAAM Administration Server.

For example:

```
http://identity.example.com:14200/oaam_admin
```

Username: oaamadminuser

Password: Welcome1

### 5.5.2 Obtaining the Software

Obtain the file `idmUpgrade.zip` that contains the upgrade scripts. Copy the script to any accessible location on LDAPHOST1, LDAPHOST2, OAMHOST1, OAMHOST2, OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2, and extract the contents of the zip file on all of the hosts. For more information about obtaining the zip file, and extracting the contents, see [Section 6.6, "Obtaining the Automated Upgrade Tool"](#).

---

---

**Note:** The instructions for performing an automated upgrade of Oracle Identity and Access Management to 11g Release 2 (11.1.2.3.0) assume you have applied the Oracle Identity and Access Management Automated Upgrade Tool Bundle Patch 2 (11.1.2.3.2). To download this patch, go to the following URL:

```
https://updates.oracle.com/download/21419345.html
```

---

---

### 5.5.3 Setting the Environment Variables

Before you start with the upgrade process, you must set the required environment variables depending on the platform on which you are upgrading Oracle Identity and

Access Management. For more information, see [Section 6.4, "Setting the Required Environment Variables Necessary for Upgrade"](#).

## 5.5.4 Updating the Properties File

You must update the `upgrade.properties` file located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties` on `LDAPHOST1`, `LDAPHOST2`, `OAMHOST1`, `OAMHOST2`, `OIMHOST1`, `OIMHOST2`, `WEBHOST1` and `WEBHOST2`, with the values for the required properties.

For information about the properties that you must update for upgrading OIM-OAM Integrated with Oracle Unified Directory (OUD) topology, see [Section 6.7, "Updating the upgrade.properties File"](#).

## 5.5.5 Performing Pre-Validation Checks all of the Hosts

After you update the properties file, you must perform the pre-validation checks on `WEBHOST1`, `WEBHOST2`, `LDAPHOST1`, `LDAPHOST2`, `OAMHOST1`, `OAMHOST2`, `OIMHOST1`, and `OIMHOST2`. To perform the pre-validation checks, you must run the `preValidate.pl` script.

---

---

**Note:** If `LDAPHOST1` and `LDAPHOST2` have only Oracle Unified Directory installed on them, that is, if `LDAPHOST1` and `LDAPHOST2` do not have Oracle Identity Manager or Oracle Access Manager installed, then you must do the following:

Copy the files `libnntz11.so` and `libclntsh.so.11.1` from either `OAMHOST`, or `OIMHOST`, or `WEBHOST` to the location `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/lib/` on both `LDAPHOST1` and `LDAPHOST2`.

The following are the locations of the files `libnntz11.so` and `libclntsh.so.11.1` on `OAMHOST`, `OIMHOST`, and `WEBHOST`:

- On `OAMHOST`, the files are located at `IDMTOP/products/access/wlserver_10.3/server/adr`.
  - On `OIMHOST`, the files are located at `IDMTOP/products/identity/wlserver_10.3/server/adr`.
  - On `WEBHOST`, the files are located at `IDMTOP/products/web/ohs/lib`.
- 
- 

To perform the pre-validation checks, do the following:

- On `WEBHOST1`, run the `preValidate.pl` script to perform pre-validation checks for Oracle HTTP Server, by specifying `WEBTIER` for the argument `-node`.
- On `WEBHOST2`, run the `preValidate.pl` script to perform pre-validation checks for Oracle HTTP Server, by specifying `WEBTIER` for the argument `-node`.
- On `LDAPHOST1`, run the `preValidate.pl` script to perform pre-validation checks for Oracle Unified Directory, by specifying `DIRECTORY` for argument `-node`.
- On `LDAPHOST2`, run the `preValidate.pl` script to perform pre-validation checks for Oracle Unified Directory by specifying `DIRECTORY` for the argument `-node`.
- On `OIMHOST1`, run the `preValidate.pl` script to perform pre-validation checks for Oracle Identity Manager, by specifying `OIM` for the argument `-node`.

- On OIMHOST2, run the `preValidate.pl` script to perform pre-validation checks for Oracle Identity Manager, by specifying `OIM` for the argument `-node`.
- On OAMHOST1, run the `preValidate.pl` script to perform pre-validation checks for Oracle Access Manager, by specifying `OAM` for the argument `-node`.
- On OAMHOST2, run the `preValidate.pl` script to perform pre-validation checks for Oracle Access Manager, by specifying `OAM` for the argument `-node`.

For general syntax of the `preValidate.pl` script and for information about running the script, see [Section 6.8, "Performing Pre-Validation Checks Using `preValidate.pl` Script"](#).

## 5.5.6 Creating BIP Schema for OIM Upgrade (Only on Solaris, IBM AIX, and HP Itanium Platforms)

If you are upgrading Oracle Identity Manager on platforms such as Solaris, IBM AIX, and HP Itanium using the automated upgrade tool, you must create the Oracle BI Publisher (BIPLATFORM) schema manually using the Repository Creation Utility (RCU) 11.1.2.3.0 from the machine that is running Linux or Windows operating system.

For more information about creating schema using RCU, see [Section 6.9, "Creating BIP Schema for Oracle Identity Manager Upgrade on Solaris, IBM AIX, and HP Itanium Platforms"](#).

---



---

**Note:** If you are upgrading Oracle Identity Manager on Linux, skip this step, as the automated upgrade tool creates the BIPLATFORM schema on Linux.

---



---

## 5.5.7 Stopping All Servers

You must stop the following server(s):

1. Oracle HTTP Server on WEBHOST1 and WEBHOST2.
2. Oracle Access Manager Managed Server(s) on OAMHOST1 and OAMHOST2.
3. Oracle Identity Manager Managed Server(s) on OIMHOST1 and OIMHOST2.
4. Oracle SOA Suite Managed Server(s) on OIMHOST1 and OIMHOST2.
5. WebLogic Administration Server(s).
6. Oracle Unified Directory on LDAPHOST1 and LDAPHOST2.

To stop all the servers on a host, you must run `stopall.sh` script on that host.

Complete the following steps to stop the servers:

1. On WEBHOST2, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:
 

```
./stopall.sh
```
2. On WEBHOST1, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:
 

```
./stopall.sh
```
3. On OAMHOST2, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:
 

```
./stopall.sh
```

4. On OAMHOST1, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:  

```
./stopall.sh
```
5. On OIMHOST2, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:  

```
./stopall.sh
```
6. On OIMHOST1, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:  

```
./stopall.sh
```
7. On LDAPHOST2, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:  

```
./stopall.sh
```
8. On LDAPHOST1, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:  

```
./stopall.sh
```

For more information about running the `stopall.sh` script to stop the servers, see [Section 6.12, "Stopping All Servers Using stopall.sh Script"](#).

## 5.5.8 Backing Up Database and WebLogic Domain

Before you run the upgrade script, you must backup your Database schemas and the file system. For more information, see [Section 6.3, "Backing up the Existing Environment"](#).

## 5.5.9 Upgrading Binaries and Configuration on all of the Hosts

After you back up your existing environment, upgrade the binaries and configuration of Oracle HTTP Server, Oracle Unified Directory, Oracle Identity Manager, and Oracle Access Manager. To do this, you must run the `idmUpgrade.pl` script on `WEBHOST1`, `WEBHOST2`, `LDAPHOST1`, `LDAPHOST2`, `OIMHOST1`, `OIMHOST2`, `OAMHOST1`, and `OAMHOST2`.

The `idmUpgrade.pl` script must be used for upgrading both binaries and configuration. The argument `-mode` represents the type of upgrade. You must perform binary upgrade on each of the nodes followed by the configuration upgrade.

---

---

**Note:** Make sure that the Database services are up and running before you run the upgrade script.

If you have shared binaries, you must perform binary upgrade on one node only. For example, if Oracle Identity Manager binaries are shared between `OIMHOST1` and `OIMHOST2`, you can perform binary upgrade on either of these hosts. Binary upgrade on both the hosts is not required.

---

---

To upgrade binaries and configuration, complete the following tasks in the same order specified:

1. On `WEBHOST1`, run the `idmUpgrade.pl` script to upgrade the binaries of Oracle HTTP Server, by specifying `binary` for the argument `-mode`, and `WEBTIER` for the argument `-node`.

2. On WEBHOST2, run the `idmUpgrade.pl` script to upgrade the binaries of Oracle HTTP Server, by specifying `binary` for the argument `-mode`, and `WEBTIER` for the argument `-node`.

This step is required only if binaries are not shared between WEBHOST1 and WEBHOST2.

3. On LDAPHOST1, run the `idmUpgrade.pl` script to upgrade the binaries of Oracle Unified Directory, by specifying `binary` for the argument `-mode`, and `DIRECTORY` for the argument `-node`.

4. On LDAPHOST2, run the `idmUpgrade.pl` script to upgrade the binaries of Oracle Unified Directory, by specifying `binary` for the argument `-mode`, and `DIRECTORY` for the argument `-node`.

This step is required only if binaries are not shared between LDAPHOST1 and LDAPHOST2.

5. On OAMHOST1, run the `idmUpgrade.pl` script to upgrade the binaries of Oracle Access Manager, by specifying `binary` for the argument `-mode`, and `OAM` for the argument `-node`.

6. On OAMHOST2, run the `idmUpgrade.pl` script to upgrade the binaries of Oracle Access Manager, by specifying `binary` for the argument `-mode`, and `OAM` for the argument `-node`.

This step is required only if binaries are not shared between OAMHOST1 and OAMHOST2.

7. On OIMHOST1, run the `idmUpgrade.pl` script to upgrade the binaries of Oracle Identity Manager, by specifying `binary` for the argument `-mode`, and `OIM` for the argument `-node`.

8. On OIMHOST2, run the `idmUpgrade.pl` script to upgrade the binaries of Oracle Identity Manager, by specifying `binary` for the argument `-mode`, and `OIM` for the argument `-node`.

This step is required only if binaries are not shared between OIMHOST1 and OIMHOST2.

9. On WEBHOST1, run the `idmUpgrade.pl` script to upgrade the configuration of Oracle HTTP Server, by specifying `config` for the argument `-mode`, and `WEBTIER` for the argument `-node`.

10. On WEBHOST2, run the `idmUpgrade.pl` script to upgrade the configuration of Oracle HTTP Server, by specifying `config` for the argument `-mode`, and `WEBTIER` for the argument `-node`.

11. On LDAPHOST1, run the `idmUpgrade.pl` script to upgrade the configuration of Oracle Unified Directory, by specifying `config` for the argument `-mode`, and `DIRECTORY` for the argument `-node`.

12. On LDAPHOST2, run the `idmUpgrade.pl` script to upgrade the configuration of Oracle Unified Directory, by specifying `config` for the argument `-mode`, and `DIRECTORY` for the argument `-node`.

13. On OAMHOST1, run the `idmUpgrade.pl` script to upgrade the configuration of Oracle Access Manager, by specifying `config` for the argument `-mode`, and `OAM` for the argument `-node`.

14. On OAMHOST2, run the `idmUpgrade.pl` script to upgrade the configuration of Oracle Access Manager, by specifying `config` for the argument `-mode`, and `OAM` for the argument `-node`.

15. On OIMHOST1, run the `idmUpgrade.pl` script to upgrade the configuration of Oracle Identity Manager, by specifying `config` for the argument `-mode`, and `OIM` for the argument `-node`.
16. On OIMHOST2, run the `idmUpgrade.pl` script to upgrade the configuration of Oracle Identity Manager, by specifying `config` for the argument `-mode`, and `OIM` for the argument `-node`.

For general syntax of the `idmUpgrade.pl` script and for information about running the script, see [Section 6.10, "Upgrading Oracle Identity and Access Management Binaries and Configuration Using `idmUpgrade.pl` script"](#).

### 5.5.10 Performing Post-Validation Checks on all of the Hosts

After you upgrade binaries and configuration, you must perform post-validation checks on LDAPHOST1, LDAPHOST2, OAMHOST1, OAMHOST2, OIMHOST1, OIMHOST2, WEBHOST1, and WEBHOST2. To perform the post-validation checks, you must run the `postValidate.pl` script.

To perform the post-validation checks, do the following:

- On LDAPHOST1, run the `postValidate.pl` script to perform post-validation checks for Oracle Unified Directory, by specifying `DIRECTORY` for the argument `-node`.
- On LDAPHOST2, run the `postValidate.pl` script to perform post-validation checks for Oracle Unified Directory, by specifying `DIRECTORY` for the argument `-node`.
- On OAMHOST1, run the `postValidate.pl` script to perform post-validation checks for Oracle Access Manager, by specifying `OAM` for the argument `-node`.
- On OAMHOST2, run the `postValidate.pl` script to perform post-validation checks for Oracle Access Manager, by specifying `OAM` for the argument `-node`.
- On OIMHOST1, run the `postValidate.pl` script to perform post-validation checks for Oracle Identity Manager, by specifying `OIM` for the argument `-node`.
- On OIMHOST2, run the `postValidate.pl` script to perform post-validation checks for Oracle Identity Manager, by specifying `OIM` for the argument `-node`.
- On WEBHOST1, run the `postValidate.pl` script to perform post-validation checks for Oracle HTTP Server, by specifying `WEBTIER` for the argument `-node`.
- On WEBHOST2, run the `postValidate.pl` script to perform post-validation checks for Oracle HTTP Server, by specifying `WEBTIER` for the argument `-node`.

For general syntax of the `postValidate.pl` script and for information about running the script, see [Section 6.11, "Performing Post-Validation Checks Using `postValidate.pl` Script"](#).

### 5.5.11 Performing the Required Post-Upgrade Tasks

This section lists the post-upgrade tasks required for some of the features to work post-upgrade. Perform the post-upgrade tasks based on your requirement.

This section includes the following topics:

- [Upgrading Oracle Access Management Identity Federation and Oracle Access Management Security Token Service](#)
- [Upgrading Server Keystore Certificate if you have Configured Oracle Adaptive Access Manager](#)
- [Configuring Reverse Proxy Settings](#)

- [Adding the JAVA System Property if you have Configured OAAM](#)

### 5.5.11.1 Upgrading Oracle Access Management Identity Federation and Oracle Access Management Security Token Service

Oracle Access Management Identity Federation and Oracle Access Management Security Token Service are the services provided by the Oracle Access Management suite. The automated upgrade utility does not handle the upgrade of Oracle Access Management Identity Federation and Oracle Access Management Security Token Service. Therefore, you must manually upgrade Oracle Access Management Identity Federation and Oracle Access Management Security Token Service to 11g Release 2 (11.1.2.3.0) on OAMHOST1 and OAMHOST2. For more information, see Section 6.14.1, "Upgrading Oracle Access Management Identity Federation and Oracle Access Management Security Token Service to 11.1.2.3.0".

### 5.5.11.2 Upgrading Server Keystore Certificate if you have Configured Oracle Adaptive Access Manager

If you have Oracle Adaptive Access Manager configured in your setup, you must upgrade the server keystore certificate by running the WLST command `upgradeServerKeystoreCertificate()` on OAMHOST1 and OAMHOST2. For more information, see Section 6.14.3, "Upgrading Server Keystore Certificates".

### 5.5.11.3 Configuring Reverse Proxy Settings

You must configure the reverse proxy settings post-upgrade, for Oracle HTTP Server to front end BI Publisher (BIP). This can be done by protecting the following URLs by adding the required parameters in the respective files located at `WEB_ORACLE_INSTANCE/config/OHS/component_name/moduleconf/` on WEBHOST1 and WEBHOST2:

- Add the required parameters in the `oimadmin_vh.conf` file for OIM to protect the URL `/xmlpservlet`.
- Add the required parameters in the `idmadmin_vh.conf` file for OAM to protect the URL `/access`.

For more information about configuring reverse proxy settings, see Section 6.14.2, "Configuring Reverse Proxy Settings to Front End Oracle Mobile Security Suite and BI Publisher".

### 5.5.11.4 Adding the JAVA System Property if you have Configured OAAM

If you have configured Oracle Adaptive Access Manager in OIM-OAM Integrated with Oracle Unified Directory (OUD) topology, you must add the JAVA system property `-Djava.security.auth.login.config` to the `setDomainEnv.sh` script located in the `IAMAccessDomain`. For more information, see [Section 6.13.1, "Adding the Java System Property for Oracle Adaptive Access Manager"](#).

## 5.5.12 Verifying the Upgrade

After you perform the post-validation checks, verify the upgraded environment by checking the log files on each of the nodes. Log files are created at the location you specified for `LOG_DIR` parameter in the `upgrade.properties` file.

## 5.6 Troubleshooting

For any issues that you may encounter during the upgrade process, refer to [Section 6.14, "Troubleshooting"](#) for workaround.

For the list of known issues related to automated upgrade and their workaround, see "Upgrade and Migration Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes for Identity Management*.

---

---

# Tasks Common to Various Automated Upgrade Scenarios

This chapter lists the upgrade tasks that need to be performed as part of the automated upgrade process.

---

---

**Note:** This chapter contains the upgrade tasks that are common to different automated upgrade scenarios. Do not perform all of the tasks described in this chapter.

For the list of supported automated upgrade scenarios and the documentation roadmap, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

This chapter includes the following topics:

- [Section 6.1, "Variables Used in This Chapter"](#)
- [Section 6.2, "Reviewing System Requirements and Certifications"](#)
- [Section 6.3, "Backing up the Existing Environment"](#)
- [Section 6.4, "Setting the Required Environment Variables Necessary for Upgrade"](#)
- [Section 6.5, "Verifying Hostnames in the Hosts File"](#)
- [Section 6.6, "Obtaining the Automated Upgrade Tool"](#)
- [Section 6.7, "Updating the upgrade.properties File"](#)
- [Section 6.8, "Performing Pre-Validation Checks Using preValidate.pl Script"](#)
- [Section 6.9, "Creating BIP Schema for Oracle Identity Manager Upgrade on Solaris, IBM AIX, and HP Itanium Platforms"](#)
- [Section 6.10, "Upgrading Oracle Identity and Access Management Binaries and Configuration Using idmUpgrade.pl script"](#)
- [Section 6.11, "Performing Post-Validation Checks Using postValidate.pl Script"](#)
- [Section 6.12, "Stopping All Servers Using stopall.sh Script"](#)
- [Section 6.13, "Post-Upgrade Tasks"](#)
- [Section 6.14, "Troubleshooting"](#)

## 6.1 Variables Used in This Chapter

[Table 6–1](#) lists the variables used in this chapter.

**Table 6–1 Variables Used in This Chapter and Their Descriptions**

Variable	Description
<code>SCRIPT_FILE_LOCATION</code>	This is the location where you copied the upgrade tool <code>idmUpgrade.zip</code> , and extracted the files.
<code>OAMHOST</code> <code>OAMHOST1</code> <code>OAMHOST2</code>	This is the host on which Oracle Access Manager is installed.
<code>OIMHOST</code> <code>OIMHOST1</code> <code>OIMHOST2</code>	This is the host on which Oracle Identity Manager is installed.
<code>WEBHOST</code> <code>WEBHOST1</code> <code>WEBHOST2</code>	This is the host on which Oracle HTTP Server is installed.
<code>LDAPHOST</code> <code>LDAPHOST1</code> <code>LDAPHOST2</code>	This is the host on which Oracle Unified Directory is installed.

## 6.2 Reviewing System Requirements and Certifications

Before performing any installation, upgrade, or migration, you should read the system requirements and certification documents to ensure that your environment meets the minimum requirements for the products you are installing or upgrading to.

- *Oracle Fusion Middleware System Requirements and Specifications*

This document contains information related to hardware and software requirements, minimum disk space and memory requirements, and required system libraries, packages, or patches.
- *Oracle Fusion Middleware Supported System Configurations*

This document contains information related to supported installation types, platforms, operating systems, databases, JDK, and third-party products.
- For interoperability and compatibility issues that may arise when installing, refer to *Oracle Fusion Middleware Interoperability and Compatibility Guide*.

This document contains important information regarding the ability of Oracle Fusion Middleware products to function with previous versions of other Oracle Fusion Middleware, Oracle, or third-party products. This information is applicable to both new Oracle Fusion Middleware users and existing users who are upgrading their existing environment.

## 6.3 Backing up the Existing Environment

Backup the Database and the file system before you start with the upgrade process. In case of any failure during upgrade, you can restore your environment by restoring the Database and file system that you backed up.

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

## 6.4 Setting the Required Environment Variables Necessary for Upgrade

This section lists the environment variables that you must set before you proceed with the upgrade.

Table 6–2 lists the environment variables to be set. Depending on the platform you are using and the upgrade scenario, set the required environment variables using the command described in the column "Command to be Used".

**Table 6–2 Environment Variables to be Set**

Variable	Applicable for Platforms	Description	Command to be Used
JAVA_HOME	All platforms	Specify the absolute path to the JDK location.	On OAM/OIM/OHS nodes: <ul style="list-style-type: none"> <li>■ <code>JAVA_HOME=MW_HOME/jdk6</code></li> <li>■ <code>export JAVA_HOME</code></li> </ul>
LIBPATH	AIX	Specify the absolute path to the directories where Sybase IQ shared libraries are located.	On OAM/OIM/LOUD/OHS nodes: <ul style="list-style-type: none"> <li>■ <code>LIBPATH=IDM_UPGRADE_HOME/lib:REPOS_HOME/perl/lib/site_perl/5.10.0/aix-thread-multi-64all/auto/XML/Parser/Expat</code></li> <li>■ <code>export LIBPATH</code></li> </ul>
LD_LIBRARY_PATH	Solaris.Sparc64 Solaris.x64 HPUX.IA64	Specify the absolute path to the directories where Sybase IQ shared libraries are located.	On OAM/OIM/LOUD/OHS nodes: On Solaris.Sparc64, run the following commands: <ul style="list-style-type: none"> <li>■ <code>LD_LIBRARY_PATH=IDM_UPGRADE_HOME/lib:REPOS_HOME/perl/lib/site_perl/5.10.0/sun4-solaris-thread-multi-64/auto/XML/Parser/Expat</code></li> <li>■ <code>export LD_LIBRARY_PATH</code></li> </ul> On Solaris.x64, run the following commands: <ul style="list-style-type: none"> <li>■ <code>LD_LIBRARY_PATH=IDM_UPGRADE_HOME/lib:REPOS_HOME/perl/lib/site_perl/5.10.0/i86pc-solaris-thread-multi-64/auto/XML/Parser/Expat</code></li> <li>■ <code>export LD_LIBRARY_PATH</code></li> </ul> On HPUX.IA64, run the following commands: <ul style="list-style-type: none"> <li>■ <code>LD_LIBRARY_PATH=IDM_UPGRADE_HOME/lib:REPOS_HOME/perl/lib/site_perl/5.10.0/IA64.ARCHREV_0-thread-multi-LP64/auto/XML/Parser/Expat</code></li> <li>■ <code>export LD_LIBRARY_PATH</code></li> </ul>

**Table 6–2 (Cont.) Environment Variables to be Set**

Variable	Applicable for Platforms	Description	Command to be Used
PERL5LIB	All platforms	Specify the perl location.	<p>On OAM/OIM/OHS nodes:</p> <ul style="list-style-type: none"> <li>■ PERL5LIB=REPOS_HOME/perl/lib/site_perl/5.10.0:REPOS_HOME/perl/lib/5.10.0</li> <li>■ export PERL5LIB</li> </ul> <p>In the above command, <i>REPOS_HOME</i> refers to the absolute path to 11.1.2.3.0 repository location.</p>
PATH	All platforms	Set the PATH variable to point to JAVA_HOME/bin & REPOS_HOME/perl/bin to use the 64-bit perl version 5.10.0.	<p>On OAM/OIM/OHS nodes:</p> <ul style="list-style-type: none"> <li>■ PATH=JAVA_HOME/bin:REPOS_HOME/perl/bin:\$PATH</li> <li>■ export PATH</li> </ul> <p>In the above command, <i>REPOS_HOME</i> refers to the absolute path to 11.1.2.3.0 repository location.</p>
SKIP_ROOTPRE	AIX	Set the SKIP_ROOTPRE environment variable to TRUE to ensure that the installer does not prompt you while performing checks.	<p>On OHS node:</p> <ul style="list-style-type: none"> <li>■ SKIP_ROOTPRE=TRUE</li> <li>■ export SKIP_ROOTPRE</li> </ul>

## 6.5 Verifying Hostnames in the Hosts File

Make sure that the `/etc/hosts` file contains both canonical host name (fully qualified host name) along with the host name entry. To verify this, run the following command:

```
more /etc/hosts
```

The following is the sample output of this command:

```
192.0.2.1 myhost.example.com myhost
```

If the `/etc/hosts` file does not contain fully qualified host names, then add the host names, and reboot the system or restart the network system. For example, `/etc/rc.d/init.d/network restart`.

## 6.6 Obtaining the Automated Upgrade Tool

You must download the upgrade tool and copy it to any location on the host where you will be performing the upgrade. To do this, complete the following steps:

1. Download the automated upgrade tool from Oracle Technology Network (OTN). The upgrade tool is available in a zip file named `idmUpgrade.zip` as part of the Oracle Identity and Access Management 11.1.2.3.0 shiphome. For information about obtaining 11g Release 2 (11.1.2.3.0) software, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.
2. Copy the upgrade tool to any location on the host where you will be performing the upgrade. This location is referred to as `SCRIPT_FILE_LOCATION` in this document.

3. Extract the contents of the `idmUpgrade.zip` file by running the following command:

```
cd SCRIPT_FILE_LOCATION;unzip -q idmUpgrade.zip
```

This command creates a new folder named `r2ps3` which contains the script file.

---

**Note:** The instructions for performing an automated upgrade of Oracle Identity and Access Management to 11g Release 2 (11.1.2.3.0) assume you have applied the Oracle Identity and Access Management Automated Upgrade Tool Bundle Patch 2 (11.1.2.3.2). To download this patch, go to the following URL:

<https://updates.oracle.com/download/21419345.html>

---

## 6.7 Updating the upgrade.properties File

You must update the `upgrade.properties` file located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties` with the values for the properties required for your upgrade scenario. The upgrade script uses the values that you specify in this properties file.

To update the `upgrade.properties` file, complete the following steps:

1. Open the `upgrade.properties` file located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties`, in a text editor.
2. Set the values for the properties required for your upgrade.

[Table 6–3](#) lists all the properties present in the `upgrade.properties` file, their description, default values, and information about when to use this property.

**Table 6–3 Properties to be Updated in the upgrade.properties File**

Property	Description	When Upgrading	Sample Value
LOG_DIR	This is the location where logs files are created.	<ul style="list-style-type: none"> <li>▪ OIM</li> <li>▪ OAM</li> <li>▪ OIM-OAM-OU</li> </ul>	<code>/IDM/BASEDIR/logs</code>
WALLET_DIR	<p>This is the location where <code>cwallet.sso</code> file is created.</p> <p>An Oracle wallet is a container that stores your credentials, such as certificates, trusted certificates, certificate requests, and private keys.</p> <p><code>cwallet.sso</code> is an auto-login wallet.</p>	<ul style="list-style-type: none"> <li>▪ OIM</li> <li>▪ OAM</li> <li>▪ OIM-OAM-OU</li> </ul>	<code>/patchAutomation</code>

**Table 6–3 (Cont.) Properties to be Updated in the upgrade.properties File**

Property	Description	When Upgrading	Sample Value
LCMCONFIG_HOME	This is the location of topology.xml which was created when the setup was deployed using the Deployment tool. The topology.xml file contains environment related properties.  The topology.xml file is located at <code>LCMCONFIG_HOME/topology/topology.xml</code> .	<ul style="list-style-type: none"> <li>■ OIM</li> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>/IDMTOP/lcmdir/provisioning/phaseguards/lcmconfig</code>
START_STOP_SCRIPT_WORKING_DIR	This is the location where IDM Start, Stop scripts are present.	<ul style="list-style-type: none"> <li>■ OIM</li> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>/IDMTOP/config/scripts</code>
IDMLCM_HOME	This is the location where IDM LCM library files are present. The IDM LCM library files are used to parse topology.xml file.  The location of the IDM LCM library files is <code>IDMLCM_HOME/common/lib</code> .	<ul style="list-style-type: none"> <li>■ OIM</li> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>/BASEDIR/idmlcm</code>
JAVA_HOME	This is the location of the Java home.	<ul style="list-style-type: none"> <li>■ OIM</li> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>/IDM/BASEDIR/jdk6</code>
DB_SYS_PASSWORD	This is the Database sys password.	<ul style="list-style-type: none"> <li>■ OIM</li> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>Password1</code>
PATCHCONFLICT_TOOL_INSTALLER_LOC	This is the location where you downloaded Patch Conflict Manager.	<ul style="list-style-type: none"> <li>■ OIM</li> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>/patchConflict_tool_installer/PCMV6</code>
OAM_ADMIN_USER_NAME	This is the username of the OAM administrator.	<ul style="list-style-type: none"> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>oamadmin</code>
OAM_ADMIN_USER_NAME_PASSWORD	This is the password of the OAM administrator.	<ul style="list-style-type: none"> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>Password1</code>
LDAP_ADMIN_USER	Specify the LDAP Admin user.	<ul style="list-style-type: none"> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>oudadmin</code>
LDAP_ADMIN_PASSWORD	Specify the LDAP Admin password.	<ul style="list-style-type: none"> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>password1</code>
IDSTORE_ADMIN_PASSWORD	Specify the ID store administrator password.	<ul style="list-style-type: none"> <li>■ OIM</li> <li>■ OAM</li> <li>■ OIM-OAM-LOUD</li> </ul>	<code>password1</code>

**Table 6–3 (Cont.) Properties to be Updated in the upgrade.properties File**

Property	Description	When Upgrading	Sample Value
OAM_ADMIN_USER	Specify the username of the Oracle Adaptive Access Manager administrator.	<ul style="list-style-type: none"> <li>■ OAM</li> <li>■ OIM-OAM-OUD</li> </ul>	oaamadminuser
OAM_ADMIN_PASSWORD	Specify the Oracle Adaptive Access Manager administrator password.	<ul style="list-style-type: none"> <li>■ OAM</li> <li>■ OIM-OAM-OUD</li> </ul>	password1
BIP_SERVER_PORT	This is the plain port of Oracle BI Publisher.	<ul style="list-style-type: none"> <li>■ OIM</li> <li>■ OIM-OAM-OUD</li> </ul>	9704
BIP_SERVER_SSL_PORT	This is the SSL port of Oracle BI Publisher.	<ul style="list-style-type: none"> <li>■ OIM</li> <li>■ OIM-OAM-OUD</li> </ul>	9804
POLICY_MGR_PORT	Specify the port for Oracle Access Management Policy Manager Managed Server.	<ul style="list-style-type: none"> <li>■ OAM</li> <li>■ OIM-OAM-OUD</li> </ul>	14150

## 6.8 Performing Pre-Validation Checks Using preValidate.pl Script

To perform the pre-validation checks, run the following command from the location `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/`:

```
perl preValidate.pl -node=node -prop=location_of_upgrade.properties
```

In this command,

- `node` refers to the component for which you running this script. Specify one of the following values depending on the component you are upgrading:
  - `WEBTIER`: Specify this value for the `-node` argument if you are running the `preValidate.pl` script for performing pre-validation checks for Oracle HTTP Server.
  - `DIRECTORY`: Specify this value for the `-node` argument if you are running the `preValidate.pl` script for performing pre-validation checks for Oracle Unified Directory.
  - `OIM`: Specify this value for the `-node` argument if you are running the `preValidate.pl` script for performing pre-validation checks for Oracle Identity Manager.
  - `OAM`: Specify this value for the `-node` argument if you are running the `preValidate.pl` script or performing pre-validation checks for Oracle Access Manager.
- `location_of_upgrade.properties` refers to the absolute path to the `upgrade.properties` file. `upgrade.properties` file is located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties`.

The `preValidate.pl` script performs a set of pre-validation checks. If any validation fails, you must check the logs generated at the location that you specified for `LOG_DIR` property in the `upgrade.properties` file.

To verify that the pre-validation checks were performed successfully, check for the following `SUCCESS` string in the log file:

SUCCESS: All upgrade properties passed during preValidation process.

If you find the following ERROR string in the log file, it implies that the pre-validation checks were failed. You must investigate the failed plugins, resolve the issue, and re-run the pre-validation checks.

ERROR: SOME PREVALIDATE TESTS FAILED

## 6.9 Creating BIP Schema for Oracle Identity Manager Upgrade on Solaris, IBM AIX, and HP Itanium Platforms

If you are upgrading Oracle Identity Manager on platforms such as Solaris, IBM AIX, and HP Itanium using the automated upgrade tool, you must create the Oracle BI Publisher (BIPLATFORM) schema manually using the Repository Creation Utility (RCU) 11.1.2.3.0 from the machine that is running Linux or Windows operating system.

---

---

**Note:** If you are upgrading Oracle Identity Manager on Linux, skip this step, as the automated upgrade tool creates the BIPLATFORM schema on Linux.

---

---

To create the database schemas using RCU, perform the following tasks:

1. [Obtaining Repository Creation Utility](#)
2. [Starting Repository Creation Utility](#)
3. [Creating Schemas](#)

### 6.9.1 Obtaining Repository Creation Utility

Download the Repository Creation Utility 11.1.2.3.0. For information about obtaining Repository Creation Utility, see "Obtaining RCU" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

### 6.9.2 Starting Repository Creation Utility

Start the Repository Creation Utility 11.1.2.3.0 from the location where you downloaded it. For information about starting Repository Creation Utility, see "Starting RCU" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

### 6.9.3 Creating Schemas

Create the necessary schemas using Repository Creation Utility. For information about creating schemas, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

---

---

**Note:** Select only **BIPLATFORM** schema on the **Select Components (for Create Operation)** screen.

---

---

## 6.10 Upgrading Oracle Identity and Access Management Binaries and Configuration Using idmUpgrade.pl script

The script `idmUpgrade.pl` can be used to upgrade both binaries and configurations. The value specified for the argument `-mode` while running the script determines if the script is run to upgrade binaries or configuration.

To upgrade Oracle Identity and Access Management binaries or configurations or both, run the following command from the location `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/`:

```
perl idmUpgrade.pl -node=node -repoLocs=repo_location -props=location_of_upgrade.properties -mode=mode
```

In this command,

- `node` refers to the component for which binary and/or configuration upgrade is performed. Specify one of the following values depending on the component you are upgrading:
  - `WEBTIER`: Specify this value for the `-node` argument if you are running the `idmUpgrade.pl` script for Oracle HTTP Server.
  - `DIRECTORY`: Specify this value for the `-node` argument if you are running the `idmUpgrade.pl` script for Oracle Unified Directory.
  - `OIM`: Specify this value for the `-node` argument if you are running the `idmUpgrade.pl` script for Oracle Identity Manager.
  - `OAM`: Specify this value for the `-node` argument if you are upgrading running the `idmUpgrade.pl` script for Oracle Access Manager.
- `repo_location` refers to the absolute path to 11.1.2.3.0 repository location. You can pass a maximum of two repository locations in the command line argument, separated by comma. For example, `repo` and `post-repo` locations.
- `location_of_upgrade.properties` refers to the absolute path to the `upgrade.properties` file. `upgrade.properties` file is located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties`.
- `mode` refers to the type of upgrade you want to perform.

For binary upgrade, specify `binary` as the value for the `-mode` argument.

For configuration upgrade, specify `config` as the value for the `-mode` argument.

For performing both binary and configuration upgrade, specify `both` as the value for the `-mode` argument. This can be used in case of single node upgrade. If you specify `both` as the value for the `-mode` argument, the upgrade script performs binary upgrade first followed by the configuration upgrade.

If you do not specify any value for the argument `-mode`, the value will be taken as `both`, and the script will upgrade the binaries first followed by the configuration.

## 6.11 Performing Post-Validation Checks Using postValidate.pl Script

After you perform binary upgrade and configurations, you must perform the post-validation checks by running the following command:

```
perl postValidate.pl -node=node -prop=location_of_upgrade.properties
```

In this command,

- *node* refers to the component for which the post-validation checks are performed. Specify one of the following values depending on the component you are upgrading:
  - **WEBTIER**: Specify this value for the `-node` argument if you are running the `postValidate.pl` script to perform post-validation checks for Oracle HTTP Server.
  - **DIRECTORY**: Specify this value for the `-node` argument if you are running the `postValidate.pl` script to perform post-validation checks for Oracle Unified Directory.
  - **OIM**: Specify this value for the `-node` argument if you are running the `postValidate.pl` script to perform post-validation checks for Oracle Identity Manager.
  - **OAM**: Specify this value for the `-node` argument if you are running the `postValidate.pl` script to perform post-validation checks for Oracle Access Manager.
- *location\_of\_upgrade.properties* refers to the absolute path to the `upgrade.properties` file. `upgrade.properties` file is located at `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/upgrade.properties`.

The `postValidate.pl` script performs a set of post-validation checks. If any validation fails, you must check the logs generated at the location that you specified for `LOG_DIR` property in the `upgrade.properties` file.

To verify that the post-validation checks were performed successfully, check for the following **SUCCESS** string in the log file:

```
SUCCESS: All upgrade properties passed during postValidation process.
```

If you find the following **ERROR** string in the log file, it implies that the post-validation checks were failed. You must investigate the failed plugins, resolve the issue, and re-run the post-validation checks.

```
ERROR: SOME POSTVALIDATE TESTS FAILED
```

## 6.12 Stopping All Servers Using stopall.sh Script

You can use the script `stopall.sh` located at `SHARED_CONFIG_DIR/config/scripts` directory to stop all of the servers in the environment. The script stops the components which are installed on a given host in the following order. What is stopped depends on what is installed on the host on which the script is running:

1. Oracle HTTP Server
2. Oracle Access Manager Managed Server(s)
3. Oracle Identity Manager Managed Server(s)
4. Oracle SOA Suite Managed Server(s)
5. WebLogic Administration Server
6. Node Manager
7. Oracle Unified Directory

To stop all of the servers on a host, run the following command from the location `SHARED_CONFIG_DIR/config/scripts`:

```
./stopall.sh
```

Specify the WebLogic and Node Manager administrator passwords when prompted.

## 6.13 Post-Upgrade Tasks

This section describes the post-upgrade tasks. You must perform only those tasks that are applicable to your upgrade scenario.

This section contains the following topics:

- [Adding the Java System Property for Oracle Adaptive Access Manager](#)

### 6.13.1 Adding the Java System Property for Oracle Adaptive Access Manager

If you upgraded OIM-OAM Integrated with Oracle Unified Directory (OUD) topology that has Oracle Adaptive Access Manager (OAAM) configured, you must add the following JAVA system property to the `IAMAccessDomain/bin/setDomainEnv.sh` script:

```
-Djava.security.auth.login.config=${ORACLE_
HOME}/designconsole/config/authwl.conf
```

After you update the JAVA system property in the `setDomainEnv.sh` file, restart the OAAM Managed Server (for example, `wls_oaam1`).

## 6.14 Troubleshooting

This section describes some of the common issues that you might encounter during the upgrade process, and their workaround. This section includes the following topics:

- [IDM URL Access Issues When Performing Pre-Validation and Post-Validation Checks on HP-UX Itanium](#)
- [Autologin to OIM Console Fails After Resetting User Password Post OIM/OAM Isolated Upgrade on AIX](#)
- [Perl Undefined Symbol Error While Running preValidate.pl Script](#)
- [/xmlpserver and /access URLs not Accessible via OHS Port After Isolated Upgrade](#)

### 6.14.1 IDM URL Access Issues When Performing Pre-Validation and Post-Validation Checks on HP-UX Itanium

When you perform pre-validation and post-validation checks on HP-UX Itanium by running the `preValidate.pl` and `postValidate.pl` scripts respectively, you might encounter failures related to "Checking Web Pages" during IDM urls access checks in Access Manager or Oracle Identity Manager domains. Ignore these messages.

The workaround for this issue is to manually check and confirm the IDM URLs accessibility from the browser.

### 6.14.2 Autologin to OIM Console Fails After Resetting User Password Post OIM/OAM Isolated Upgrade on AIX

After you perform OIM or OAM isolated upgrade on AIX, autologin to OIM console fails with the following system error message:

```
System error. Please re-try your action.If you continue to get this error, please
```

contact the Administrator.

The workaround for this issue is to use the new user credentials to log in to the OIM console.

### 6.14.3 Perl Undefined Symbol Error While Running preValidate.pl Script

If your perl version is 5.10.1, the following error is seen when you run the preValidate.pl script to perform pre-validation checks:

```
Checking webpage $OAM_ADMIN_LBRURL/console
Making request to http://host.example.com:port/console...
perl: symbol lookup error:
/upgrade_script/r2ps3/idmUpgrade/auto/Crypt/SSLeay/SSLeay.so:
undefined symbol: Perl_Tstack_sp_ptr
```

The workaround for this issue is to delete the SSLeay.so file from the directory `SCRIPT_FILE_LOCATION/r2ps3/idmUpgrade/auto/Crypt/SSLeay/` before you run the automated upgrade script.

### 6.14.4 /xmlpserver and /access URLs not Accessible via OHS Port After Isolated Upgrade

After you perform isolated upgrade, that is, upgrading Oracle Identity Manager only or Oracle Access Management only in an environment that is deployed using the Life Cycle Management (LCM) tools, the following URLs are not accessible via Oracle HTTP Server port:

- `http://host:port/xmlpserver`
- `http://host:port/access`

The workaround for this issue is as follows:

If you have upgraded Oracle Identity Manager only, add the following lines to the `OHS_INSTANCE_HOME/moduleconf/idm.conf` file, to resolve this issue:

```
# Oracle BIP console
<Location /xmlpserver>
  SetHandler weblogic-handler
  WLCookieName JSESSIONID
  WebLogicHost host.example.com
  WebLogicPort wls_port

  WLLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
</Location>
```

If you have upgraded Oracle Access Management only, add the following lines to the `OHS_INSTANCE_HOME/moduleconf/idm.conf` file:

```
<Location /access>
  SetHandler weblogic-handler
  WebLogicHost host.example.com
  WebLogicPort wls_port
  WLCookieName OAMSESSIONID
</Location>
```

# Part III

---

## Upgrading Oracle Identity and Access Management 11g Release 2 (11.1.2.x.x) Environments

This part includes the following chapters:

- [Chapter 8, "Upgrading Oracle Access Management 11g Release 2 \(11.1.2.x.x\) Environments"](#)
- [Chapter 9, "Upgrading Oracle Adaptive Access Manager 11g Release 2 \(11.1.2.x.x\) Environments"](#)
- [Chapter 10, "Upgrading Oracle Identity Manager 11g Release 2 \(11.1.2.x.x\) Environments"](#)
- [Chapter 11, "Upgrading Oracle Entitlements Server 11g Release 2 \(11.1.2.x.x\) Environments"](#)
- [Chapter 7, "Upgrading Oracle Privileged Account Manager 11g Release 2 \(11.1.2.x.x\) Environments"](#)



---

---

# Upgrading Oracle Privileged Account Manager 11g Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade Oracle Privileged Account Manager (OPAM) 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0) and 11g Release 2 (11.1.2) environments to Oracle Privileged Account Manager 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

---

---

**Note:** This chapter refers to Oracle Privileged Account Manager 11g Release 2 (11.1.2), 11g Release 2 (11.1.2.1.0), and 11g Release 2 (11.1.2.2.0) environments as 11.1.2.x.x.

---

---

This chapter includes the following sections:

- [Section 7.1, "Upgrade Roadmap for Oracle Privileged Account Manager"](#)
- [Section 7.2, "Performing the Required Pre-Upgrade Tasks"](#)
- [Section 7.3, "Exporting the Pre-Upgrade Data"](#)
- [Section 7.4, "Stopping the Administration Servers and the Managed Server\(s\)"](#)
- [Section 7.5, "Upgrading Oracle WebLogic Server to 10.3.6"](#)
- [Section 7.6, "Updating Oracle Privileged Account Manager Binaries to 11.1.2.3.0"](#)
- [Section 7.7, "Upgrading the Database Schemas"](#)
- [Section 7.8, "Start the Administration Server and the Managed Server\(s\)"](#)
- [Section 7.9, "Redeploying the Applications"](#)
- [Section 7.10, "Enabling TDE or Non-TDE Mode in OPAM Data Store"](#)
- [Section 7.11, "Importing the Pre-Upgrade Data"](#)
- [Section 7.12, "Clearing Pre-Upgrade OPSS Artifacts"](#)

- [Section 7.13, "Optional: Configuring the Oracle Privileged Account Manager 11.1.2.3.0 Session Manager"](#)
- [Section 7.14, "Optional: Configuring Oracle Privileged Account Manager Console Application on OPAM Managed Server"](#)
- [Section 7.15, "Verifying the Oracle Privileged Account Manager Upgrade"](#)

## 7.1 Upgrade Roadmap for Oracle Privileged Account Manager

[Table 7–1](#) lists the tasks to be performed to upgrade Oracle Privileged Account Manager 11.1.2.x.x to Oracle Privileged Account Manager 11.1.2.3.0.

**Table 7–1 Roadmap for Upgrading Oracle Privileged Account Manager 11.1.2.x.x to 11.1.2.3.0**

SI No	Task	For More Information
1	Complete the necessary pre-upgrade tasks before you begin with the upgrade process.	See, <a href="#">Performing the Required Pre-Upgrade Tasks</a>
2	If you are upgrading Oracle Privileged Account Manager 11.1.2 to Oracle Privileged Account Manager 11.1.2.3.0, you must export the pre-upgrade data.  If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to Oracle Privileged Account Manager 11.1.2.3.0, skip this task.	See, <a href="#">Section 7.3, "Exporting the Pre-Upgrade Data"</a>
3	Stop the Administration Server and all the Managed Servers.	See, <a href="#">Stopping the Administration Servers and the Managed Server(s)</a>
4	If you are not using Oracle WebLogic Server 10.3.6, and you must upgrade Oracle WebLogic Server to 10.3.6.	See, <a href="#">Upgrading Oracle WebLogic Server to 10.3.6</a>
5	Upgrade the Oracle Privileged Account Manager binaries to 11.1.2.3.0.	See, <a href="#">Updating Oracle Privileged Account Manager Binaries to 11.1.2.3.0</a>
6	Upgrade the 11.1.2.x.x Database schemas.	See, <a href="#">Upgrading the Database Schemas</a>
7	Start all the servers.	See, <a href="#">Start the Administration Server and the Managed Server(s)</a>
8	Redeploy the Oracle Privileged Account Manager Console application, Oracle Privileged Account Manager applications, and Oracle Privileged Account Manager Session Manager application.	See, <a href="#">Redeploying the Applications</a>
9	If your starting point is 11g Release 2 (11.1.2), complete the following tasks: <ol style="list-style-type: none"> <li>1. Set up either TDE mode or non-TDE mode in the OPAM Data Store.</li> <li>2. Import the pre-upgrade data.</li> <li>3. Clear the pre-upgrade OPSS artifacts</li> </ol> If your starting point is 11g Release 2 (11.1.2.2.0) or 11g Release 2 (11.1.2.1.0), skip the above tasks.	See: <ul style="list-style-type: none"> <li>■ <a href="#">Enabling TDE or Non-TDE Mode in OPAM Data Store</a></li> <li>■ <a href="#">Importing the Pre-Upgrade Data</a></li> <li>■ <a href="#">Clearing Pre-Upgrade OPSS Artifacts</a></li> </ul>

**Table 7–1 (Cont.) Roadmap for Upgrading Oracle Privileged Account Manager 11.1.2.x.x to 11.1.2.3.0**

SI No	Task	For More Information
10	<p>If your starting point is 11g Release 2 (11.1.2.1.0) or 11g Release 2 (11.1.2), complete the following tasks:</p> <ul style="list-style-type: none"> <li>■ Configure the Oracle Privileged Account Manager session manager (if required)</li> <li>■ Configure the Oracle Privileged Account Manager Console application (if required).</li> </ul>	<p>See:</p> <ul style="list-style-type: none"> <li>■ <a href="#">Optional: Configuring the Oracle Privileged Account Manager 11.1.2.3.0 Session Manager</a></li> <li>■ <a href="#">Optional: Configuring Oracle Privileged Account Manager Console Application on OPAM Managed Server</a></li> </ul>
11	Verify the upgrade.	See, <a href="#">Verifying the Oracle Privileged Account Manager Upgrade</a>

## 7.2 Performing the Required Pre-Upgrade Tasks

Before you begin with the upgrade, you must complete the following prerequisites:

- Review the *Oracle Fusion Middleware System Requirements and Specifications* and *Oracle Fusion Middleware Supported System Configurations* documents to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).
- Ensure that you are using a Java Development Kit (JDK) version that is supported and certified with Oracle Identity and Access Management 11.1.2.3.0.

You can verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

---

**Note:** For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

---

## 7.3 Exporting the Pre-Upgrade Data

If you are upgrading Oracle Privileged Account Manager 11.1.2 to 11.1.2.3.0, you must export the pre-upgrade Oracle Privileged Account Manager data before you start the upgrade process.

---

**Note:** If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to 11.1.2.3.0, skip this task.

---

You must export the pre-upgrade OPAM data such as targets, accounts, and users, before you upgrade Oracle Privileged Account Manager 11.1.2 to 11.1.2.3.0. The steps provided in this section describes the process to export the OPAM data to an XML file. A manual export is required because the back end data store will be moved from the OPSS schema to a native OPAM data store in the new version.

Use the following procedure to export the OPAM data:

1. Set the following environment variables:

Variable	Description
ORACLE_HOME	Where Oracle Privileged Account Manager is installed.
JAVA_HOME	Location of JDK used for the WebLogic installation.

2. Navigate to `ORACLE_HOME/opam/bin`.
3. Execute the following command with all the parameters mentioned:

**On UNIX:**

```
./opam.sh
[-url <OPAM server url>]] (defaults to https://localhost:18102/opam)
-u [user name] (the user should have OPAM_SECURITY_ADMIN and OPAM_USER_MANAGER
roles)
-p <password>
-x export -f [export xml file]
[-encpassword <encryption/decryption password>] (provide a value for
encpassword for better security)
[-enckeylen <Key Length for encryption/decryption of password>] (defaults to
128)
[-log <log file Location>] (defaults to opamlog_<timestamp>.txt)
```

**On Windows:**

```
./opam.bat
[-url <OPAM server url>]] (defaults to https://localhost:18102/opam)
-u [user name] (the user should have OPAM_SECURITY_ADMIN and OPAM_USER_MANAGER
roles)
-p <password>
-x export -f [export xml file]
[-encpassword <encryption/decryption password>] (provide a value for
encpassword for better security)
[-enckeylen <Key Length for encryption/decryption of password>] (defaults to
128)
[-log <log file Location>] (defaults to opamlog_<timestamp>.txt)
```

---

**Note:** If the data was exported without an encryption password, then specify this with the parameter `"-noencrypt true"` while importing the data.

---

## 7.4 Stopping the Administration Servers and the Managed Server(s)

The upgrade process involves changes to the binaries and to the schema. So, before you begin the upgrade process, you must shut down the WebLogic Administration Server and the Oracle Privileged Account Manager Managed Server(s).

For information about stopping the WebLogic Administration Server and the Managed Servers, see [Section 24.1.9, "Stopping the Servers"](#).

## 7.5 Upgrading Oracle WebLogic Server to 10.3.6

Oracle Identity and Access Management 11.1.2.3.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Privileged Account Manager environment is using Oracle WebLogic Server 10.3.5 or any earlier version, you must upgrade Oracle WebLogic Server to 10.3.6.

---

---

**Note:** If you are already using Oracle WebLogic Server 10.3.6, ensure that you apply the mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server 10.3.6, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

---

---

For information about upgrading Oracle WebLogic Server to 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

## 7.6 Updating Oracle Privileged Account Manager Binaries to 11.1.2.3.0

To update Oracle Privileged Account Manager 11.1.2.x.x binaries to 11.1.2.3.0, you must use the Oracle Identity and Access Management 11.1.2.3.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Oracle Privileged Account Manager Middleware Home. Your Oracle Home is upgraded from 11.1.2.x.x to 11.1.2.3.0.

For information about updating the Oracle Privileged Account Manager binaries to 11.1.2.3.0, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 7.7 Upgrading the Database Schemas

Upgrade the following schemas using the Patch Set Assistant.

- OPAM
- OPSS - OPSS is selected as a dependency when you select OPAM.

For information about upgrading schemas using Patch Set Assistant, see [Section 24.1.4, "Upgrading Schemas Using Patch Set Assistant"](#).

After you upgrade the OPAM and OPSS schemas, the version of the OPAM schema will be 11.1.2.3.0.

## 7.8 Start the Administration Server and the Managed Server(s)

After you upgrade the schemas, start the WebLogic Administration Server and the Oracle Privileged Account Manager Managed Server(s).

For information about starting the WebLogic Administration Server and the Managed Servers, see [Section 24.1.8, "Starting the Servers"](#).

## 7.9 Redeploying the Applications

After you start the WebLogic Administration Server and the Oracle Privileged Account Manager Managed Servers, you must redeloy the Oracle Privileged Account Manager console and Oracle Privileged Account Manager applications. To do this, complete the following tasks:

- [Redeploying Oracle Privileged Account Manager Console Application](#)
- [Redeploying Oracle Privileged Account Manager Application](#)
- [Redeploying Oracle Privileged Account Manager Session Manager Application](#)

### 7.9.1 Redeploying Oracle Privileged Account Manager Console Application

Updating `oinav.ear` redeploys Oracle Privileged Account Manager Console application. There are two ways of updating the `oinav.ear` - using the WebLogic Administration console, and using the WebLogic Scripting Tool.

Redeploy Oracle Privileged Account Manager Console applications using one of the following ways:

- [Redeploying OPAM Console Application Using WebLogic Server Administration Console](#)
- [Redeploying OPAM Console Application Using WebLogic Scripting Tool \(WLST\)](#)

#### Redeploying OPAM Console Application Using WebLogic Server Administration Console

Complete the following steps to redeploy Oracle Privileged Account Manager Console Application through the WebLogic Administration console:

1. Log in to WebLogic Administration console:  
`http://admin_server_host:admin_server_port/console`
2. Under Domain Structure, click **Deployments**.
3. Select **oinav (11.1.1.3.0)** from the **Name** table.
4. Click **Update** and click **Finish** in the **Update Application Assistant** screen after verifying the source path.

---

---

**Note:** If WebLogic is running in production mode, click **Lock & Edit** before clicking **Update**.

---

---

#### Redeploying OPAM Console Application Using WebLogic Scripting Tool (WLST)

Complete the following steps to redeploy Oracle Privileged Account Manager Console application through the WLST console:

##### On UNIX

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location `MW_HOME/wlserver_10.3/common/bin`:  
On UNIX: `./wlst.sh`  
On Windows: `wlst.cmd`
2. Connect to the Administration Server using the following command:  
`connect('weblogic-username','weblogic-password','weblogic-url')`

3. At the WLST prompt, run the following command:  

```
redeploy('oinav#11.1.1.3.0')
```
4. Exit the WLST console using the `exit()` command.

## 7.9.2 Redeploying Oracle Privileged Account Manager Application

---

**Note:** The OPAM application version number is 11.1.2.0.0 while the actual Oracle Privileged Account Manager version number should be 11.1.2.3.0.

This is not an error. The discrepancy is caused by a difference between how OPAM and Identity Access Management releases are tracked internally.

---

Updating `opam.ear` redeploys Oracle Privileged Account Manager. There are two ways of updating the `opam.ear` - using the WebLogic Administration console, and using the WebLogic Scripting Tool.

Redeploy Oracle Privileged Account Manager applications using one of the following ways:

- [Redeploying OPAM Applications Using WebLogic Server Administration Console](#)
- [Redeploying OPAM Applications Using WebLogic Scripting Tool \(WLST\)](#)

### Redeploying OPAM Applications Using WebLogic Server Administration Console

Complete the following steps to upgrade Oracle Privileged Account Manager through the WebLogic Administration console:

1. Log in to WebLogic Administration console:  

```
http://admin_server_host:admin_server_port/console
```
2. Under Domain Structure, click **Deployments**.
3. Select **opam (11.1.2.0.0)** from the **Name** table.
4. Click **Update** and click **Finish** in the **Update Application Assistant** screen after verifying the source path.

---

**Note:** If WebLogic is running in production mode, click **Lock & Edit** before clicking **Update**.

---

### Redeploying OPAM Applications Using WebLogic Scripting Tool (WLST)

Complete the following steps to upgrade Oracle Privileged Account Manager through the WLST console:

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location `MW_HOME/wlserver_10.3/common/bin`:  

```
On UNIX: ./wlst.sh
```

```
On Windows: wlst.cmd
```
2. Connect to the Administration Server using the following command:

```
connect('weblogic-username','weblogic-password','weblogic-url')
```

3. At the WLST prompt, run the following command:

```
redeploy('opam#11.1.2.0.0')
```

4. Exit the WLST console using the `exit()` command.

### 7.9.3 Redeploying Oracle Privileged Account Manager Session Manager Application

Updating `opamsessionmgr.ear` redeploys Oracle Privileged Account Manager Session Manager. There are two ways of updating the `opamsessionmgr.ear` - using the WebLogic Administration console, and using the WebLogic Scripting Tool.

Redeploy Oracle Privileged Account Manager Session Manager applications using one of the following ways:

- [Redeploying OPAM Session Manager Using WebLogic Server Administration Console](#)
- [Redeploying OPAM Session Manager Using WebLogic Server Administration Console](#)

#### Redeploying OPAM Session Manager Using WebLogic Server Administration Console

Complete the following steps to upgrade Oracle Privileged Account Manager Session Manager through the WebLogic Administration console:

1. Log in to WebLogic Administration console:

```
http://admin_server_host:admin_server_port/console
```

2. Under Domain Structure, click **Deployments**.
3. Select **opamsessionmgr** from the **Name** table.
4. Click **Update** and click **Finish** in the **Update Application Assistant** screen after verifying the source path.

---

---

**Note:** If WebLogic is running in production mode, click **Lock & Edit** before clicking **Update**.

---

---

#### Redeploying OPAM Session Manager Using WebLogic Scripting Tool (WLST)

Complete the following steps to upgrade Oracle Privileged Account Manager Session Manager through the WLST console:

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location `MW_HOME/wlserver_10.3/common/bin`:

On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

2. Connect to the Administration Server using the following command:

```
connect('weblogic-username','weblogic-password','weblogic-url')
```

3. At the WLST prompt, run the following command:

```
redeploy('opamsessionmgr')
```

4. Exit the WLST console using the `exit()` command.

## 7.10 Enabling TDE or Non-TDE Mode in OPAM Data Store

If you are upgrading Oracle Privileged Account Manager 11.1.2 to 11.1.2.3.0, you must enable TDE or non-TDE mode in the Oracle Privileged Account Manager data store.

---

---

**Note:** If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to 11.1.2.3.0, skip this task.

---

---

Oracle Privileged Account Manager can operate with Oracle Database TDE (Transparent Data Encryption) mode. You can choose to either enable or disable the TDE mode. Oracle strongly recommends to enable the TDE mode for enhanced security. Depending upon what mode you wish to enable, complete one of the following tasks:

- [Configuring TDE Mode in Data Store](#)
- [Configuring Non-TDE Mode in Data Store](#)

### 7.10.1 Configuring TDE Mode in Data Store

To enable TDE mode in Oracle Privileged Account Manager data store, complete the following steps:

1. [Enabling TDE in the Database](#)
2. [Enabling Encryption in OPAM Schema](#)

#### 7.10.1.1 Enabling TDE in the Database

For information about enabling Transparent Data Encryption (TDE) in the database for Oracle Privileged Account Manager, see "Enabling Transparent Data Encryption" in the *Oracle Database Advanced Security Administrator's Guide*.

For more information, see "Securing Stored Data Using Transparent Data Encryption" in the *Oracle Database Advanced Security Administrator's Guide*

After enabling TDE in the database for Oracle Privileged Account Manager, you must enable encryption in OPAM schema, as described in "Enabling Encryption in OPAM Schema" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

#### 7.10.1.2 Enabling Encryption in OPAM Schema

To enable encryption in the OPAM schema, run the `opamxencrypt.sql` script with the OPAM schema user, using `sqlplus` or any other client.

```
IAM_HOME/opam/sql/opamxencrypt.sql
```

Example:

```
sqlplus DEV_OPAM/welcome1 @IAM_HOME/opam/sql/opamxencrypt.sql
```

### 7.10.2 Configuring Non-TDE Mode in Data Store

---

---

**Note:** This step is only necessary if you did not enable TDE as described in [Section 7.10.1, "Configuring TDE Mode in Data Store"](#).

---

---

While it is not recommended, if non-TDE mode is required by the user, the flag "tdemode" must be set to `false`. For more information, see "Setting Up Non-TDE Mode" in *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

---



---

**Caution:** Oracle recommends that you always use Transparent Data Encryption(TDE). Without TDE, your data is not secure.

For more information on switching between the two modes, see "Securing Data On Disk" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Privileged Account Manager*.

---



---

## 7.11 Importing the Pre-Upgrade Data

If you are upgrading Oracle Privileged Account Manager 11.1.2 to 11.1.2.3.0, you must export the pre-upgrade Oracle Privileged Account Manager data after you upgrade to 11.1.2.3.0.

---



---

**Note:** If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to 11.1.2.3.0, skip this task.

---



---

To import the pre-upgrade OPAM data, do the following:

1. Set the following environment variables:

Variable	Description
ORACLE_HOME	Oracle Privileged Account Manager is installed.
JAVA_HOME	Location of JDK used for the WebLogic installation.

2. Navigate to `ORACLE_HOME/opam/bin`.
3. Execute the `opam.sh` script with the following parameters:

```
./opam.sh
-url <OPAM server url> (defaults to https://localhost:18102/opam)
-u <user name> (the user should have OPAM_SECURITY_ADMIN and OPAM_USER_MANAGER
roles)
-p <password>
-x import -f <import xml file>
-encpassword <encryption/decryption password>
-enckeylen <Key Length for encryption/decryption of password> (Defaults to 128)
-log <log file Location> (defaults to opamlog_<timestamp>.txt)
```

## 7.12 Clearing Pre-Upgrade OPSS Artifacts

If you are upgrading Oracle Privileged Account Manager 11.1.2 to 11.1.2.3.0, you must clear the pre-upgrade OPSS artifacts after you upgrade to 11.1.2.3.0.

---



---

**Note:** If you are upgrading Oracle Privileged Account Manager 11.1.2.1.0 to 11.1.2.3.0, skip this task.

---



---

To clear the OPSS artifacts of the pre-upgrade instance, do the following:

**On UNIX:**

```
$ORACLE_HOME/common/bin/wlst.sh $ORACLE_HOME/opam/config/clean-opss.py <WebLogic
Administrator Username> <WebLogic Administrator Password>
<t3://<adminserver-host>:<adminserver-port>
```

**On Windows:**

```
$ORACLE_HOME\common\bin\wlst.cmd $ORACLE_HOME\opam\config\clean-opss.py <WebLogic
Administrator Username> <WebLogic Administrator Password>
<t3://<adminserver-host>:<adminserver-port>
```

## 7.13 Optional: Configuring the Oracle Privileged Account Manager 11.1.2.3.0 Session Manager

If you are upgrading Oracle Privileged Account Manager 11g Release 2 (11.1.2.2.0) to 11.1.2.3.0, this step is not required.

If you wish to configure the Oracle Privileged Account Manager 11.1.2.3.0 session manager, complete the following steps:

1. Stop the WebLogic Administration Server and the Oracle Privileged Account Manager Managed Servers.

For information about stopping the servers, see [Section 7.4, "Stopping the Administration Servers and the Managed Server\(s\)"](#).

2. Run the WLST script `configureSessionManager.py` from the location `ORACLE_HOME/opam/tools` as shown in the following example:

**On UNIX:**

```
./wlst.sh ORACLE_HOME/opam/tools/configureSessionManager.py -d <Path_
to_WebLogic_Domain_Directory> -o <Path_to_Oracle_Home_Directory>
```

**On Windows:**

```
wlst.cmd ORACLE_HOME\opam\tools\configureSessionManager.py -d <Path_
to_WebLogic_Domain_Directory> -o <Path_to_Oracle_Home_Directory>
```

## 7.14 Optional: Configuring Oracle Privileged Account Manager Console Application on OPAM Managed Server

If you are upgrading Oracle Privileged Account Manager 11g Release 2 (11.1.2.2.0) to 11.1.2.3.0, this step is not required.

If you wish to configure Oracle Privileged Account Manager Console application on the Oracle Privileged Account Manager Managed Server, complete the following steps:

1. Stop the WebLogic Administration Server and the Oracle Privileged Account Manager Managed Server(s). For information about stopping the servers, see [Section 24.1.9, "Stopping the Servers"](#).
2. Run the following WLST command from the location `MW_HOME/oracle_common/common/bin`:

**On UNIX:**

```
./wlst.sh ORACLE_HOME/opam/tools/configureOPAMConsole.py -d DOMAIN_HOME
-o ORACLE_HOME
```

On Windows:

```
wlst.cmd ORACLE_HOME/opam/tools/configureOPAMConsole.py -d DOMAIN_HOME  
-o ORACLE_HOME
```

## 7.15 Verifying the Oracle Privileged Account Manager Upgrade

Verify the Oracle Privileged Account Manager upgrade by doing the following:

1. Log in to the Oracle Privileged Account Manager 11.1.2.3.0 console using the following URL:

```
http://adminserver_host:adminserver_port/oinav/opam
```

If you have configured Oracle Identity Navigator on the Oracle Privileged Account Manager Managed Server, you can also use the following URL to log in to the Oracle Privileged Account Manager 11.1.2.3.0 console:

```
http://opamserver_host:opamserver_nonssl_port/oinav/opam
```

2. Verify that the pre-upgrade data, targets, accounts, grants are present, and working as expected.

---

---

# Upgrading Oracle Access Management 11g Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade your existing Oracle Access Management 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0) and 11g Release 2 (11.1.2) environments to Oracle Access Management 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0). For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

If you wish to upgrade Oracle Access Management multi-data center environments, refer to [Chapter 18, "Upgrading Oracle Access Management Multi-Data Center Environments"](#).

---

---

---

---

**Note:** This chapter refers to Oracle Access Management Access Manager 11g Release 2 (11.1.2), 11g Release 2 (11.1.2.1.0), 11g Release 2 (11.1.2.2.0) environments as 11.1.2.x.x.

---

---

This chapter contains the following sections:

- [Section 8.1, "Upgrade Roadmap for Oracle Access Management"](#)
- [Section 8.2, "Performing the Required Pre-Upgrade Tasks"](#)
- [Section 8.3, "Upgrading Oracle Home"](#)
- [Section 8.4, "Creating OMSM Schema"](#)
- [Section 8.5, "Upgrading the Database Schemas"](#)
- [Section 8.6, "Upgrading Oracle Platform Security Services"](#)
- [Section 8.7, "Copying Modified System mbean Configurations"](#)
- [Section 8.8, "Undeploying coherence#3.7.1.1 Library"](#)
- [Section 8.9, "Restarting the Servers"](#)
- [Section 8.10, "Upgrading System Configuration"](#)

- [Section 8.11, "Extending the Oracle Access Management Domain to Include Mobile Security Suite and Policy Manager"](#)
- [Section 8.12, "Starting the Servers"](#)
- [Section 8.13, "Performing the Required Post-Upgrade Tasks"](#)
- [Section 8.14, "Verifying the Oracle Access Management Upgrade"](#)
- [Section 8.15, "Troubleshooting"](#)

## 8.1 Upgrade Roadmap for Oracle Access Management

---

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Access Management upgrade may not be successful.

---

[Table 8–1](#) lists the steps to upgrade Oracle Access Management 11.1.2.x.x environments to 11.1.2.3.0.

**Table 8–1 Roadmap for Upgrading Oracle Access Management 11.1.2.x.x to 11.1.2.3.0.**

Task No.	Task	For More Information
1	Complete the pre-upgrade tasks before you start the upgrade process.	See, <a href="#">Performing the Required Pre-Upgrade Tasks</a>
2	Upgrade Oracle Home by upgrading Oracle WebLogic Server to 10.3.6 (if you are not using Oracle WebLogic Server 10.3.6), applying mandatory patches for Oracle Access Manager, and upgrading Oracle Access Manager binaries to 11.1.2.3.0.	See, <a href="#">Upgrading Oracle Home</a>
3	Create Oracle Mobile Security Manager (OMSM) schema, if you wish to configure Oracle Mobile Security Suite post upgrade.	See, <a href="#">Creating OMSM Schema</a>
4	Upgrade the following schemas using the Patch Set Assistant: <ul style="list-style-type: none"> <li>■ Oracle Access Manager (OAM) schema</li> <li>■ Oracle Platform Security Services (OPSS) schema</li> <li>■ Audit Services (IAU) schema</li> </ul> When you select Oracle Access Manager (OAM) schema, the OPSS and IAU schemas are also selected.	See, <a href="#">Upgrading the Database Schemas</a>
5	Upgrade Oracle Platform Security Services (OPSS). It is highly recommended that you perform this step.	See, <a href="#">Upgrading Oracle Platform Security Services</a>

**Table 8–1 (Cont.) Roadmap for Upgrading Oracle Access Management 11.1.2.x.x to**

<b>Task No.</b>	<b>Task</b>	<b>For More Information</b>
6	<p>If you are upgrading Oracle Access Management 11.1.2 to 11.1.2.3.0, you must copy the modified system or domain mbean configurations.</p> <p>If you are upgrading Oracle Access Management 11.1.2.1.0 or 11.1.2.2.0 to 11.1.2.3.0, skip this task.</p>	See, <a href="#">Copying Modified System mbean Configurations</a>
7	Restart the WebLogic Administration Server and the Access Manager Managed Server(s).	See, <a href="#">Restarting the Servers</a>
8	Undeploy the coherence#3.7.1.1 library.	See, <a href="#">Undeploying coherence#3.7.1.1 Library</a>
9	<p>Upgrade the system configuration of Oracle Access Management. This step is required for the 11.1.2.3.0 features to work.</p> <p>If you do not perform this step, the upgraded environment will still work, as compatibility mode is supported for Oracle Access Management 11.1.2.x.x upgrade.</p>	See, <a href="#">Upgrading System Configuration</a>
10	Extend the Oracle Access Management domain to include Oracle Mobile Security Suite and Policy Manager.	See, <a href="#">Extending the Oracle Access Management Domain to Include Mobile Security Suite and Policy Manager</a>
11	Start the WebLogic Administration Server and the Oracle Access Management Access Manager (Access Manager) Managed Server(s).	See, <a href="#">Starting the Servers</a>
12	Perform the required post-upgrade tasks.	See, <a href="#">Performing the Required Post-Upgrade Tasks</a>
13	Verify the Oracle Access Management upgrade.	See, <a href="#">Verifying the Oracle Access Management Upgrade</a>

## 8.2 Performing the Required Pre-Upgrade Tasks

Before you begin with the upgrade, you must complete the following prerequisites:

- Review the *Oracle Fusion Middleware System Requirements and Specifications* and *Oracle Fusion Middleware Supported System Configurations* documents to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).
- Ensure that you are using a Java Development Kit (JDK) version that is supported and certified with Oracle Identity and Access Management 11.1.2.3.0.

You can verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

---



---

**Note:** For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

---



---

- If you are upgrading Oracle Access Management 11g Release 2 (11.1.2.0, 11.1.2.1, 11.1.2.2) environments and/or if this was upgraded from 11g Release 1, then check whether the **upgrade.properties** file exists under `DOMAIN_HOME/config/fmwconfig`. If it does, then rename the file to some other name, before you start with the upgrade.
- Back up all files under the `DOMAIN_HOME/config/fmwconfig` directory.
- Oracle Access Management 11.1.2.3.0 has additional components configured in its Administration Server. Therefore, ensure that the WebLogic domain memory settings are updated to suite the machine configurations.

If the servers are started using command line, you must update the memory settings in the `setDomainEnv.sh` file. If the servers are started using Node Manager, you must update the memory settings using the WebLogic Administration console. It is recommended to do both.

To update the memory settings in the `setDomainEnv.sh` file, complete the following steps:

1. Go to the `DOMAIN_HOME/bin` directory.
2. Take a backup of file `setDomainEnv.sh` (on UNIX) or `setDomainEnv.cmd` (on Windows).
3. Open the `setDomainEnv.sh` (on UNIX) or `setDomainEnv.cmd` (on Windows) in an editor, and search for the following lines:

On UNIX:

```
# IF USER_MEM_ARGS the environment variable is set, use it to override ALL
# MEM_ARGS values

if [ "${USER_MEM_ARGS}" != "" ] ; then
MEM_ARGS="${USER_MEM_ARGS}"
export MEM_ARGS
fi
```

On Windows:

```
@REM IF USER_MEM_ARGS the environment variable is set, use it to override
ALL MEM_ARGS values

if NOT "%USER_MEM_ARGS%"==" " (
set MEM_ARGS=%USER_MEM_ARGS%
)
```

4. Add the `USER_MEM_ARGS` settings as shown in the following example:

On UNIX:

```
# IF USER_MEM_ARGS the environment variable is set, use it to override ALL
MEM_ARGS values

# Added for OAM 11.1.2.3 upgrade
USER_MEM_ARGS="-Xms4096m -Xmx4096m -XX:MaxPermSize=512m"
```

```
export USER_MEM_ARGS

if [ "${USER_MEM_ARGS}" != "" ] ; then
MEM_ARGS="${USER_MEM_ARGS}"
export MEM_ARGS
fi
```

#### On Windows:

```
@REM IF USER_MEM_ARGS the environment variable is set, use it to override
ALL MEM_ARGS values
```

```
@REM Added for OAM 11.1.2.3 upgrade
set USER_MEM_ARGS=-Xms4096m -Xmx4096m -XX:MaxPermSize=512m
```

```
if NOT "%USER_MEM_ARGS%"==" " (
set MEM_ARGS=%USER_MEM_ARGS%
)
```

#### 5. Save the changes to the file

To update the memory settings using the WebLogic Administration console, complete the following steps:

##### 1. Log in to the WebLogic Administration Console using the following URL:

```
http://host:port/console
```

##### 2. Click **Servers** on the left navigation pane.

##### 3. Select the OAM Server.

##### 4. Go to the **Server Start** tab.

##### 5. Click Arguments.

##### 6. Set the value of JVM arguments for the OAM Server. For example:

```
-Xms4096m -Xmx4096m
```

##### 7. Save the changes.

For more information about the memory requirements for Oracle Identity and Access Management, see "Memory and Space Requirements for Oracle Fusion Middleware and Oracle Identity and Access Management" in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* for 11g Release 2 (11.1.2).

- Shut down the WebLogic Administration Server and Access Manager Managed Servers. For information about stopping the servers, see [Section 24.1.9, "Stopping the Servers"](#).
- Back up the following before you proceed with the upgrade:
  - `MW_HOME` directory, including the Oracle Home directories inside Middleware Home
  - Domain Home directory
  - Oracle Access Manager schemas
  - MDS schemas
  - Audit and any other dependent schemas
  - Database instance using Oracle Recovery Manager (RMAN). For more information about backing up the database instance as repository database

backup, see Overview of the Backup Strategies in the *Fusion Middleware Administrator's Guide*.

For information about backing up the Middleware Home and schemas, see [Section 24.1.2, "Backing up the Existing Environment"](#).

## 8.3 Upgrading Oracle Home

This section describes the tasks to be completed to upgrade the existing Oracle home.

This section includes the following topics:

- [Upgrading Oracle WebLogic Server to 10.3.6](#)
- [Applying Mandatory Patches for Oracle WebLogic Server](#)
- [Upgrading Oracle Access Management Binaries to 11.1.2.3.0](#)

### 8.3.1 Upgrading Oracle WebLogic Server to 10.3.6

Oracle Identity and Access Management 11.1.2.3.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Access Management environment is using Oracle WebLogic Server 10.3.5 or any earlier version, you must upgrade it to Oracle WebLogic Server 10.3.6.

For information about upgrading Oracle WebLogic Server, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

### 8.3.2 Applying Mandatory Patches for Oracle WebLogic Server

Ensure that you apply some mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server 10.3.6, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

### 8.3.3 Upgrading Oracle Access Management Binaries to 11.1.2.3.0

Upgrade the Oracle Access Management binaries using the Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) installer. During the procedure, point the Middleware Home to your existing 11.1.1.x.x Oracle Access Management Middleware Home.

---

---

**Note:** Before upgrading the Oracle Access Management binaries to 11g Release 2 (11.1.2.3.0), you must ensure that the OPatch version in `ORACLE_HOME` and `MW_HOME/oracle_common` is 11.1.0.10.3. Different OPatch version might cause patch application failure. If you have upgraded opatch to a newer version, you will have to roll back to version 11.1.0.10.3.

---

---

For information about upgrading Oracle Access Management binaries to Oracle Access Management Access Manager 11.1.2.3.0, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 8.4 Creating OMSM Schema

If you wish to configure Oracle Mobile Security Suite (OMSS) post-upgrade, you must create Oracle Mobile Security Manager (OMSM) schema using the Repository Creation utility (RCU) 11.1.1.9.0.

For information about creating schemas using Run Repository Creation utility, see [Section 24.1.3, "Creating Database Schemas Using Repository Creation Utility"](#).

## 8.5 Upgrading the Database Schemas

After you upgrade Oracle Access Management binaries to 11.1.2.3.0, you must upgrade the following schemas by running the Patch Set Assistant (PSA):

- Oracle Access Manager (OAM) schema
- Oracle Platform Security Services (OPSS) schema
- Audit Services (IAU) schema
- Oracle Metadata Services (MDS) schema

When you run the PSA to upgrade schemas, select Oracle Access Manager (OAM) schema. This automatically selects Oracle Platform Security Services (OPSS) schema and Audit Services (IAU) schema. Once you upgrade these schemas, run the PSA again to upgrade Oracle Metadata Services (MDS) schema.

---

---

**Note:** Oracle Mobile Security Suite (OMSS) requires Oracle Metadata Services (MDS) schema. Therefore, to configure Oracle Mobile Security Suite (OMSS) post-upgrade, you must upgrade the Oracle Metadata Services (MDS) schema.

---

---

For information about upgrading schemas using Patch Set Assistant, see [Section 24.1.4, "Upgrading Schemas Using Patch Set Assistant"](#).

## 8.6 Upgrading Oracle Platform Security Services

After you upgrade schemas, it is highly recommended that you upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Access Manager to 11.1.2.3.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see [Section 24.1.7, "Upgrading Oracle Platform Security Services"](#)

## 8.7 Copying Modified System mbean Configurations

If you are upgrading Oracle Access Management 11.1.2 to Oracle Access Management 11.1.2.3.0, you must copy the modified system or domain mbean configurations from the `OAM_ORACLE_HOME` to the `DOMAIN_HOME`, after you update the Access Manager binaries to 11.1.2.3.0.

---

---

**Note:** If you are upgrading Oracle Access Management 11.1.2.2.0 or 11.1.2.1.0 to 11.1.2.3.0, skip this section.

---

---

To do this, complete the following steps:

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location `$ORACLE_HOME/common/bin`:

On UNIX: `wlst.sh`

On Windows: `wlst.cmd`

2. Run the following command:

```
copyMbeanXmlFiles('DOMAIN_HOME', 'OAM_ORACLE_HOME')
```

In this command, `DOMAIN_HOME` is the absolute path to the Access Manager WebLogic domain, and `OAM_ORACLE_HOME` is the absolute path to the OAM Oracle home. The second parameter `OAM_ORACLE_HOME` is optional.

For example:

**On UNIX:**

```
copyMbeanXmlFiles('/Oracle/Middleware/user_projects/domains/base_
domain', '/Oracle/Middleware/Oracle_IDM1')
```

**On Windows:**

```
copyMbeanXmlFiles('C:\\Oracle\\Middleware\\user_projects\\domains\\base_
domain', 'C:\\Oracle\\Middleware\\Oracle_IDM1')
```

3. If the modified system or domain mbean configurations are copied successfully, the following status is displayed on the command line:

```
STATUS: SUCCESS
```

The mbean xml files have been upgraded to new version.

The original mbean xml is saved in "`<domain_directory>/output/upgrade`".

Please restart the admin and oam servers.

If the STATUS shows SUCCESS, start the WebLogic Administration Server and the Access Manager Managed Server(s).

For information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

## 8.8 Undeploying coherence#3.7.1.1 Library

After you upgrade the system configurations, you must undeploy the coherence#3.7.1.1 library, as it is not shipped with Access Manager 11.1.2.3.0. You can undeploy the coherence#3.7.1.1 library either by running the WLST command `undeploy()` or using the WebLogic Administration console.

---

---

**Note:** The deployments for any application that references this library must be stopped and deleted before you undeploy the library.

For the list of applications that reference this library, log in to the WebLogic Administration Console, navigate to **Deployments** in the **Domain Structure**, click **coherence(3.7.1.1,3.7.1.1)**, and go to the **Overview** tab. The applications that reference this library are listed at the bottom of the page.

---

---

To undeploy the coherence#3.7.1.1 library using the WLST command, complete the following steps:

1. Start the WebLogic Administration Server and the Access Manager Managed Server(s), if you have not done already.

For more information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

2. Launch the WebLogic Scripting Tool (WLST) by running the following command from the location `ORACLE_HOME/common/bin`:

On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

3. Connect to the WebLogic Administration Server by running the following command:

```
connect('wls_admin_username','wls_admin_password','t3://hostname:port')
```

In this command,

`wls_admin_username` is the username used to connect to the WebLogic Administration Server.

`wls_admin_password` is the password used to connect to the WebLogic Administration Server.

`hostname` is the host on which the WebLogic Administration Server is running.

`port` is the port of the WebLogic Administration Server.

4. Run the following command to undeploy the `coherence#3.7.1.1` library:

```
undeploy('coherence#3.7.1.1@3.7.1.1')
```

To undeploy the `coherence#3.7.1.1` library using the WebLogic Administration Console, complete the following steps:

1. Log in to the WebLogic Administration Console using the following URL:  
`http://host:port/console`
2. In the **Change Center** of the Administration Console, click **Lock & Edit**.
3. Click **Deployments** under **Domain Structure** on the left navigation pane.
4. Select **coherence(3.7.1.1,3.7.1.1)** library, and click **Delete**.
5. Click **Activate Changes**.

---

**Note:** Before you restart the servers, add the `oam_server` and `oam_admin` servers after you have upgraded coherence.

---

## 8.9 Restarting the Servers

Restart the WebLogic Administration Server and the Access Manager Managed Server(s).

For information about stopping the servers, see [Section 24.1.9, "Stopping the Servers"](#).

For information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

## 8.10 Upgrading System Configuration

For the Oracle Access Management 11.1.2.3.0 features to work, you must run the `upgradeConfig()` utility on the machine that hosts Administration Server. This utility

upgrades the system configuration and policy store of Oracle Access Management to 11.1.2.3.0.

---



---

**Note:** If you are upgrading Oracle Access Management 11.1.2.1.0 to 11.1.2.3.0, then you must do the following before running the `upgradeConfig.sh` command:

1. Go to the directory `ORACLE_HOME/common/script_handlers`.
  2. Remove all the `.class` files by running the following command:  

```
rm *.class
```
- 
- 

To upgrade the system configuration of Oracle Access Management, do the following:

1. Stop the WebLogic Administration Server and the Access Manager Managed Server(s). For more information, see [Section 24.1.9, "Stopping the Servers"](#).
2. The `upgradeConfig` command needs to be run using the IPv4 stack. Therefore, you must add the following property to the `wlst.sh` file (on UNIX) or `wlst.cmd` file (on Windows) located at `ORACLE_HOME/common/bin`:

```
-Djava.net.preferIPv4Stack=true
```

To do this, open the `wlst.sh` or `wlst.cmd` file in a text editor, add the property, and save the file.

3. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location `ORACLE_HOME/common/bin`:

On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

4. Before you run the `upgradeConfig()` command, ensure that the output of `upgradeConfig` command is captured in a log file, for review in case of upgrade issues. To do this, run the following command:

```
redirect('outputFile')
```

In this command, `outputFile` is the name of the log file.

For example:

```
redirect('wlst.log')
```

5. Run the following command in offline mode:

```
upgradeConfig("domain_home", "sysdbaUser", "sysdbaPwd",  
"oamSchemaOwner", "oamdbJdbcUrl")
```

In this command,

- `domain_home` is the absolute path to the Oracle Access Management WebLogic domain.
- `sysdbauser` is the database username having `sysdba` privileges.
- `sysdbapwd` is the password of the database user having `sysdba` privileges.
- `oamSchemaOwner` is the database username for OAM schema.
- `oamdbjdbcUrl` is the JDBC URL to connect to the Access Manager database. The JDBC URL must be in specified in the format `"jdbc:oracle:thin:@<server_host>:<server_port>/<service_name>"`.

For example:

On UNIX:

```
upgradeConfig("/Oracle/Middleware/user_projects/domains/base_domain",
"sys", "pwd", "PREFIX_OAM", "jdbc:oracle:thin:@localhost:1521/orcl")
```

On Windows:

```
upgradeConfig("C:\\Oracle\\Middleware\\user_projects\\domains\\base_
domain", "sys", "pwd", "PREFIX_OAM",
"jdbc:oracle:thin:@localhost:1521/orcl")
```

## 8.11 Extending the Oracle Access Management Domain to Include Mobile Security Suite and Policy Manager

Extend the Oracle Access Management domain to include Oracle Mobile Security Suite and Policy Manager. Using the functionality of Oracle Mobile Security Suite is optional. However, you must perform this step to enable the Policy Manager.

For more information, see [Section 24.3.1, "Extending the 11.1.2.3.0 Access Manager Domain to Include Mobile Security Suite and Policy Manager"](#).

## 8.12 Starting the Servers

Before you start the servers, restore the **.oamkeystore** file that you had backed up from the `DOMAIN_HOME/config/fmwconfig` directory before starting the upgrade.

Start the WebLogic Administration Server, Oracle Access Management Access Manager Managed Server(s), and the OMSS Server.

For more information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

## 8.13 Performing the Required Post-Upgrade Tasks

This section describes the post-upgrade tasks required to enable the features of Oracle Access Management 11.1.2.3.0. These tasks are optional.

This section includes the following topics:

- [Optional: Enabling Oracle Mobile Security Suite](#)
- [Optional: Upgrading Oracle Access Management Mobile and Service](#)
- [Optional: Upgrading Oracle Access Management Identity Federation](#)
- [Assigning Necessary Roles to Admin](#)

### 8.13.1 Optional: Enabling Oracle Mobile Security Suite

If you wish to use the functionality of Oracle Mobile Security Suite, you must enable Oracle Mobile Security Suite after extending the Oracle Access Management domain with Oracle Mobile Security Suite component.

For more information, see [Section 24.3.2, "Enabling Oracle Mobile Security Suite"](#).

### 8.13.2 Optional: Upgrading Oracle Access Management Mobile and Service

If you are using the Social Identity feature in Oracle Access Management Mobile and Service, you must update the Social Identity configuration by running the `msUpgrade()` command. To do this, complete the following steps:

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location `$ORACLE_HOME/common/bin`:

On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

2. Run the following command to update the Social Identity configuration:

`msUpgrade()`

### 8.13.3 Optional: Upgrading Oracle Access Management Identity Federation

If you have configured Oracle Access Management Identity Federation, you must upgrade Oracle Access Management Identity Federation to 11.1.2.3.0.

For more information about upgrading Oracle Access Management Identity Federation to 11.1.2.3.0, see [Section 24.3.3, "Upgrading Oracle Access Management Identity Federation"](#).

### 8.13.4 Assigning Necessary Roles to Admin

Ensure that you assign necessary roles to the global role **Admin**, by setting the role conditions as **IDM Administrators**, **Administrators**, or **OAMAdministrators**.

For more information about creating and managing global security roles, see "Create global security roles" in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* for 11g Release 1 (10.3.6).

## 8.14 Verifying the Oracle Access Management Upgrade

Verify the Oracle Access Management upgrade by accessing the Oracle Access Management Administration Console 11g Release 2 (11.1.2.3.0).

If you have enabled Oracle Mobile Security Suite (OMSS) and wish to use the functionality of OMSS, use the following URL to access the Oracle Access Management Administration Console:

`http://<oam_admin_server_host>:<oam_admin_server_port>/access`

If you have not enabled Oracle Mobile Security Suite (OMSS), use the following URL to access the Oracle Access Management Administration Console:

`http://<oam_admin_server_host>:<oam_admin_server_port>/oamconsole`

## 8.15 Troubleshooting

For the list of common issues that you might encounter during the Oracle Access Management upgrade process, and their workaround, see [Section 25.2, "Troubleshooting Oracle Access Management Upgrade Issues"](#).

For the list of known issues related to upgrade, and their workaround, see "Upgrade and Migration Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes for Identity Management*.

---

---

# Upgrading Oracle Adaptive Access Manager 11g Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade Oracle Adaptive Access Manager 11g Release 2 (11.1.2.1.0) and 11g Release 2 (11.1.2) environments to Oracle Adaptive Access Manager 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

---

---

**Note:** This chapter refers to Oracle Adaptive Access Manager 11g Release 2 (11.1.2) and 11g Release 2 (11.1.2.1.0) environments as 11.1.2.x.x.

---

---

This chapter includes the following sections:

- [Section 9.1, "Upgrade Roadmap for Oracle Adaptive Access Manager"](#)
- [Section 9.2, "Performing the Required Pre-Upgrade Tasks"](#)
- [Section 9.3, "Shutting Down Administration Server and Managed Servers"](#)
- [Section 9.4, "Backing Up Oracle Adaptive Access Manager 11.1.2.x.x"](#)
- [Section 9.5, "Optional: Upgrading Oracle WebLogic Server"](#)
- [Section 9.6, "Updating Oracle Adaptive Access Manager Binaries to 11.1.2.3.0"](#)
- [Section 9.7, "Upgrading OAAM, MDS, IAU, and OPSS Schemas"](#)
- [Section 9.8, "Upgrading Oracle Platform Security Services"](#)
- [Section 9.9, "Starting the Servers"](#)
- [Section 9.10, "Redeploying Oracle Adaptive Access Manager Applications"](#)
- [Section 9.11, "Restarting the Servers"](#)
- [Section 9.12, "Verifying the Oracle Adaptive Access Manager Upgrade"](#)

- [Section 9.13, "Troubleshooting"](#)

## 9.1 Upgrade Roadmap for Oracle Adaptive Access Manager

---

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Adaptive Access Manager upgrade may not be successful.

---

[Table 9–1](#) lists the steps to upgrade Oracle Adaptive Access Manager.

**Table 9–1 Roadmap for Upgrading Oracle Adaptive Access Manager 11.1.2.x.x to 11.1.2.3.0.**

SI No	Task	For More Information
1	Perform the required pre-upgrade tasks before you start with the upgrade process.	See, <a href="#">Performing the Required Pre-Upgrade Tasks</a>
2	Stop the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Server(s) before you start the upgrade process.	See, <a href="#">Shutting Down Administration Server and Managed Servers</a>
3	Back up your existing Oracle Adaptive Access Manager 11.1.2.x.x Environment.	See, <a href="#">Backing Up Oracle Adaptive Access Manager 11.1.2.x.x</a>
4	Upgrade Oracle WebLogic Server to 10.3.6, if necessary.	See, <a href="#">Optional: Upgrading Oracle WebLogic Server</a>
5	Update the Oracle Adaptive Access Manager 11.1.2.x.x binaries to 11.1.2.3.0.	See, <a href="#">Updating Oracle Adaptive Access Manager Binaries to 11.1.2.3.0</a>
6	Upgrade the OAAM, MDS, IAU, and OPSS Schemas using Patch Set Assistant.	See, <a href="#">Upgrading OAAM, MDS, IAU, and OPSS Schemas</a>
7	Upgrade the Oracle Platform Security Services.	See, <a href="#">Upgrading Oracle Platform Security Services</a>
8	Start the WebLogic Administration Server and Oracle Adaptive Access Manager Managed Server(s).	See, <a href="#">Starting the Servers</a>
9	If you are upgrading Oracle Adaptive Access Manager 11.1.2 to 11.1.2.3.0, you must redeploy the applications after you start the servers.	See, <a href="#">Redeploying Oracle Adaptive Access Manager Applications</a>
10	Restart the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Server(s).	See, <a href="#">Restarting the Servers</a>
11	Verify the Oracle Adaptive Access Manager upgrade.	See, <a href="#">Verifying the Oracle Adaptive Access Manager Upgrade</a>

## 9.2 Performing the Required Pre-Upgrade Tasks

Before you begin with the upgrade, you must complete the following prerequisites:

- Review the *Oracle Fusion Middleware System Requirements and Specifications* and *Oracle Fusion Middleware Supported System Configurations* documents to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).
- Ensure that you are using a Java Development Kit (JDK) version that is supported and certified with Oracle Identity and Access Management 11.1.2.3.0.

You can verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

---

**Note:** For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

---

### 9.3 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Servers.

For more information about stopping the WebLogic Administration Server and the Managed Servers, see [Section 24.1.9, "Stopping the Servers"](#).

### 9.4 Backing Up Oracle Adaptive Access Manager 11.1.2.x.x

You must back up your Oracle Adaptive Access Manager 11.1.2.x.x environment before you upgrade to Oracle Adaptive Access Manager 11.1.2.3.0.

After stopping the servers, you must back up the following:

- *MW\_HOME* directory, including the Oracle Home directories inside Middleware Home
- Oracle Adaptive Access Manager Domain Home directory
- Oracle Adaptive Access Manager schema
- IAU schema, if it is part of any of your Oracle Adaptive Access Manager 11.1.2.x.x schema
- MDS schema

For more information about backing up the Middleware Home and the schemas, see [Section 24.1.2, "Backing up the Existing Environment"](#).

### 9.5 Optional: Upgrading Oracle WebLogic Server

Oracle Identity and Access Management 11.1.2.3.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Adaptive Access Manager environment is using Oracle WebLogic Server 10.3.5 or any earlier version, you must upgrade it to Oracle WebLogic Server 10.3.6.

---

---

**Note:** If you are already using Oracle WebLogic Server 10.3.6, ensure that you apply the mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server 10.3.6, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

---

---

For information about upgrading Oracle WebLogic Server to 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

## 9.6 Updating Oracle Adaptive Access Manager Binaries to 11.1.2.3.0

To update the Oracle Adaptive Access Manager 11.1.2.x.x binaries to 11.1.2.3.0, you must use the Oracle Identity and Access Management 11.1.2.3.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Middleware Home. Your Oracle Home is upgraded from 11.1.2.x.x to 11.1.2.3.0.

For information about updating the Oracle Adaptive Access Manager binaries to 11.1.2.3.0, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 9.7 Upgrading OAAM, MDS, IAU, and OPSS Schemas

You must upgrade the following schemas using Patch Set Assistant:

- OAAM schema
- MDS schema
- OPSS schema
- IAU schema (You must upgrade Audit schema (IAU) only if it is part of your 11.1.2.x.x schemas)

---

---

**Note:** When upgrading schemas using Patch Set Assistant, you must select **OAAM** or **OAAM\_PARTN** as appropriate, and provide details on all screens to complete the upgrade.

---

---

For information about upgrading schemas using Patch Set Assistant, see [Section 24.1.4, "Upgrading Schemas Using Patch Set Assistant"](#).

## 9.8 Upgrading Oracle Platform Security Services

After you upgrade schemas, you must upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Adaptive Access Manager to 11.1.2.3.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see [Section 24.1.7, "Upgrading Oracle Platform Security Services"](#).

## 9.9 Starting the Servers

Start the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Server(s).

For information about starting the WebLogic Administration Server and the Managed Servers, see [Section 24.1.8, "Starting the Servers"](#).

## 9.10 Redeploying Oracle Adaptive Access Manager Applications

After you start the servers, you must redeploy your Oracle Adaptive Access Manager applications on the Oracle Adaptive Access Manager 11.1.2.3.0 servers.

You can redeploy the application using command line or using the WebLogic Administration console. Complete the following steps described in one of the following sections to redeploy applications:

- [Redeploying Applications Using Command Line](#)
- [Redeploying Applications Using WebLogic Administration Console](#)

### Redeploying Applications Using Command Line

To redeploy applications on Oracle Adaptive Access Manager 11.1.2.3.0 servers using command line, do the following:

1. Launch the WebLogic Scripting Tool (WLST) by running the following command from the location `IAM_HOME/common/bin`:

On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

2. Connect to the Administration Server using the following command:

```
connect('weblogic-username', 'weblogic-password', 'weblogic-url')
```

For example:

```
connect('wlsuser', 'wlspassword', 'localhost:7001')
```

3. Stop the applications by running the following commands:

- `stopApplication('oaam_admin')`
- `stopApplication('oaam_server')`

---

**Note:** If you have Oracle Adaptive Access Manager Offline Server in your setup, run the `stopApplication()` command to stop 'oaam\_offline' too.

---

4. Redeploy the applications by running the following commands:

- `redeploy('oracle.oaam.extensions')`
- `redeploy('oaam_admin')`
- `redeploy('oaam_server')`

---

---

**Note:** If you have Oracle Adaptive Access Manager Offline Server in your setup, run the `redeploy()` command to redeploy applications on 'oaam\_offline' too.

---

---

5. Start the applications by running the following commands:

- `startApplication('oaam_admin')`
- `startApplication('oaam_server')`

---

---

**Note:** If you have Oracle Adaptive Access Manager Offline Server in your setup, run the `startApplication()` command to stop 'oaam\_offline' too.

---

---

6. Exit the WLST console using the `exit()` command.

For more information about using the `redeploy` command, see "redeploy" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

### Redeploying Applications Using WebLogic Administration Console

To redeploy applications on Oracle Adaptive Access Manager 11.1.2.3.0 servers using the WebLogic Administration console, do the following

1. Log in to the WebLogic Administration console using the following URL:  
`http://admin_host:admin_port/console`
2. Go to the **Deployments** tab.
3. Click **lock and Edit** on the left panel.
4. Stop the `oaam_admin` and `oaam_server` applications. If `oaam_offline` is available in your environment, stop it too.
5. Select **oaam\_extension\_library**.
6. Click **Update**.
7. The console shows the location of the `.ear` file. Confirm if that is the correct location of the `.ear` file that you wish to deploy; Otherwise, change the location.
8. Click **Finish**.
9. When the deployment is completed, click **Release configuration**.
10. Repeat the procedure for `OAM_ADMIN`, `OAM_SERVER`, and `OAM_OFFLINE` as applicable.

## 9.11 Restarting the Servers

After you redeploy the applications, restart the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Server(s).

---

**Note:** After redeploying the applications, when you stop the servers for the first time, the following exception might be displayed:

```
<Error> <oracle.oaam> <BEA-000000> <Exception
writing monitor data:
java.lang.IllegalStateException: Attempting to execute an operation
on a closed EntityManagerFactory. at
org.eclipse.persistence.internal.jpa.EntityManagerFactoryDelegate.v
erifyOpen(EntityManagerFactoryDelegate.java:305) at
org.eclipse.persistence.internal.jpa.EntityManagerFactoryDelegate.c
reateEntityManagerImpl(EntityManagerFactoryDelegate.java:276) at
org.eclipse.persistence.internal.jpa.EntityManagerFactoryImpl.creat
eEntityManagerImpl(EntityManagerFactoryImpl.java:294) at
org.eclipse.persistence.internal.jpa.EntityManagerFactoryImpl.creat
eEntityManager(EntityManagerFactoryImpl.java:272) at
com.bharosa.common.toplink.TopLink11gDBMgr.createSession(TopLink11g
DBMgr.java: 313) at
com.bharosa.common.db.BharosaDBMgr.beginSession(BharosaDBMgr.java:1
66) at
com.bharosa.common.dataaccess.DataAccessMgr.beginSession(DataAccess
Mgr.java:95) at
java.lang.Thread.run(Thread.java:662) >
<Nov 24, 2014 2:43:22 AM PST> <Error> <oracle.oaam> <BEA-000000>
<Session not found in endSession for database default.
This is not okay. refCount=null java.lang.Throwable at
com.bharosa.common.db.BharosaDBMgr.endSession(BharosaDBMgr.java:245
) at
com.bharosa.common.dataaccess.DataAccessMgr.endSession(DataAccessMg
r.java:137) at
com.bharosa.common.monitoring.Monitor.run(Monitor.java:113) at
java.lang.Thread.run(Thread.java:662) >
```

This is a one time exception, seen the first time you stop the servers after upgrade. You can ignore this exception.

---

For information about stopping the servers, see [Section 24.1.9, "Stopping the Servers"](#).

For information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

## 9.12 Verifying the Oracle Adaptive Access Manager Upgrade

To verify the Oracle Adaptive Access Manager upgrade, do the following:

- Verify the log file at the location *MW\_HOME/oracle\_common/upgrade/logs* to ensure that the upgrade was successful.
- Verify the version of the OAAM schema by connecting to the OAAM schema as *OAAM\_schema\_user*, and running the following query:

```
select version,status,upgraded from schema_version_registry where
owner=<OAAM_SCHEMA_NAME>;
```

Ensure that the version number is 11.1.2.3.0.

- Log in to the OAAM Administration console using the following URL:

```
http://oaam.example.com:<admin_port>/oaam_admin
```

Verify if the version number of Oracle Adaptive Access Manager is 11.1.2.3.0.

## 9.13 Troubleshooting

For the list of known issues related to upgrade, and their workaround, see "Upgrade and Migration Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes for Identity Management*.

---

---

## Upgrading Oracle Identity Manager 11g Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade Oracle Identity Manager 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0), and 11g Release 2 (11.1.2) environments to Oracle Identity Manager 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

---

---

**Note:** This chapter refers to Oracle Identity Manager 11g Release 2 (11.1.2), 11g Release 2 (11.1.2.1.0), and 11g Release 2 (11.1.2.2.0) environments as 11.1.2.x.x.

---

---

This chapter includes the following sections:

- [Upgrade Roadmap for Oracle Identity Manager](#)
- [Performing the Required Pre-Upgrade Tasks](#)
- [Upgrading Oracle Home](#)
- [Creating Necessary Schemas and Upgrading Existing Schemas](#)
- [Upgrading Oracle Identity Manager Middle Tier](#)
- [Upgrading Other Oracle Identity Manager Installed Components](#)
- [Performing the Required Post-Upgrade Tasks](#)
- [Verifying the Oracle Identity Manager Upgrade](#)
- [Troubleshooting](#)

### 10.1 Upgrade Roadmap for Oracle Identity Manager

The procedure for upgrading Oracle Identity Manager 11.1.2.x.x to 11.1.2.3.0 involves the following high-level steps

1. **Performing the Required Pre-Upgrade Tasks:** This step involves the necessary pre-upgrade tasks like reviewing system requirements and certification, generating the pre-upgrade report, analyzing the report and performing the necessary pre-upgrade tasks described in the report, backing up the existing 11.1.2.x.x environment.
2. **Upgrading the Oracle Home:** This step involves tasks like upgrading Oracle WebLogic Server to 10.3.6, upgrading Oracle SOA Suite to 11.1.1.9.0, and upgrading Oracle Identity Manager to 11.1.2.3.0.
3. **Creating Necessary Schemas and Upgrading the Existing Schemas:** This step involves tasks like creating Oracle BI Publisher (BIP) schema using Repository Creation Utility 11.1.2.3.0, and upgrading the existing schemas using the Patch Set Assistant.
4. **Upgrading Oracle Identity Manager Middle Tier:** This step involves upgrading Oracle Identity Manager middle tier.
5. **Upgrading Other Oracle Identity Manager Installed Components:** This step involves tasks like upgrading Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manger to 11.1.2.3.0.
6. **Performing the Required Post-Upgrade Tasks:** This step involves any post-upgrade tasks, and the steps to verify the upgrade.

Table 10–1 lists the steps to upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.3.0.

**Table 10–1 Roadmap for Upgrading Oracle Identity Manager 11.1.2.x.x to 11.1.2.3.0**

SI No	Task	For More Information
1	Complete the following pre-upgrade tasks: <ol style="list-style-type: none"> <li>1. Review the news features of Oracle Identity Manager 11.1.2.3.0.</li> <li>2. Review system requirements and certifications.</li> <li>3. Ensure that you are using a supported JDK version.</li> <li>4. Review the customizations that are lost or overwritten as part of the upgrade process.</li> <li>5. Generate the pre-upgrade report, analyze the information provided in the report, and perform the necessary tasks described in the report before you proceed with the upgrade process.</li> <li>6. Stop all the servers. This includes the Node Manager, WebLogic Administration Server, SOA Managed Server(s), and Oracle Identity Manager Managed Server(s).</li> <li>7. Back up your existing Oracle Identity Manager 11.1.2.x.x environment.</li> </ol>	See, <a href="#">Performing the Required Pre-Upgrade Tasks</a>

**Table 10–1 (Cont.) Roadmap for Upgrading Oracle Identity Manager 11.1.2.x.x to**

SI No	Task	For More Information
2	Upgrade the Oracle Home by completing the following tasks: <ol style="list-style-type: none"> <li>1. Upgrade Oracle WebLogic Server to 10.3.6 if you are using a previous version.</li> <li>2. Upgrade Oracle SOA suite to 11g Release 1 (11.1.1.9.0).</li> <li>3. Upgrade Oracle Identity Manager binaries to 11.1.2.3.0.</li> </ol>	See, <a href="#">Upgrading Oracle Home</a>
3	Create the Oracle BI Publisher (BIP) schema using the Repository Creation Utility (RCU), and upgrade your existing database schemas using the Patch Set Assistant (PSA).	See, <a href="#">Creating Necessary Schemas and Upgrading Existing Schemas</a>
4	Upgrade the Oracle Identity Manager middle tier. This is done by running the OIM middle tier upgrade utility <code>OIMUpgrade.sh</code> or <code>OIMUpgrade.bat</code> in offline and online mode.	See, <a href="#">Upgrading Oracle Identity Manager Middle Tier</a>
5	Upgrade other Oracle Identity Manager installed components like Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager to 11.1.2.3.0.	See, <a href="#">Upgrading Other Oracle Identity Manager Installed Components</a>
6	Complete the required post-upgrade tasks.	See, <a href="#">Performing the Required Post-Upgrade Tasks</a>
7	Verify the upgraded environment.	See, <a href="#">Verifying the Oracle Identity Manager Upgrade</a>

## 10.2 Performing the Required Pre-Upgrade Tasks

This section describes all the pre-upgrade steps that you must complete before you start upgrading the Oracle Identity Manager 11.1.2.x.x environment. This section includes the following topics:

- [Feature Comparison](#)
- [Reviewing System Requirements and Certification](#)
- [Ensuring that you are Using a Certified JDK Version](#)
- [Reviewing the Customizations that are Lost or Overwritten as Part of Upgrade](#)
- [Generating and Analyzing the Pre-Upgrade Report](#)
- [Backing Up Oracle Identity Manager 11.1.2.x.x Environment](#)
- [Shutting Down Node Manager, Administration Server and Managed Server\(s\)](#)

### 10.2.1 Feature Comparison

[Table 10–2](#) lists the key differences in functionality between Oracle Identity Manager 11g Release 2 (11.1.2.x.x) and Oracle Identity Manager 11g Release 2 (11.1.2.3.0).

**Table 10–2 Features Comparison**

Oracle Identity Manager 11.1.2.x.x	Oracle Identity Manager 11.1.2.3.0
<p>Oracle Identity Manager 11.1.2.2.0 uses Skyros skin.</p>	<p>Oracle Identity Manager 11.1.2.3.0 uses Alta skin which is business friendly (mobile, cloud). Oracle Identity Manager 11.1.2.3.0 has new <b>Home</b> page, new <b>My Profile</b> page with user friendly Inbox.</p>
<p>In Oracle Identity Manager 11.1.2, the Access Catalog was introduced to provide meaningful and contextual information to end users during the request and access review.</p>	<p>Most of the UI customizations need to be redone post upgrade, to match the look and feel of 11.1.2.3.0.</p>
<p>In Oracle Identity Manager 11.1.2.1.0, certification was introduced and the workflow supported one level of access in each phase.</p>	<p>Oracle Identity Manager 11.1.2.3.0 has a new advanced search catalog, where UDFs that are marked as searchable will automatically be part of advance search form.</p>
<p>Certification workflow in 11.1.2.2.0 enables business to define more robust processes for compliance, enabling more granular oversight of "who has access to what". Certification reviews can mirror access request workflow, where they can be reviewed or approved by multiple sets of business and IT owners before they are deemed complete in each phase. This ensures improved visibility of user access privileges, and all review decisions are captured in a comprehensive audit trail that is recorded live during the certification as well as in reports.</p>	<p>You can also customize the search form. Attributes can be used to search catalog items. The catalog includes enhanced pagination and categories to simplify resource searches.</p>
<p>Till 11.1.2.2.0, BI Publisher was a separate standalone Managed Server.</p>	<p>Certification feature of Oracle Identity Manager 11.1.2.3.0 uses the Alta UI and has been enhanced to provide inline SoD violation checks.</p>
<p>Till 11.1.2.2.0, BI Publisher was a separate standalone Managed Server.</p>	<p>Oracle Identity Manager 11.1.2.3.0 has embedded BI Publisher, and therefore all BI reports are embedded in OIM.</p> <p>A business user now can launch a custom report from within OIM Self Service Console.</p>

**Table 10–2 (Cont.) Features Comparison**

Oracle Identity Manager 11.1.2.x.x	Oracle Identity Manager 11.1.2.3.0
<p>Oracle Identity Manager 11.1.2.0.0 had to be integrated with Oracle Identity Analytics (OIA) to leverage the advanced access review capabilities.</p>	<p>OIA functionality is now ported into Oracle Identity Governance (OIG). Customers can define and manage identity audit policies based on IDA rules. Customers can define owners and remediators for a policy, which can be a specific user, a list of users or an OIM role.</p>
<p>In Oracle Identity Manager 11.1.2.1.0 and 11.1.2.2.0, the advanced access review capabilities of OIA were converged into OIM to provide a complete identity governance platform that enables an enterprise to do enterprise grade access request, provisioning, and access review from a single product.</p>	<p>Customers can use preventive and detective scan capabilities which can create actionable policy violations.</p>
<p>Till Oracle Identity Manager 11.1.2.2.0, policies were implemented and customized using OIM plug-in and pre-pop adapters implemented via plug-in framework, which required writing custom java code to extend and customize OOTB policies.</p>	<p>Oracle Identity Manager 11.1.2.3.0 has comprehensive role lifecycle management and workflow approval capabilities with direct involvement from business, featuring a business friendly UI.</p>
<p>The existing 11.1.2.x.x certification feature provides certifier selection based on User Manager, Organization Manager, Catalog Owner, and Selected User.</p>	<p>It also includes detailed Role Analytics to aid with the composition and modifications of roles.</p>
<p>In Oracle Identity Manager 11.1.2.x.x, the concept of request profile was introduced. You could draft and save the request. Request has to go through two levels of approval process.</p>	<p>Oracle Identity Manager 11.1.2.3.0 introduces declarative policies that enable you to define and configure various policy types that are evaluated at run time. Policy is configured via a UI/API rather than customized via Java plug-in or pre-pop adapter.</p>
<p>In Oracle Identity Manager 11.1.2.x.x, the concept of request profile was introduced. You could draft and save the request. Request has to go through two levels of approval process.</p>	<p>Oracle Identity Manager 11.1.2.3.0 introduces additional certifier selection where role can be used to define certifiers. All members of a certifier role can see the certification in their inbox, but the first member who claims the certification will be the primary reviewer for that certification.</p>
<p>Till Oracle Identity Manager 11.1.2.2.0, only out-of-the box admin roles were available.</p>	<p>Oracle Identity Manager 11.1.2.3.0 includes a number of enhancements to the request workflow.</p>
<p><b>10.2.2 Reviewing System Requirements and Certification</b></p>	<p>Temporal grants allow the requester to specify the start and end date (grant duration) of the role, account, and entitlements at the time of assignment.</p>
<p>Before you start the upgrade process, review the <i>Oracle Fusion Middleware System Requirements and Specifications</i> and <i>Oracle Fusion Middleware Supported System</i></p>	<p>Administrators can configure approvals by creating workflow policy rules instead of approval policies.</p>
<p>Upgrading Oracle Identity Manager 11g Release 2 (11.1.2.x.x) Environments <b>10-5</b></p>	<p>It also supports role requests (create, modify, delete etc). In 11.1.2.3.0, enabling SOA is optional.</p>
<p>Till Oracle Identity Manager 11.1.2.2.0, only out-of-the box admin roles were available.</p>	<p>Oracle Identity Manager 11.1.2.3.0 provides a fine grained authorization engine to help you create various admin roles. For example, by using attributes to define membership, you can restrict an administrator to managing home organization members only.</p>

## 10.2.2 Reviewing System Requirements and Certification

Before you start the upgrade process, review the *Oracle Fusion Middleware System Requirements and Specifications* and *Oracle Fusion Middleware Supported System*

*Configurations* documents to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).

### 10.2.3 Ensuring that you are Using a Certified JDK Version

Ensure that you are using a Java Development Kit (JDK) version that is supported and certified with Oracle Identity and Access Management 11.1.2.3.0.

You can verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

---

---

**Note:** For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

---

---

### 10.2.4 Reviewing the Customizations that are Lost or Overwritten as Part of Upgrade

This section lists the customizations that will be lost or overwritten as part of the upgrade process.

The following customizations will be lost or overwritten as part of the Oracle Identity Manager upgrade process:

- The configuration files like `web.xml` that are directly manipulated for changing the session time out will be overwritten as part of the binary upgrade.
- The custom JARs included in the OIM Home will be lost as part of the binary upgrade.
- Oracle Identity Manager Design Console configuration settings will be lost as part of the binary upgrade.
- Oracle Identity Manager Remote Manager configuration settings will be lost as part of the binary upgrade.
- UI war file `oracle.iam.ui.custom-dev-starter-pack.war` that is used for custom UI will be lost as part of the binary upgrade.
- Customization done to Email Validation Pattern will be overwritten as part of the upgrade process.
- The following scripts will be modified as part of the Oracle Identity Manager middle tier upgrade offline.
  - Startup scripts - `startWebLogic.sh` and `startManagedWebLogic.sh` located at `DOMAIN_HOME/bin/` (on UNIX), `startWebLogic.cmd` and `startManagedWebLogic.cmd` located at `DOMAIN_HOME\bin\` (on Windows)
  - Domain environment script - `setDomainEnv.sh` located at `DOMAIN_HOME/bin/` (on UNIX), `setDomainEnv.bat` located at `DOMAIN_HOME\bin\` (on Windows)
  - Unprotected Metadata files

For the list of protected metadata files for which the customizations will be retained after upgrade, see [Section 24.2.1, "Protected Metadata Files for Which Customization will be Retained After Upgrade"](#).

Any manual edits done to these scripts will be overwritten. Therefore, you must revisit these after middle tier upgrade offline.

- If you have SSL configured environment, the file `ORACLE_HOME\designconsole\config\xl.policy` will be overwritten as part of the Oracle Identity Manager binary upgrade. Therefore, backup the `xl.policy` file if you have customized it, before you begin with the upgrade process.

## 10.2.5 Generating and Analyzing the Pre-Upgrade Report

You must run the pre-upgrade report utility before you begin the upgrade process, and address all the issues listed as part of this report with the solution provided in the report. The pre-upgrade report utility analyzes your existing Oracle Identity Manager 11.1.2.x.x environment, and provides information about the mandatory prerequisites that you must complete before you upgrade the existing Oracle Identity Manager environment.

The information in the pre-upgrade report include challenge questions localization, authorization feature data upgrade, event handlers that are affected by upgrade, mandatory database components or settings, cyclic groups in LDAP that need to be removed, certification records processed during the upgrade, and the potential application instance creation issues.

For information about generating the pre-upgrade report, and analyzing it, see [Section 24.2.2, "Generating and Analyzing Pre-Upgrade Report for Oracle Identity Manager"](#).

---

---

**Note:** Run this report until no pending issues are listed in the report.

It is important to address all the issues listed in the pre-upgrade report, before you can proceed with the upgrade, as upgrade might fail if the issues are not fixed.

---

---

## 10.2.6 Shutting Down Node Manager, Administration Server and Managed Server(s)

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Oracle Identity Manager Managed Server(s), SOA Managed Server(s), WebLogic Administration Server, and the Node Manager.

For information about stopping the WebLogic Administration Server, Managed Server(s), and the Node Manager, see [Section 24.1.9, "Stopping the Servers"](#).

---

---

**Note:** If you are upgrading highly available environment, you must shut down the servers on all of the hosts.

---

---

## 10.2.7 Backing Up Oracle Identity Manager 11.1.2.x.x Environment

You must back up your existing Oracle Identity Manager 11.1.2.x.x environment before you upgrade to Oracle Identity Manager 11.1.2.3.0.

After stopping the servers, back up the following:

- *MW\_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Identity Manager schema
- MDS schema
- ORASDPM schema
- SOAINFRA schemas
- OPSS schema

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

---

---

**Note:** If you are upgrading highly available environment, you must back up the Oracle Home directories and the domain home directories on all of the hosts.

---

---

### 10.2.8 Disabling OIM Materialized-View Creation

Before you upgrade the OIM schemas, disable the materialized view 'OIM\_RECON\_CHANGES\_BY\_RES\_MV' view. This view is created by the `oim_mview_recon_changes_by_res.sql` script, and is used for the “Fine Grained Exception by Resource” report.

To disable the view creation:

1. Stop the Oracle Fusion Middleware Patch Set Assistant.
2. Comment the reference to `oim_mview_recon_changes_by_res.sql` from the `sequence.properties` file. The `sequence.properties` file is located at: `OIM_ORACLE_HOME/server/db/oim/oracle/StoredProcedures/MaterializedViews`.
3. Start the Oracle Fusion Middleware Patch Set Assistant.

After the OIM schema upgrade is complete, restore the reference to `oim_mview_recon_changes_by_res.sql` from the `sequence.properties` file.

## 10.3 Upgrading Oracle Home

This section describes the tasks to be completed to upgrade the existing Oracle home.

---

---

**Note:** Before you begin with the upgrade process, make sure that you have read and write permission to the domain including the `/security/SerializedSystemIni.dat` file.

---

---

This section includes the following topics:

- [Upgrading Oracle WebLogic Server to 10.3.6](#)
- [Upgrading Oracle SOA Suite to 11.1.1.9.0](#)
- [Upgrading Oracle Identity Manager Binaries to 11.1.2.3.0](#)

### 10.3.1 Upgrading Oracle WebLogic Server to 10.3.6

Oracle Identity and Access Management 11.1.2.3.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Identity Manager environment is using Oracle WebLogic Server 10.3.5 or the earlier version, you must upgrade Oracle WebLogic Server to 10.3.6.

---

---

**Note:** If you are already using Oracle WebLogic Server 10.3.6, ensure that you apply the mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server 10.3.6, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

---

---

For information about upgrading Oracle WebLogic Server to 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

### 10.3.2 Upgrading Oracle SOA Suite to 11.1.1.9.0

Oracle Identity Manager 11.1.2.3.0 is certified with Oracle SOA Suite 11.1.1.9.0. Therefore, you must upgrade Oracle SOA Suite to 11.1.1.9.0 if you are using any earlier version of Oracle SOA Suite.

For information about upgrading Oracle SOA Suite, see [Section 24.2.3, "Upgrading Oracle SOA Suite to 11g Release 1 \(11.1.1.9.0\)"](#).

### 10.3.3 Upgrading Oracle Identity Manager Binaries to 11.1.2.3.0

You must upgrade the Oracle Identity Manager 11.1.2.x.x binaries Oracle Identity Manager 11.1.2.3.0 using the Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) Installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Middleware Home. This upgrades the Oracle Identity Manager binaries 11.1.2.3.0.

---

---

**Note:** ■ Before upgrading the Oracle Identity Manager binaries to 11g Release 2 (11.1.2.3.0), you must ensure that the OPatch version in `ORACLE_HOME` and `MW_HOME/oracle_common` is 11.1.0.10.3. Different OPatch version might cause patch application failure. If you have upgraded opatch to a newer version, you will have to roll back to version 11.1.0.10.3.

---

---

For information about updating Oracle Identity Manager binaries to 11.1.2.3.0, see [Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)](#).

After the binary upgrade, check the installer logs at the following location:

- On UNIX: `ORACLE_INVENTORY_LOCATION/logs`

To find the location of the Oracle Inventory directory on UNIX, check the file `ORACLE_HOME/oraInst.loc`.

- On Windows: `ORACLE_INVENTORY_LOCATION\logs`  
The default location of the Oracle Inventory Directory on Windows is `C:\Program Files\Oracle\Inventory\logs`.

The following install log files are written to the log directory:

- `installDATE-TIME_STAMP.log`
- `installDATE-TIME_STAMP.out`
- `installActionsDATE-TIME_STAMP.log`
- `installProfileDATE-TIME_STAMP.log`
- `oraInstallDATE-TIME_STAMP.err`
- `oraInstallDATE-TIME_STAMP.log`

## 10.4 Creating Necessary Schemas and Upgrading Existing Schemas

You must create new Oracle BI Publisher schema by running the Repository Creation Utility (RCU). Also, you must upgrade the existing database schemas using the Patch Set Assistant (PSA). To do this, complete the following steps:

- [Creating Oracle BI Publisher Schema](#)
- [Upgrading Existing Schemas](#)

### 10.4.1 Creating Oracle BI Publisher Schema

You must create Oracle BI Publisher schema 11.1.1.9.0 using the Repository Creation Utility (RCU) 11.1.2.3.0. For information about creating schemas using RCU, see [Section 24.1.3, "Creating Database Schemas Using Repository Creation Utility"](#).

---

---

**Note:** When you create schema using Repository Creation Utility, select only **Business Intelligence Platform (BIPLATFORM)** under **Oracle Business Intelligence** on the **Select Components** screen.

Do not select any other schema.

---

---

### 10.4.2 Upgrading Existing Schemas

After you update Oracle Identity Manager binaries to 11.1.2.3.0, you must upgrade the following schemas using Patch Set Assistant (PSA):

- Oracle Platform Security Services (OPSS) schema
- Metadata Services (MDS) schema
- Oracle Identity Manager (OIM) schema
- ORASDPM schema
- SOA Infrastructure (SOAINFRA) schema

---

**Note:** If the you Oracle Identity Manager database access policies, you must complete the following steps before you upgrade the existing schemas:

1. Open the `oim_upg_R2PS2_R2PS3_common_policy_engine.sql` file located at `OIM_HOME/server/db/oim/oracle/Upgrade/oim11gR2PS2_2_R2PS3`, in a text editor.
  2. Replace the line# 280:
 

```
EXECUTE IMMEDIATE sqlstr USING v_pol_owner(idx);
```

 with
 

```
EXECUTE IMMEDIATE sqlstr USING v_pol_owner_type(idx);
```
  3. Save the modified file.
- 

When you select the Oracle Identity Manager schema on the PSA screen, it automatically selects all dependent schemas and upgrades them too.

For information about upgrading schemas using the Patch Set Assistant, see [Upgrading Schemas Using Patch Set Assistant](#).

After you upgrade schemas, verify the upgrade by checking the version numbers of the schemas as described in [Version Numbers After Upgrading Schemas](#).

### Version Numbers After Upgrading Schemas

Connect to oim schema as `oim_schema_user`, and run the following query:

```
select version,status,upgraded from schema_version_registry where
owner=<SCHEMA_NAME>;
```

Ensure that the version numbers are upgraded, as listed in [Table 10–3](#):

**Table 10–3 Component Version Numbers After Upgrading the Schemas**

Component	Version No.
OPSS	11.1.1.9.0
MDS	11.1.1.9.0
OIM	11.1.2.3.0
ORASDPM	11.1.1.9.0
SOAINFRA	11.1.1.9.0

## 10.5 Upgrading Oracle Identity Manager Middle Tier

To upgrade Oracle Identity Manager middle tier, you must run the middle tier upgrade utility `OIMUpgrade` in offline and online mode. For more information about upgrading the Oracle Identity Manager middle tier, see [Section 24.2.4, "Upgrading Oracle Identity Manager Middle Tier"](#).

## 10.6 Upgrading Other Oracle Identity Manager Installed Components

After you upgrade the Oracle Identity Manager middle tier, you must upgrade the other Oracle Identity Manager installed components like Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager to 11.1.2.3.0.

For more information about upgrading Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager, see [Section 24.2.5, "Upgrading Other Oracle Identity Manager Installed Components"](#).

## 10.7 Performing the Required Post-Upgrade Tasks

After you upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.3.0, you must perform the following post-upgrade tasks described in [Section 24.2.6, "Performing Oracle Identity Manager Post-Upgrade Tasks"](#):

- [Enabling Oracle BI Publisher](#)
- [Reviewing Performance Tuning Recommendations](#)
- [Creating PeopleSoft Enterprise HRMS Reconciliation Profile](#)
- [Reviewing OIM Data Purge Job Parameters](#)
- [Reconfiguring Lookup Based UDF Field](#)
- [Reviewing Connector Certification](#)
- [Verifying the Functionality of Connectors](#)
- [Rebuilding the Indexes of Oracle Identity Manager Table to Change to Reverse Type](#)
- [Reviewing System Property](#)
- [Updating the URI of the Human Task Service Component with Oracle HTTP Server Details](#)
- [Migrating Approval Policies to Approval Workflow Rules](#)
- [Disabling Oracle SOA Suite Server](#)
- [Adjusting the Width of UDF Components](#)
- [Enabling Certification Using the System Property `OIG.IsIdentityAuditorEnabled`](#)
- [Observing the UI Changes in the Catalog Page](#)
- [oimclient.jar Needs Update and ipf.jar for Some passwordmgmt VOs](#)

## 10.8 Verifying the Oracle Identity Manager Upgrade

To verify your Oracle Identity Manager upgrade, perform the following steps:

1. Verify that Oracle Identity Manager 11.1.2.3.0 is running using the following URLs:

```
http://<oim_host>:<oim_port>/sysadmin
```

```
http://<oim_host>:<oim_port>/identity
```

where

`<oim_host>` is the host on which Oracle Identity Manager is running.

`<oim_port>` is the port number.

2. Verify that Oracle BI Publisher 11.1.1.9.0 is running using the following URL:

```
http://<bip_host>:<bip_port>/xmlpserver
```

where

`<bip_host>` is the host on which Oracle BI Publisher is running.

---

<biport> is the port number. The default http port for BI Publisher is 9704, if not changed during upgrade.

3. Use Fusion Middleware Control to verify that Oracle Identity Manager and any other Oracle Identity Management components are running in the Oracle Fusion Middleware environment.

---

---

**Note:** SOA composites `DefaultRequestApproval` and `DefaultOperationApproval` are available twice with versions 1.0 and 3.0 on Oracle Enterprise Manager, after you upgrade Oracle Identity Manager 11.1.2 or 11.1.2.1.0 to Oracle Identity Manager 11.1.2.3.0. The 1.0 composites are required for processing requests generated before upgrade, or any other functionality.

---

---

## 10.9 Troubleshooting

For the list of common issues that you might encounter during the Oracle Identity Manager upgrade process, and their workaround, see [Section 25.1, "Troubleshooting Oracle Identity Manager Upgrade Issues"](#).

For the list of known issues related to upgrade, and their workaround, see "Upgrade and Migration Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes for Identity Management*.



---

---

## Upgrading Oracle Entitlements Server 11g Release 2 (11.1.2.x.x) Environments

This chapter describes how to upgrade Oracle Entitlements Server 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0) and 11g Release 2 (11.1.2) environments to Oracle Entitlements Server 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

---

---

**Note:** This chapter refers to Oracle Entitlements Server 11g Release 2 (11.1.2), 11g Release 2 (11.1.2.1.0), and 11g Release 2 (11.1.2.2.0) environments as 11.1.2.x.x.

---

---

This chapter includes the following sections:

- [Upgrading Oracle Entitlements Server 11.1.2.x.x Administration Server](#)
- [Upgrading Oracle Entitlements Server 11.1.2.x.x Client](#)

### 11.1 Upgrading Oracle Entitlements Server 11.1.2.x.x Administration Server

This section describes how to upgrade Oracle Entitlements Server Administration Server to 11.1.2.3.0.

This section includes the following topics:

- [Section 11.1.1, "Upgrade Roadmap for Oracle Entitlements Server Administration Server"](#)
- [Section 11.1.2, "Performing the Required Pre-Upgrade Tasks"](#)
- [Section 11.1.3, "Shutting Down Administration Server and Oracle Entitlements Server Managed Servers"](#)

- [Section 11.1.4, "Upgrading Oracle WebLogic Server"](#)
- [Section 11.1.5, "Updating Oracle Entitlements Server Binaries to 11.1.2.3.0"](#)
- [Section 11.1.6, "Deleting all py.class Files"](#)
- [Section 11.1.7, "Upgrading Oracle Platform Security Services Schema"](#)
- [Section 11.1.8, "Upgrading Oracle Platform Security Services"](#)
- [Section 11.1.9, "Deleting Certain Directories From the Domain"](#)
- [Section 11.1.10, "Starting the Administration Server and the Managed Servers"](#)
- [Section 11.1.11, "Verifying the Oracle Entitlements Server Administration Server Upgrade"](#)

### 11.1.1 Upgrade Roadmap for Oracle Entitlements Server Administration Server

Table 11–1 lists the steps to upgrade Oracle Entitlements Server Administration Server upgrade.

---

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Entitlements Server Administration Server upgrade may not be successful.

---

**Table 11–1 Roadmap for Upgrading Oracle Entitlements Server Administration Server 11.1.2.x.x to 11.1.2.3.0**

SI No	Task	For More Information
1	Complete the pre-upgrade steps before you begin with the upgrade process.	See, <a href="#">Performing the Required Pre-Upgrade Tasks</a>
2	Stop the Administration Server and all the Oracle Entitlements Server Managed Servers.	See, <a href="#">Shutting Down Administration Server and Oracle Entitlements Server Managed Servers</a>
3	Upgrade your existing Oracle WebLogic Server to 10.3.6 (if necessary).	See, <a href="#">Upgrading Oracle WebLogic Server</a>
4	Upgrade the Oracle Entitlements Server binaries to 11.1.2.3.0.	See, <a href="#">Updating Oracle Entitlements Server Binaries to 11.1.2.3.0</a>
5	Delete all the <code>py.class</code> files in the newly installed Oracle Entitlements Server home.	See, <a href="#">Deleting all py.class Files</a>
6	Upgrade the Oracle Platform Security Services schemas.	See, <a href="#">Upgrading Oracle Platform Security Services Schema</a>
7	Upgrade Oracle Platform Security Services to 11.1.2.3.0. This task is optional but is recommended.	See, <a href="#">Upgrading Oracle Platform Security Services</a>
8	Delete the <code>tmp</code> , <code>cache</code> , and <code>stage</code> directories from the domain.	See, <a href="#">Deleting Certain Directories From the Domain</a>
9	Start all the servers.	See, <a href="#">Starting the Administration Server and the Managed Servers</a>
10	Verify the Oracle Entitlements Server Administration Server upgrade.	See, <a href="#">Verifying the Oracle Entitlements Server Administration Server Upgrade</a>

## 11.1.2 Performing the Required Pre-Upgrade Tasks

Before you begin with the upgrade, you must complete the following prerequisites:

- Review the *Oracle Fusion Middleware System Requirements and Specifications* and *Oracle Fusion Middleware Supported System Configurations* documents to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).
- Ensure that you are using a Java Development Kit (JDK) version that is supported and certified with Oracle Identity and Access Management 11.1.2.3.0.

You can verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

---

**Note:** For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

---

## 11.1.3 Shutting Down Administration Server and Oracle Entitlements Server Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Oracle Entitlements Server Managed Server(s) and the WebLogic Administration Server.

For information about stopping the WebLogic Administration Server and the Managed Servers, see [Section 24.1.9, "Stopping the Servers"](#).

## 11.1.4 Upgrading Oracle WebLogic Server

Oracle Identity and Access Management 11.1.2.3.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Entitlements Server environment is using Oracle WebLogic Server 10.3.5 or any earlier version, you must upgrade it to Oracle WebLogic Server 10.3.6.

---

**Note:** If you are already using Oracle WebLogic Server 10.3.6, ensure that you apply the mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server 10.3.6, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

---

For information about upgrading to Oracle WebLogic Server 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

## 11.1.5 Updating Oracle Entitlements Server Binaries to 11.1.2.3.0

To upgrade Oracle Entitlements Server binaries to 11.1.2.3.0, you must use the Oracle Identity and Access Management 11.1.2.3.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Middleware Home.

For information about updating the Oracle Entitlements Server binaries to 11.1.2.3.0, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 11.1.6 Deleting all py.class Files

After you upgrade the Oracle Entitlements Server binaries, delete all the files with postfix `py.class` in the newly installed Oracle Entitlements Server home (`MW_HOME/ORACLE_HOME/`).

## 11.1.7 Upgrading Oracle Platform Security Services Schema

Upgrade the Oracle Platform Security Services schemas using Patch Set Assistant.

For more information about upgrading schemas using Patch Set Assistant, see [Section 24.1.4, "Upgrading Schemas Using Patch Set Assistant"](#).

## 11.1.8 Upgrading Oracle Platform Security Services

After you upgrade Oracle Platform Security Services schemas, you must upgrade Oracle Platform Security Services (OPSS). This task is optional; however, it is recommended that you perform this task.

---

---

**Note:** If you are upgrading Oracle Entitlements Server 11.1.2.1.0 to 11.1.2.3.0, you must upgrade Oracle Platform Security Services if Audit schema is installed. This step is required to upgrade the policy store to include the new 11.1.2.3.0 audit policies.

---

---

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Entitlements Server to 11.1.2.3.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see [Section 24.1.7, "Upgrading Oracle Platform Security Services"](#).

## 11.1.9 Deleting Certain Directories From the Domain

Delete the following directories from the location `DOMAIN_HOME/servers/ServerName:`

- tmp
- cache
- stage

## 11.1.10 Starting the Administration Server and the Managed Servers

After the upgrade is complete, start the WebLogic Administration Server, and the Oracle Entitlements Server Managed Server(s).

For information about starting the WebLogic Administration Server and the Managed Server(s), see [Section 24.1.8, "Starting the Servers"](#).

## 11.1.11 Verifying the Oracle Entitlements Server Administration Server Upgrade

To verify the Oracle Entitlements Server upgrade, do the following:

- Verify the schema version in the policy store by running the following SQL query:

```
select attrval from jps_attrs where attrname='orclProductVersion' and
rownum = 1;
```

Ensure that the schema version is 11.1.1.9.0.

- The application MAPI works with both old and new functionality.  
Create a new policy to see if CRUD operations on the policy store artifacts, using their entity managers, are working.

For more information, see "Creating Fine Grained Elements for a Simple Policy" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*.

- The Application Runtime Authorization continues working.

To verify, create an authorization, as mentioned in "Using the PEP API" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*, and see if it works correctly.

## 11.2 Upgrading Oracle Entitlements Server 11.1.2.x.x Client

This section describes how to upgrade Oracle Entitlements Server client server to 11.1.2.3.0.

This section includes the following topics:

- [Section 11.2.1, "Upgrade Roadmap for Oracle Entitlements Server Client"](#)
- [Section 11.2.2, "Stopping all Security Module Instances"](#)
- [Section 11.2.3, "Upgrade Oracle Entitlements Server Client to 11.1.2.3.0"](#)
- [Section 11.2.4, "Deleting all py.class Files"](#)
- [Section 11.2.5, "Starting the Security Modules"](#)
- [Section 11.2.6, "Verifying Oracle Entitlements Server Client Upgrade"](#)

### 11.2.1 Upgrade Roadmap for Oracle Entitlements Server Client

Table 11–2 lists the steps to upgrade Oracle Entitlements Server Client Server upgrade.

---



---

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Entitlements Server Client Server upgrade may not be successful.

---



---

**Table 11–2 Roadmap for Upgrading Oracle Entitlements Server Client 11.1.2.x.x to 11.1.2.3.0**

SI No	Task	For More Information
1	Stop all the security module instances, and the servers.	See, <a href="#">Stopping all Security Module Instances</a>
2	Upgrade the Oracle Entitlements Server Client to 11.1.2.3.0.	See, <a href="#">Upgrade Oracle Entitlements Server Client to 11.1.2.3.0</a>

**Table 11–2 (Cont.) Roadmap for Upgrading Oracle Entitlements Server Client 11.1.2.x.x to 11.1.2.3.0**

SI No	Task	For More Information
3	Delete all the <code>py.class</code> files in the newly installed Oracle Entitlements Server home.	See, <a href="#">Deleting all py.class Files</a>
4	Start the security modules.	See, <a href="#">Starting the Security Modules</a>
5	Verify the Oracle Entitlements Server Client Server upgrade.	See, <a href="#">Verifying Oracle Entitlements Server Client Upgrade</a>

## 11.2.2 Stopping all Security Module Instances

Bring down all security module instances, Administration Server, and Managed Servers.

The security module instances shuts down when the Administration Server and Managed Servers are shut down.

To stop the servers, see [Section 11.1.3, "Shutting Down Administration Server and Oracle Entitlements Server Managed Servers"](#).

## 11.2.3 Upgrade Oracle Entitlements Server Client to 11.1.2.3.0

To upgrade Oracle Entitlements Server Client, you must use the 11.1.2.3.0 installer. During the procedure, point the Middleware Home to your existing 11.1.2.x.x Oracle Entitlements Server Client Middleware Home. This upgrades your Middleware Home and Oracle Home from 11.1.2.x.x to 11.1.2.3.0.

This section contains the following topics:

- [Prerequisites](#)
- [Obtaining the Software](#)
- [Installing Oracle Entitlements Server Client 11g Release 2 \(11.1.2.3.0\)](#)
- [Verifying the Installation](#)

### 11.2.3.1 Prerequisites

You must install and configure Oracle Entitlements Server Administration Server, as described in [Section 11.1.5, "Updating Oracle Entitlements Server Binaries to 11.1.2.3.0"](#).

### 11.2.3.2 Obtaining the Software

For more information on obtaining Oracle Fusion Middleware 11g software, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

### 11.2.3.3 Installing Oracle Entitlements Server Client 11g Release 2 (11.1.2.3.0)

For more information on installing Oracle Entitlements Server Client 11.1.2.3.0, see "Installing Oracle Entitlements Server Client" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

### 11.2.3.4 Verifying the Installation

To verify that your Oracle Entitlements Server Client install was successful, go to your Oracle Home directory which you specified during installation and verify that the Oracle Entitlements Server Client installation files are created.

## 11.2.4 Deleting all py.class Files

After you upgrade the Oracle Entitlements Server Client, delete all the files with postfix `py.class` in the newly installed Oracle Entitlements Server home (`MW_HOME/ORACLE_HOME/`).

## 11.2.5 Starting the Security Modules

Start the Security Modules. Prior to starting the security modules, ensure that you have started WebLogic Administration Server and the Managed Servers.

To start the servers, see [Section 11.1.10, "Starting the Administration Server and the Managed Servers"](#).

---

---

**Note:** When starting the Oracle Service Bus Security Module, you must use the parameter `-Doracle.oes.osbresource.converter.distinguishtransportprivilege=false` while running the script.

---

---

## 11.2.6 Verifying Oracle Entitlements Server Client Upgrade

To verify, create an authorization, as mentioned in "Using the PEP API" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*, and see if it works correctly.

The Application Runtime Authorization continues working.



# Part IV

---

## Upgrading Oracle Identity and Access Management 11g Release 1 (11.1.1.x.x) and 9.x Environments

This part includes the following chapters:

- [Chapter 12, "Upgrading Oracle Access Manager 11g Release 1 \(11.1.1.x.x\) Environments"](#)
- [Chapter 13, "Upgrading Oracle Adaptive Access Manager 11g Release 1 \(11.1.1.x.x\) Environments"](#)
- [Chapter 14, "Upgrading Oracle Identity Manager 11g Release 1 \(11.1.1.x.x\) Environments"](#)
- [Chapter 15, "Upgrading Oracle Entitlements Server 11g Release 1 \(11.1.1.5.0\) Environment"](#)
- [Chapter 16, "Upgrading Oracle Identity Manager 9.1.x.x Environments"](#)



---

---

## Upgrading Oracle Access Manager 11g Release 1 (11.1.1.x.x) Environments

This chapter describes how to upgrade your existing Oracle Access Manager 11g Release 1 (11.1.1.5.0) and 11g Release 1 (11.1.1.7.0) environments to Oracle Access Management 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0). For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

If you wish to upgrade Oracle Access Management multi-data center environments, refer to [Chapter 18, "Upgrading Oracle Access Management Multi-Data Center Environments"](#).

---

---

---

---

**Note:** This chapter refers to Oracle Access Manager 11g Release 1 (11.1.1.5.0) and 11g Release 1 (11.1.1.7.0) environments as 11.1.1.x.x.

---

---

This chapter includes the following sections:

- [Section 12.1, "Upgrade Roadmap for Oracle Access Manager"](#)
- [Section 12.2, "Performing the Required Pre-Upgrade Tasks"](#)
- [Section 12.3, "Upgrading Oracle Home"](#)
- [Section 12.4, "Creating Necessary Schemas"](#)
- [Section 12.5, "Extending Oracle Access Manager 11.1.1.x.x Domain with Oracle Platform Security Services Template"](#)
- [Section 12.6, "Upgrading Oracle Platform Security Services"](#)
- [Section 12.7, "Configuring Oracle Platform Security Services Security Store"](#)
- [Section 12.8, "Exporting Access Data"](#)
- [Section 12.9, "Importing Access Data"](#)
- [Section 12.10, "Copying Modified System mbean Configurations"](#)

- [Section 12.11, "Ensuring that the Newly Created OAM Policy Schema is in Use"](#)
- [Section 12.12, "Starting the Administration Server and Access Manager Managed Servers"](#)
- [Section 12.13, "Redeploying Access Manager Server Applications and Shared Libraries"](#)
- [Section 12.14, "Stopping the Administration Server and Access Manager Managed Servers"](#)
- [Section 12.15, "Deleting Folders"](#)
- [Section 12.16, "Upgrading System Configuration"](#)
- [Section 12.17, "Starting the Servers"](#)
- [Section 12.18, "Extending the Oracle Access Management Domain to Include Mobile Security Suite and Policy Manager"](#)
- [Section 12.19, "Performing the Required Post-Upgrade Tasks"](#)
- [Section 12.20, "Verifying the Oracle Access Management Upgrade"](#)
- [Section 12.21, "Troubleshooting"](#)

## 12.1 Upgrade Roadmap for Oracle Access Manager

---

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Access Manager upgrade may not be successful.

---

Table 12–1 lists the tasks that you must complete to upgrade Oracle Access Manager 11.1.1.x.x environments.

**Table 12–1 Upgrade Flow**

Task No.	Task	For More Information
1	Complete the necessary prerequisites before you upgrade Oracle Access Manager 11.1.1.x.x to 11.1.2.3.0.	See, <a href="#">Performing the Required Pre-Upgrade Tasks</a>
2	Upgrade Oracle Home by upgrading Oracle WebLogic Server to 10.3.6, applying mandatory patches for Oracle Access Manager, and upgrading Oracle Access Manager binaries to 11.1.2.3.0.	See, <a href="#">Upgrading Oracle Home</a>
3	Create Oracle Access Manager (OAM) and Oracle Platform Security Services (OPSS) schema using the Repository Creation Utility.	See, <a href="#">Creating Necessary Schemas</a>
4	Upgrade 11.1.1.x.x Oracle Home to 11.1.2.3.0.	See, <a href="#">Upgrading Oracle Access Manager Binaries to 11.1.2.3.0</a>
5	Extend your Oracle Access Manager 11.1.1.x.x domain with the OPSS template.	See, <a href="#">Extending Oracle Access Manager 11.1.1.x.x Domain with Oracle Platform Security Services Template</a>
6	Upgrade Oracle Platform Security Services.	See, <a href="#">Upgrading Oracle Platform Security Services</a>

**Table 12–1 (Cont.) Upgrade Flow**

Task No.	Task	For More Information
7	Run the <code>configuresecuritystore.py</code> script to configure policy stores.	See, <a href="#">Configuring Oracle Platform Security Services Security Store</a>
8	Export access data.	See, <a href="#">Exporting Access Data</a>
9	Import access data.	See, <a href="#">Importing Access Data</a>
10	Copy infrastructure mbean jar and configuration files	See, <a href="#">Copying Modified System mbean Configurations</a>
11	Start the Administration Server and Oracle Access Management Access Manager Managed Servers.	See, <a href="#">Starting the Administration Server and Access Manager Managed Servers</a>
12	Redeploy Access Manager servers and shared libraries.	See, <a href="#">Redeploying Access Manager Server Applications and Shared Libraries</a>
13	Stop the Administration Server and Oracle Access Management Access Manager Managed Server.	See, <a href="#">Stopping the Administration Server and Access Manager Managed Servers</a>
14	Delete the <code>tmp</code> and <code>stage</code> folders.	See, <a href="#">Deleting Folders</a>
15	Upgrade the system configuration of Oracle Access Management. This step is required for the 11.1.2.3.0 features to work.  This step is mandatory as compatibility mode is not supported for Oracle Access Manager 11.1.1.x.x upgrade.	See, <a href="#">Upgrading System Configuration</a>
16	Start the WebLogic Administration Server and the Oracle Access Management Access Manager Managed Server(s).	See, <a href="#">Starting the Servers</a>
17	Extend the Oracle Access Management domain to include Oracle Mobile Security Suite and Policy Manager.	See, <a href="#">Extending the Oracle Access Management Domain to Include Mobile Security Suite and Policy Manager</a>
18	Perform the required post-upgrade tasks.	See, <a href="#">Performing the Required Post-Upgrade Tasks</a>
19	Verify the Oracle Access Management upgrade.	See, <a href="#">Verifying the Oracle Access Management Upgrade</a>

## 12.2 Performing the Required Pre-Upgrade Tasks

Before you begin with the upgrade, you must complete the following prerequisites:

- Review the *Oracle Fusion Middleware System Requirements and Specifications* and *Oracle Fusion Middleware Supported System Configurations* documents to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).
- Ensure that you are using a Java Development Kit (JDK) version that is supported and certified with Oracle Identity and Access Management 11.1.2.3.0.

You can verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

---



---

**Note:** For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

---



---

- Ensure that the following artifacts are present in your environment:

- oamclient-truststore.jks

This file is located at `DOMAIN_HOME/output/webgate-ssl/oamclient-keystore.jks`.

- oamclient-keystore.jks

This file is located at `DOMAIN_HOME/output/webgate-ssl/oamclient-truststore.jks`.

If the artifacts are not present, generate them using the `keytool` command. For information about creating these artifacts, see "Creating Oracle Access Manager Key Store" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management for 11g Release 1 (11.1.1.5.0)*.

When you generate these files, they are created in the directory where the command for creating them is run. You must copy these files to the location `DOMAIN_HOME/output/webgate-ssl/` and rename them as mentioned.

- Oracle Access Management 11.1.2.3.0 has additional components configured in its Administration Server. Therefore, ensure that the WebLogic domain memory settings are updated to suite the machine configurations.

If the servers are started using command line, you must update the memory settings in the `setDomainEnv.sh` file. If the servers are started using Node Manager, you must update the memory settings using the WebLogic Administration console. It is recommended to do both.

To update the memory settings in the `setDomainEnv.sh` file, complete the following steps:

1. Go to the `DOMAIN_HOME/bin` directory.
2. Take a backup of file `setDomainEnv.sh` (on UNIX) or `setDomainEnv.cmd` (on Windows).
3. Open the `setDomainEnv.sh` (on UNIX) or `setDomainEnv.cmd` (on Windows) in an editor, and search for the following lines:

On UNIX:

```
# IF USER_MEM_ARGS the environment variable is set, use it to override ALL
# MEM_ARGS values
```

```
if [ "${USER_MEM_ARGS}" != "" ] ; then
MEM_ARGS="${USER_MEM_ARGS}"
export MEM_ARGS
fi
```

On Windows:

```
@REM IF USER_MEM_ARGS the environment variable is set, use it to override
```

```
ALL MEM_ARGS values
```

```
if NOT "%USER_MEM_ARGS%"==" " (
set MEM_ARGS=%USER_MEM_ARGS%
)
```

4. Add the USER\_MEM\_ARGS settings as shown in the following example:

On UNIX:

```
# IF USER_MEM_ARGS the environment variable is set, use it to override ALL
MEM_ARGS values
```

```
# Added for OAM 11.1.2.3 upgrade
USER_MEM_ARGS="-Xms4096m -Xmx4096m -XX:MaxPermSize=512m"
export USER_MEM_ARGS
```

```
if [ "${USER_MEM_ARGS}" != " " ] ; then
MEM_ARGS="${USER_MEM_ARGS}"
export MEM_ARGS
fi
```

On Windows:

```
@REM IF USER_MEM_ARGS the environment variable is set, use it to override
ALL MEM_ARGS values
```

```
@REM Added for OAM 11.1.2.3 upgrade
set USER_MEM_ARGS=-Xms4096m -Xmx4096m -XX:MaxPermSize=512m
```

```
if NOT "%USER_MEM_ARGS%"==" " (
set MEM_ARGS=%USER_MEM_ARGS%
)
```

5. Save the changes to the file

To update the memory settings using the WebLogic Administration console, complete the following steps:

1. Log in to the WebLogic Administration Console using the following URL:

```
http://host:port/console
```

2. Click **Servers** on the left navigation pane.
3. Select the OAM Server.
4. Go to the **Server Start** tab.
5. Click **Arguments**.
6. Set the value of JVM arguments for the OAM Server. For example:

```
-Xms4096m -Xmx4096m
```

7. Save the changes.

For more information about the memory requirements for Oracle Identity and Access Management, see "Memory and Space Requirements for Oracle Fusion Middleware and Oracle Identity and Access Management" in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management* for 11g Release 2 (11.1.2).

- Verify the Oracle Access Manager 11.1.1.x.x schema and credentials. To verify the Oracle Access Manager 11.1.1.x.x schema, check the schema name in the `DOMAIN_`

`HOME/config/jdbc/oam-db-jdbc.xml` file or verify the OAM datasource on the WebLogic Administration console by doing the following:

1. Log in to the WebLogic Administration Console using the following URL:

`http://host:port/console`

2. Click **Services** on the left navigation pane.
3. Click **Data Sources**, and then select **oamDS**.
4. Click **Connection pool** and verify the OAM data source.

To verify the schema credentials, use the schema name and password to connect to the database.

- Shut down the WebLogic Administration Server and Oracle Access Manager Managed Servers. For information about stopping the servers, see [Section 24.1.9, "Stopping the Servers"](#).
- Back up the following before you proceed with the upgrade:
  - `MW_HOME` directory, including the Oracle Home directories inside Middleware Home
  - Domain Home directory
  - Oracle Access Manager schemas
  - MDS schemas
  - Audit and any other dependent schemas

For information about backing up the Middleware Home and schemas, see [Section 24.1.2, "Backing up the Existing Environment"](#).

## 12.3 Upgrading Oracle Home

This section describes the tasks to be completed to upgrade the existing Oracle home.

This section includes the following topics:

- [Upgrading Oracle WebLogic Server to 10.3.6](#)
- [Applying Mandatory Patches for Oracle WebLogic Server](#)
- [Upgrading Oracle Access Manager Binaries to 11.1.2.3.0](#)

### 12.3.1 Upgrading Oracle WebLogic Server to 10.3.6

Oracle Identity and Access Management 11.1.2.3.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Access Manager environment is using Oracle WebLogic Server 10.3.5 or any earlier version, you must upgrade it to Oracle WebLogic Server 10.3.6.

For information about upgrading Oracle WebLogic Server, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

### 12.3.2 Applying Mandatory Patches for Oracle WebLogic Server

Ensure that you apply some mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server 10.3.6, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

### 12.3.3 Upgrading Oracle Access Manager Binaries to 11.1.2.3.0

Upgrade the Oracle Access Manager binaries using the Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) installer. During the procedure, point the Middleware Home to your existing 11.1.1.x.x Oracle Access Manager Middleware Home.

---

---

**Note:** Before upgrading the Oracle Access Manager binaries to 11g Release 2 (11.1.2.3.0), you must ensure that the OPatch version in `ORACLE_HOME` and `MW_HOME/oracle_common` is 11.1.0.10.3. Different OPatch version might cause patch application failure. If you have upgraded opatch to a newer version, you will have to roll back to version 11.1.0.10.3.

---

---

For information about upgrading Oracle Access Manager binaries to Oracle Access Management Access Manager 11.1.2.3.0, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 12.4 Creating Necessary Schemas

You must create the following schemas by running Repository Creation utility (RCU) 11.1.1.9.0:

- Oracle Access Manager (OAM) schema
- Oracle Platform Security Services (OPSS) schema
- Oracle Mobile Security Manager (OMSM) schema - (If you wish to configure Oracle Mobile Security Suite)
- Oracle Metadata Services (MDS) schema

For information about creating schemas using Run Repository Creation utility, see [Section 24.1.3, "Creating Database Schemas Using Repository Creation Utility"](#).

---

---

**Note:** Even if you are creating new schemas, do not delete your Oracle Access Manager 11.1.1.x.x schemas and do not use the old schema name, as you will need the old schema credentials while ["Exporting Access Data"](#).

---

---

## 12.5 Extending Oracle Access Manager 11.1.1.x.x Domain with Oracle Platform Security Services Template

Oracle Access Management Access Manager 11.1.2.3.0 uses the database to store policies. This requires extending Oracle Access Manager 11.1.1.x.x domain to include the Oracle Platform Security Services (OPSS) data source.

To extend your Oracle Access Manager 11.1.1.x.x domain with the OPSS template, complete the following steps:

1. Run the following command:

**On UNIX:**

```
./config.sh
```

It is located in the <MW\_HOME>/<Oracle\_IDM1>/common/bin directory.

**On Windows:**

```
config.cmd
```

It is located in the <MW\_HOME>\<Oracle\_IDM1>\common\bin directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured Oracle Access Manager. Click **Next**. The **Select Extension Source** screen appears.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle\_IDM1]** option. After selecting the domain configuration options, click **Next**. The **Configure JDBC Component Schema** screen appears.
5. On the **Configure JDBC Component Schema** screen, do the following:
  - Select **OAM Infrastructure**, and update the Oracle Access Manager 11.1.1.x.x schema information with the Access Manager 11.1.2.3.0 schema details.
  - Select **OPSS Schema**, and specify the values for Schema Owner, Schema Password, Database and Service, Host Name, and Port.
  - Click **Next**.

The **Test JDBC Component Schema** screen appears. After the test succeeds, the **Select Optional Configuration** screen appears.
6. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select anything as you have already configured your Oracle Access Manager 11.1.1.x.x environment. Click **Next**.
7. On the **Configuration Summary** screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Access Manager domain is extended to support Oracle Platform Security Services (OPSS), and Oracle Access Manager is configured to use the newly created 11.1.2.3.0 OPSS policy schema.

## 12.6 Upgrading Oracle Platform Security Services

You must upgrade Oracle Platform Security Services (OPSS) by running `upgradeOpss` command.

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Access Manager to 11.1.2.3.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see [Section 24.1.7, "Upgrading Oracle Platform Security Services"](#)

## 12.7 Configuring Oracle Platform Security Services Security Store

You must configure the Database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11.1.2.3.0.

For more information on configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 12.8 Exporting Access Data

Policy information from Oracle Access Manager 11.1.1.x.x schema needs to be extracted before importing it to the Access Manager 11.1.2.3.0 schema. The `exportAccessData` WLST command exports the Access Manager policy and configuration information from the 11.1.1.x.x Oracle Access Manager domain. You must export Oracle Access Manager 11.1.1.x.x configuration details, policy stores, keys, and CSF Passwords.

---



---

**Note:** Make sure to shutdown all WebLogic Server processes (administration server, Oracle Access Manager managed server, and node manager) before executing these export commands.

---



---

Complete the following steps to export data:

### On UNIX:

1. Move from your present working directory to the `<MW_HOME>/<Oracle_IDM1>/common/bin` directory by running the following command on the command line:

```
cd <MW_HOME>/<Oracle_IDM1>/common/bin
```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
./wlst.sh
```

3. At the WLST prompt, run the following script:

```
exportAccessData ("<UPGRADE_PROPERTIES_FILE>")
```

For example:

```
exportAccessData ("<ORACLE_HOME>/oam/server/wlst/scripts/sample_properties/oam_upgrade.properties")
```

See [Table 12-3](#) for sample properties and description.

4. Exit the WLST console using the `exit()` command.

### On Windows:

1. Move from your present working directory to the `<MW_HOME>\<Oracle_IDM1>\common\bin` directory by running the following command on the command line:

```
cd <MW_HOME>\<Oracle_IDM1>\common\bin
```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
wlst.cmd
```

- At the WLST prompt, run the following script:

```
exportAccessData (" <UPGRADE_PROPERTIES_FILE> ")
```

For example:

```
exportAccessData (" <ORACLE_HOME> \oam\server\wlst\scripts\sample_
properties\oam_upgrade-windows.properties ")
```

See [Table 12–3](#) for sample properties and description.

- Exit the WLST console using the `exit()` command.

[Table 12–2](#) describes the parameters you must specify on the command line:

**Table 12–2 Parameters for Exporting Data**

Parameter	Description
properties_location	Specify the path to the <code>oam_upgrade.properties</code> file in the Access Manager 11.1.1.x.x installation. The following example shows the complete path:  On UNIX, it is located in the <code>&lt;ORACLE_HOME&gt;/oam/server/wlst/scripts/sample_properties/oam_upgrade.properties</code> directory.  On Windows, it is located in the <code>&lt;ORACLE_HOME&gt;\oam\server\wlst\scripts\sample_properties\oam_upgrade-windows.properties</code> directory.

[Table 12–3](#) lists the properties of `oam_upgrade.properties`:

**Table 12–3 List of Properties Specified in `oam_upgrade.properties` File**

Properties	Description
MIDDLEWARE_HOME	Specify the complete path to the Middleware Home. For example: On UNIX: <code>/Oracle/Middleware</code> On Windows: <code>Oracle\Middleware</code>
ORACLE_HOME	This property refers to the location of the Oracle Identity and Access Management software. For example: On UNIX: <code>/Oracle/Middleware/Oracle_IDM1</code> On Windows: <code>&lt;MW_HOME&gt;\Oracle_IDM1</code>
OAM_DOMAIN_HOME	This property refers to the existing Oracle Access Manager 11.1.1.x.x domain home. For example: On UNIX: <code>/Oracle/Middleware/user_projects/domains/oam_domain</code> On Windows: <code>&lt;MW_HOME&gt;\user_projects\domains\&lt;oam_domain&gt;</code> directory.
ORACLE_COMMON_HOME	This property refers to the common components home. The following example shows the complete path: On UNIX, it is located in the <code>&lt;MW_HOME&gt;/oracle_common</code> directory. On Windows, it is located in the <code>&lt;MW_HOME&gt;\oracle_common</code> directory.

**Table 12–3 (Cont.) List of Properties Specified in oam\_upgrade.properties File**

Properties	Description
OAM_DEST_ARTIFACTS_LOCATION	<p>This property refers to the location where you want to place the upgrade artifacts, such as Oracle Access Manager 11.1.1.x.x configuration and policy files.</p> <p><b>Note:</b> Make sure that the artifacts folder has read/write access.</p>
OAM_TYPE_OF_UPGRADE	This is an InPlace upgrade.
OAM_IS_INCREMENTAL	<p>This property is used to specify if you run the upgrade in an incremental mode.</p> <p>Incremental form of upgrade is not supported in Access Manager 11.1.2.3.0. Therefore, set the value as <code>False</code>.</p>
OAM_POLICY_UPGRADE_OPTIMIZATION	<p>As a part of the Oracle Access Manager policy upgrade, the changes to the out of the box Access Manager policies are applied on top of the existing (11.1.1.x.x) out of the box policies. This process involves a three way merge of the Access Manager policies. This is a time consuming process (takes about 30 minutes).</p> <p>If you want to proceed with the merge, set the property to <code>false</code>.</p> <p>If you want to replace the Oracle Access Manager 11.1.1.x.x out of the box policies with the new ones, without the merge process, set this property to <code>true</code>.</p>
OAM_PS1_SCHEMA_OWNER	Use this property to connect to the 11.1.1.x.x policy store. Specify the Oracle Access Manager 11.1.1.x.x schema owner.
OAM_PS1_SCHEMA_CRED	Use this property to connect to the 11.1.1.x.x policy store. Specify the Oracle Access Manager 11.1.1.x.x schema credentials.
OAM_PS1_CREDENTIAL_ALIAS	<p>Use this property to connect to the 11.1.1.x.x policy store. Specify the Oracle Access Manager 11.1.1.x.x Oracle Entitlements Server database credential alias as:</p> <p><code>OESDBCredentialAlias</code></p>
OAM_PS1_JDBC_CONN_STRING	<p>Use this property to connect to the 11.1.1.x.x policy store. Specify the JDBC connection string in the following format:</p> <p><code>jdbc:oracle:thin:@dbhost:dbport/sid</code></p>
OAM_PS1_JDBC_DRIVER_CLASS	<p>Use this property to connect to the 11.1.1.x.x policy store. Specify the JDBC driver class in the following format:</p> <p><code>oracle.jdbc.OracleDriver</code></p>
OAM_PS1_ROOT_DN	<p>Use this property to connect to the 11.1.1.x.x policy store. Specify the properties as:</p> <p><code>cn=farm,cn=JPSText,cn=jpsroot</code></p>
OAM_PS1_POLICY_FILE	<p>This property refers to the absolute path to the XML file where extracted 11.1.1.x.x policy needs to be saved. Specify the path where you want to save the extracted Oracle Access Manager 11.1.1.x.x policies.</p> <p>For example:</p> <p>On UNIX, specify the following path:</p> <p><code>OAM_PS1_POLICY_FILE=&lt;UPGRADE_ARTIFACTS_DIR&gt;/oam-policy-ps1.xml</code></p> <p>On Windows, specify the following path:</p> <p><code>OAM_PS1_POLICY_FILE=&lt;UPGRADE_ARTIFACTS_DIR&gt;\oam-policy-ps1.xml</code></p>

**Table 12–3 (Cont.) List of Properties Specified in oam\_upgrade.properties File**

Properties	Description
OAM_PS1_POLICY_JARS	<p>Upgrade frameworks loads version specific jars for Exporting and Importing data. This property refers to the Oracle Access Manager 11.1.1.x.x policy jars available at the following path:</p> <p>On UNIX, it is located in the <code>&lt;ORACLE_HOME&gt;/oam/server/lib/upgrade/ps1-policy</code> directory.</p> <p>On Windows, it is located in the <code>&lt;ORACLE_HOME&gt;\oam\server\lib\upgrade\ps1-policy</code> directory.</p>
OAM_PS1_CONFIG_FILE_LOC	<p>This property refers to the Oracle Access Manager 11.1.1.x.x configuration files available in the following location:</p> <p>On UNIX, it is located in the <code>&lt;DOMAIN_HOME&gt;/config/fmwconfig/oam-config.xml</code> directory.</p> <p>On Windows, it is located in the <code>&lt;DOMAIN_HOME&gt;\config\fmwconfig\oam-config.xml</code> directory.</p>
OAM_PS1_POLICY_FILE_TEMP	<p>This property refers to the absolute path to the temporary policy XML. This temporary XML will be used for policy transformation.</p> <p>Specify the temporary location of the XML file.</p> <p>For example:</p> <p>On UNIX, specify the following path:</p> <pre>OAM_PS1_POLICY_FILE_TEMP=&lt;UPGRADE_ATRIFACTS_DIR&gt;/oam-policy-ps1_temp.xml</pre> <p>On Windows, specify the following path:</p> <pre>OAM_PS1_POLICY_FILE_TEMP=&lt;UPGRADE_ATRIFACTS_DIR&gt;\oam-policy-ps1_temp.xml</pre>
OAM_R2_POLICY_JARS	<p>Upgrade frameworks loads version specific jars for exporting and importing data. This property refers to the Access Manager 11.1.2.3.0 policy jars available at the following location:</p> <p>On UNIX, it is located in the <code>&lt;ORACLE_HOME&gt;/oam/server/lib/upgrade/ps2-policy</code> directory.</p> <p>On Windows, it is located in the <code>&lt;ORACLE_HOME&gt;\oam\server\lib\upgrade\ps2-policy</code> directory.</p>
OAM_R2_CONFIG_FILE_LOC	<p>This property refers to the Access Manager 11.1.2.3.0 configuration files available at the following location:</p> <p>On UNIX, it is located in the <code>&lt;ORACLE_HOME&gt;/oam/server/config/oam-config.xml</code> directory.</p> <p>On Windows, it is located in the <code>&lt;ORACLE_HOME&gt;\oam\server\config\oam-config.xml</code> directory.</p>
OAM_SOURCE_VERSION	<p>Specify the source version of Oracle Access Manager.</p> <p>If the source version is 11g Release 1 (11.1.1.7.0), specify 11.1.1.7.0. If the source version is 11g Release 1 (11.1.1.5.0), specify 11.1.1.5.0.</p> <p>If you have applied bundle patches, the minor bundle patch version should not be specified. For example, 11.1.1.5.2.</p>
OAM_TARGET_VERSION	<p>The Oracle Access Manager target version is 11.1.2.0.0.</p>
OAM_OFFLINE_POLICY_MIGRATION	<p>This property is used for the offline redeployment feature of the upgrade. This feature is not supported in this release. Therefore, the value of this property must be set to <code>false</code>.</p>

---

**Note:** The variables listed in [Table 12–3](#) are not environment variables. These variables must be defined in the `oam_upgrade.properties` file.

When you specify paths to any files in the `oam_upgrade.properties` file, make sure it is in the format specified in the following example:

- On UNIX: `/directory_1/directory_2/file`
  - On Windows: `\\directory_1\\directory_2\\file`
- 

### Sample Output of `exportAccessData`

```
wls:/offline> exportAccessData("<ORACLE_HOME>/oam/server/wlst/scripts/sample_
properties/oam_upgrade.properties")
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.WLSTExecutor executeCommand
INFO: EXPORT_DATA_COMMAND
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.util.WLSTExportDataUtil
executeCommand
INFO: OAM PRODUCT
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.util.WLSTExportDataUtil
executeCommand
INFO: OAM PRODUCT
Jul 7, 2012 1:37:30 AM oracle.security.access.upgrade.util.WLSTExportDataUtil
executeCommand
INFO: oamPlugin.getName() =
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory
Jul 7, 2012 1:37:30 AM oracle.security.am.upgrade.plugin.util.UpgradeUtil
exportConfiguration
INFO: Copying configuration file....
oracle.security.am.upgrade.plugin.upgradehelper.OAMVersionSpecificClassLoader@1e33
0f43
[EL Info]: 2012-07-07 01:37:32.849--ServerSession(503497062)--EclipseLink,
version: Eclipse Persistence Services - 1.1.0.r3634
[EL Info]: 2012-07-07 01:37:35.212--ServerSession(503497062)--file:$ORACLE_
HOME/oam/server/lib/upgrade/ps1-policy/oes-d8/jps-internal.jar-JpsDBDataManager
login successful
Jul 7, 2012 1:37:39 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:37:39.026/135.466 Oracle Coherence 3.5.3/465p2 <Info>
(thread=Main Thread, member=n/a): Loaded operational configuration from resource
"jar:file:$ORACLE_
HOME/oam/server/lib/upgrade/ps1-policy/coherence.jar!/tangosol-coherence.xml"
Jul 7, 2012 1:37:39 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:37:39.035/135.474 Oracle Coherence 3.5.3/465p2 <Info>
(thread=Main Thread, member=n/a): Loaded operational overrides from resource
"jar:file:$ORACLE_
HOME/oam/server/lib/upgrade/ps1-policy/coherence.jar!/tangosol-coherence-override-
dev.xml"
.....
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:37:47 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:37:47 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:37:47 AM
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory exportData
INFO: Extraction Done!!
Jul 7, 2012 1:37:47 AM oracle.security.am.upgrade.plugin.util.UpgradeCommonUtil
removedDirectory
INFO: Deletion of Directory: true path: $OAM_ARTIFACTS_DIRECTORY/temp.zip
```

```
Jul 7, 2012 1:37:47 AM
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory exportData
INFO: Export completed successfully!
```

## 12.9 Importing Access Data

It is necessary to import the extracted Oracle Access Manager 11.1.1.x.x data to the Access Manager 11.1.2 schema. The Oracle Access Manager 11.1.1.x.x domain configuration is also merged with the Access Manager 11.1.2 configuration.

---

---

**Note:** Make sure to shutdown all WebLogic Server processes (administration server, Oracle Access Manager managed server, and node manager) before executing these import commands.

---

---

To import Oracle Access Manager 11.1.1.x.x configuration data into Access Manager 11.1.2.3.0, complete the following steps:

### On UNIX:

1. Move from your present working directory to the <MW\_HOME>/<Oracle\_IDM1>/common/bin directory by running the following command on the command line:

```
cd <MW_HOME>/<Oracle_IDM1>/common/bin
```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
./wlst.sh
```

3. At the WLST prompt, run the following script:

```
importAccessData ("<UPGRADE_PROPERTIES_FILE>")
```

For example:

```
importAccessData ("<ORACLE_HOME>/oam/server/wlst/scripts/sample_
properties/oam_upgrade.properties")
```

See [Table 12-3](#) for sample properties and description.

4. Exit the WLST console using the `exit()` command.

### On Windows:

1. Move from your present working directory to the <MW\_HOME>\<Oracle\_IDM1>\common\bin directory by running the following command on the command line:

```
cd <MW_HOME>\<Oracle_IDM1>\common\bin
```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
wlst.cmd
```

3. At the WLST prompt, run the following script:

```
importAccessData ("<UPGRADE_PROPERTIES_FILE>")
```

For example:

```
importAccessData ("<ORACLE_HOME>\\oam\\server\\wlst\\scripts\\sample_
properties\\oam_upgrade.properties")
```

See [Table 12-3](#) for sample properties and description.

4. Exit the WLST console using the `exit()` command.

[Table 12-4](#) describes the parameters you need to specify on the command line:

**Table 12-4 Parameters for Importing Data**

Parameter	Description
<code>properties_location</code>	Specify the path to the <code>oam_upgrade.properties</code> file in the Oracle Access Manager 11.1.1.x.x installation. The following example shows the complete path:  On UNIX, it is located in the <code>IDM_HOME/oam/server/wlst/scripts/sample_properties/oam_upgrade.properties</code> directory.  On Windows, it is located in the <code>IDM_HOME\oam\server\wlst\scripts\sample_properties\oam_upgrade.properties</code> directory.

### Sample Output of `importAccessData`

```
wls:/offline> importAccessData("<ORACLE_HOME>/oam/server/wlst/scripts/sample_
properties/oam_upgrade.properties")
LOGGER intialised java.util.logging.Logger@1e26e4b1
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.WLSTExecutor executeCommand
INFO: IMPORT_DATA_COMMAND
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.util.WLSTImportDataUtil
executeCommand
INFO: OAAM PRODUCT IMPORT DATA
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.util.WLSTImportDataUtil
executeCommand
INFO: OAM PRODUCT
Jul 7, 2012 1:38:25 AM oracle.security.access.upgrade.util.WLSTImportDataUtil
executeCommand
INFO: oamPlugin.getName() =
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory
Jul 7, 2012 1:38:27 AM
oracle.security.am.common.policy.admin.provider.xml.XMLStore <init>
INFO: Loading policy store file: $OAM_ARTIFACTS_DIRECTORY/oam-policy.xml.
Jul 7, 2012 1:38:30 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:38:30.069/17.816 Oracle Coherence 3.7.1.1 <Info> (thread=Main
Thread, member=n/a): Loaded operational configuration from "jar:file:$MIDDLEWARE_
HOMEoracle_common/modules/oracle.coherence/coherence.jar!/tangosol-coherence.xml"
Jul 7, 2012 1:38:30 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:38:30.103/17.850 Oracle Coherence 3.7.1.1 <Info> (thread=Main
Thread, member=n/a): Loaded operational overrides from "jar:file:$MIDDLEWARE_
HOMEoracle_
common/modules/oracle.coherence/coherence.jar!/tangosol-coherence-override-dev.xml"
"
Jul 7, 2012 1:38:30 AM com.tangosol.coherence.component.util.logOutput.Jdk log
INFO: 2012-07-07 01:38:30.107/17.854 Oracle Coherence 3.7.1.1 <Info> (thread=Main
Thread, member=n/a): Loaded operational overrides from "jar:file:$ORACLE_
HOME/oam/server/lib/upgrade/ps2-policy/mapstore-coherence.jar!/tangosol-coherence-
override.xml"
.....
Jul 7, 2012 1:38:36 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:38:36 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
Jul 7, 2012 1:38:36 AM oracle.security.am.common.audit.AuditHandler getAuditor
WARNING: Cannot load audit configuration.
```

```
Jul 7, 2012 1:38:38 AM
oracle.security.am.upgrade.plugin.upgradehelper.UpgradeFactory importData
INFO: Import completed successfully!!
```

---

---

**Note:** When you execute the `importAccessData()` command, the output might include additional text after the line `INFO: Import completed successfully!!`. The additional text has no impact on the result and can be ignored.

---

---

## 12.10 Copying Modified System mbean Configurations

After updating the Oracle Access Manager binaries to 11.1.2.3.0 you must copy the modified system or domain mbean configurations from the `OAM_ORACLE_HOME` to the `DOMAIN_HOME`.

### On UNIX:

1. Move from your present working directory to the `<MW_HOME>/common/bin` directory by running the following command on the command line:
2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
cd <MW_HOME><Oracle_IDM1>/common/bin
```

```
./wlst.sh
```

3. At the WLST prompt, run the following script:

```
copyMbeanXmlFiles('DOMAIN_HOME', 'OAM_ORACLE_HOME')
```

For example:

```
copyMbeanXmlFiles('/Oracle/Middleware/user_projects/domains/base_
domain', '/Oracle/Middleware/Oracle_IDM1')
```

4. Exit the WLST console using the `exit()` command.

### On Windows:

1. Move from your present working directory to the `<MW_HOME>\common\bin` directory by running the following command on the command line:
2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
cd <MW_HOME>\<Oracle_IDM1>\common\bin
```

```
wlst.cmd
```

3. At the WLST prompt, run the following script:

```
copyMbeanXmlFiles ('<domain_name>', 'Oracle_IDM1')
```

For example:

```
copyMbeanXmlFiles('C:\\Oracle\\Middleware\\user_projects\\domains\\base_
domain', 'C:\\Oracle\\Middleware\\Oracle_IDM1')
```

4. Exit the WLST console using the `exit()` command.

## 12.11 Ensuring that the Newly Created OAM Policy Schema is in Use

Verify the database details to check if the newly created 11.1.2.3.0 OAM policy schema is in use. This can be done using the WebLogic Administration console or by checking

the `DOMAIN_HOME/config/jdbc/oam-db-jdbc.xml` file. Ensure that the following tag in the `oam-db-jdbc.xml` file contains the name of the newly created 11.1.2.3.0 OAM Policy schema:

```
<name>oamDS</name>
```

## 12.12 Starting the Administration Server and Access Manager Managed Servers

Start the WebLogic Administration Server and the Access Manager Managed Servers. For more information, see [Section 24.1.8, "Starting the Servers"](#).

---

**Note:** When you start the servers, you may see the following exception:

```
<Error> <oracle.idaas.common> <BEA-000000> <ORA-00942: table or
view does not exist
.
java.sql.SQLException: ORA-00942: table or view does not
exist
.
    at
oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:462)
    at
oracle.jdbc.driver.T4CTTIoer.processError(T4CTTIoer.java:405)
    at
oracle.jdbc.driver.T4C8Oall.processError(T4C8Oall.java:931)
    at oracle.jdbc.driver.T4CTTIfun.receive(T4CTTIfun.java:481)
    at oracle.jdbc.driver.T4CTTIfun.doRPC(T4CTTIfun.java:205)
    at oracle.jdbc.driver.T4C8Oall.doOALL(T4C8Oall.java:548)
    at
oracle.jdbc.driver.T4CPreparedStatement.doOall8(T4CPreparedStatement.java:217)
```

Ignore this warning and proceed.

---

## 12.13 Redeploying Access Manager Server Applications and Shared Libraries

You must redeploy Oracle Access Management Access Manager server applications for the following reasons:

- To uptake new shared libraries that Access Manager servers are dependent on.
- To uptake newer versions of Oracle Access Management Administration and Managed Server applications.

Access Manager Server applications can be redeployed using the WLST command `redeployOAM`.

**Note:** Before you run the `redeployOAM` command, ensure that the Access Manager Managed Server(s) are in `RUNNING` state and not in the `ADMIN` state.

If the servers are in `ADMIN` state, do the following:

1. Log in to the WebLogic Administration Server using the following URL:  
`http://host:port/console`
2. Click Deployments.
3. Click `oam_server(11.1.2.0.0)` on the **Summary of Deployments** page.
4. Click `OAM_SERVER` on the **Summary of Servers** page.
5. Go to the **Control** tab and click **RESUME**.

To redeploy Access Manager server applications and shared Access Manager libraries, complete the following steps:

1. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location `$MW_HOME/ORACLE_HOME/common/bin`:

On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

2. Connect to the Administration Server using the following command:

```
connect('<weblogic_username>', '<weblogic_password>', '<weblogic_host>:<port>')
```

3. Run the following command to redeploy the applications and shared libraries:

```
redeployOAM("ORACLE_HOME", "ORACLE_COMMON_HOME", adminTarget="Admin_server_name", serverTarget="oam_server")
```

**Note:** If you are upgrading Oracle Access Manager high availability environments, specify the `oam_cluster` for the argument `serverTarget` while running `redeployOAM` command.

Table 12–5 describes the parameters you need to specify on the command line:

**Table 12–5 Parameters to be Specified When Running `redeployOAM` Command**

Parameter	Description
<code>ORACLE_HOME</code>	Specify the absolute path to the Oracle Home. For example: On UNIX, it is located at <code>Oracle/Middleware</code> directory. On Windows, it is located at <code>Oracle\Middleware</code> directory.
<code>ORACLE_COMMON_HOME</code>	Specify the absolute path to the Oracle common home. For example: On UNIX, it is located in the <code>Oracle/Middleware/Common_home</code> directory. On Windows, it is located in the <code>Oracle\Middleware\Common_home</code> directory.
<code>adminTarget</code>	Specify the Administration Server name you had specified while configuring Access Manager.

**Table 12–5 (Cont.) Parameters to be Specified When Running redeployOAM Command**

Parameter	Description
serverTarget	Specify the name of the Access Manager Server you had specified while configuring Access Manager Server.

For example:

```
redeployOAM("/scratch/Oracle/Middleware/Oracle_
IDM1", "/scratch/Oracle/Middleware/oracle_
common", adminTarget="AdminServer", serverTarget="OAM_SERVER")
```

---



---

**Note:**

- You might see the following exception after the Access Manager server deployment. This is because tmp and stage directories still exist. You can ignore the errors:

```
HTTP:101216]Servlet: "AMInitServlet" failed to preload on
startup in Web application: "oam".
java.lang.ExceptionInInitializerError
at java.lang.J9VMInternals.initialize(J9VMInternals.java:222)
at
oracle.security.am.engines.sso.adapter.AbstractSessionAdapterIm
pl.checkAndInit(AbstractSessionAdapterImpl.java:97)
at
oracle.security.am.engines.sso.adapter.AbstractSessionAdapterIm
pl.<init>(AbstractSessionAdapterImpl.java:75)
at
oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapt
erImpl.<init>(MultipleUserSessionAdapterImpl.java:56)
at
oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapt
erImpl.<clinit>(MultipleUserSessionAdapterImpl.java:45)
at java.lang.J9VMInternals.initializeImpl(Native Method)
at java.lang.J9VMInternals.initialize(J9VMInternals.java:200)
at
oracle.security.am.engines.sso.adapter.SessionManagementAdapter
Factory.getAdapter(SessionManagementAdapterFactory.java:46)
Caused by:
oracle.security.am.common.utilities.exception.AmRuntimeExceptio
n:OAM Server Key initialization failed
Caused by: javax.crypto.BadPaddingException: Given final block
not properly padded
```

- When you execute the redeployOAM command, the following warning may be displayed:

```
***** Performing OAM Admin server
deployment and Data Migration. This operation will take some
time. Please wait until it completes.*****
```

Note that redeployment takes approximately 30 minutes to complete due to policy migration. In addition, note that the time for completion of redeployment also depends on the amount of data present in the Oracle Access Manager system that is being upgraded.

---



---

4. Exit the WLST console using the `exit()` command.

The deployment may fail if the SDP library is already installed as a part of the SOA or OIM deployments. For recovery procedure, see [Section 25.2.3, "Exception While Deploying Application"](#).

---

---

**Note:**

After redeploying Oracle Access Management Access Manager, you must verify that the following libraries and applications are deployed to Access Manager cluster (OAM\_CLUSTER):

**Libraries**

- `oracle.oaam.libs` (11.1.2.0.0)
- `oracle.sdp.client` (11.1.1)
- `coherence` (3.7.1.1)
- `oracle.idm.ids.config.ui` (11.1.2,11.1.2)
- `oracle.idm.ipf` (11.1.2,11.1.2)

**Applications**

- `oamsso_logout` (11.1.2.0.0)
  - `oam_server` (11.1.2.0.0)
- 
- 

## 12.14 Stopping the Administration Server and Access Manager Managed Servers

Stop the WebLogic Administration Server and the Access Manager Managed Server(s). For more information, see [Section 24.1.9, "Stopping the Servers"](#).

## 12.15 Deleting Folders

This step is required to uptake new version of the Access Manager Managed Server. The `redeploy` command does not delete the `tmp` directories.

In order to deploy Oracle Access Management 11.1.1.x.x server content and applications to Access Manager 11.1.2.3.0, you must delete all folders in the following location:

**On UNIX:**

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAM_MANAGED_SERVER_NAME>
```

**On Windows:**

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAM_MANAGED_SERVER_NAME>
```

## 12.16 Upgrading System Configuration

For the Oracle Access Management 11.1.2.3.0 features to work, you must run the `upgradeConfig()` utility on the machine that hosts Administration Server. This utility upgrades the system configuration and policy store of Oracle Access Management to 11.1.2.3.0. This step is mandatory for the upgraded environment to work.

---



---

**Note:** Compatibility mode is not supported for Oracle Access Manager 11.1.1.x.x upgrade. Therefore, it is mandatory to upgrade the system configurations in order to complete the Access Manager upgrade process.

---



---

To upgrade the system configuration of Oracle Access Management, do the following:

1. Stop the WebLogic Administration Server and the Access Manager Managed Server(s). For more information, see [Section 24.1.9, "Stopping the Servers"](#)
2. The `upgradeConfig` command needs to be run using the IPv4 stack. Therefore, you must add the following property to the `wlst.sh` file (on UNIX) or `wlst.cmd` file (on Windows) located at `ORACLE_HOME/common/bin`:

```
-Djava.net.preferIPv4Stack=true
```

To do this, open the `wlst.sh` or `wlst.cmd` file in a text editor, add the property, and save the file.

3. Run the following command to launch the WebLogic Scripting Tool (WLST) from the location `$ORACLE_HOME/common/bin`:

On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

4. Run the following command in offline mode:

```
upgradeConfig("domain_home", "sysdbaUser", "sysdbaPwd",
"oamSchemaOwner", "oamdbJdbcUrl")
```

In this command,

- `domain_home` is the absolute path to the Access Manager WebLogic domain.
- `sysdbauser` is the database username having `sysdba` privileges.
- `sysdbapwd` is the password of the database user having `sysdba` privileges.
- `oamSchemaOwner` is the database username for OAM schema.
- `oamdbjdbcUrl` is the JDBC URL to connect to the Access Manager database. The JDBC URL must be in specified in the format `"jdbc:oracle:thin:@<server_host>:<server_port>/<service_name>"`.

For example:

On UNIX:

```
upgradeConfig("/Oracle/Middleware/user_projects/domains/base_domain",
"sys", "pwd", "PREFIX_OAM", "jdbc:oracle:thin:@localhost:1521/orcl")
```

On Windows:

```
upgradeConfig("C:\\Oracle\\Middleware\\user_projects\\domains\\base_
domain", "sys", "pwd", "PREFIX_OAM",
"jdbc:oracle:thin:@localhost:1521/orcl")
```

## 12.17 Starting the Servers

Start the WebLogic Administration Server, Access Manager Managed Server(s), and the OMSS server. For more information, see [Section 12.12, "Starting the Administration Server and Access Manager Managed Servers"](#).

## 12.18 Extending the Oracle Access Management Domain to Include Mobile Security Suite and Policy Manager

Extend the Oracle Access Management domain to include Oracle Mobile Security Suite (OMSS) and Policy Manager. Using the functionality of Oracle Mobile Security Suite is optional. However, you must perform this step to enable the Policy Manager.

For more information, see [Section 24.3.1, "Extending the 11.1.2.3.0 Access Manager Domain to Include Mobile Security Suite and Policy Manager"](#).

---

---

**Note:** To start using the features of Oracle Mobile Security Suite, you must enable Oracle Mobile Security Suite as described in [Section 12.19.1, "Optional: Enabling Oracle Mobile Security Suite"](#).

---

---

## 12.19 Performing the Required Post-Upgrade Tasks

This section describes the post-upgrade tasks required to enable the features of Access Manager 11.1.2.3.0. These tasks are optional.

This section includes the following topics:

- [Optional: Enabling Oracle Mobile Security Suite](#)
- [Assigning Necessary Roles to Admin](#)

### 12.19.1 Optional: Enabling Oracle Mobile Security Suite

If you wish to use the functionality of Oracle Mobile Security Suite, you must enable Oracle Mobile Security Suite after extending the Access Manager domain with Oracle Mobile Security Suite component.

For more information, see [Section 24.3.2, "Enabling Oracle Mobile Security Suite"](#).

### 12.19.2 Assigning Necessary Roles to Admin

Ensure that you assign necessary roles to the global role **Admin**, by setting the role conditions as **IDM Administrators**, **Administrators**, or **OAMAdministrators**.

For more information about creating and managing global security roles, see "Create global security roles" in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* for 11g Release 1 (10.3.6).

## 12.20 Verifying the Oracle Access Management Upgrade

Verify the Oracle Access Management upgrade by accessing the Oracle Access Management Access Manager Administration Console 11g Release 2 (11.1.2.3.0).

If you have enabled Oracle Mobile Security Suite (OMSS) and wish to use the functionality of OMSS, use the following URL to access the Access Manager Administration Console:

`http://<oam_admin_server_host>:<oam_admin_server_port>/access`

If you have not enabled Oracle Mobile Security Suite (OMSS), use the following URL to access the Access Manager Administration Console:

`http://<oam_admin_server_host>:<oam_admin_server_port>/oamconsole`

---

---

**Note:** This note is applicable only to users who currently have Oracle Identity Manager and Oracle Access Manager components integrated in 11g R1 (11.1.1.5.1) or earlier versions, and are upgrading both Oracle Identity Manager and Access Manager to 11g Release 2 (11.1.2.3.0).

After upgrading the components to 11g Release 2 (11.1.2.3.0), see "Using the idmConfigTool Command" in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

---

---

## 12.21 Troubleshooting

For the list of common issues that you might encounter during the Oracle Access Management upgrade process, and their workaround, see [Section 25.2, "Troubleshooting Oracle Access Management Upgrade Issues"](#).

For the list of known issues related to upgrade, and their workaround, see "Upgrade and Migration Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes for Identity Management*.



---

---

## Upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x) Environments

This chapter describes how to upgrade your existing Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0) and 11g Release 1 (11.1.1.7.0) environments to Oracle Adaptive Access Manager 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

---

---

**Note:** This chapter refers to Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0) and 11g Release 1 (11.1.1.7.0) environments as 11.1.1.x.x.

---

---

This chapter includes the following sections:

- [Section 13.1, "Upgrade Roadmap for Oracle Adaptive Access Manager"](#)
- [Section 13.2, "Performing the Required Pre-Upgrade Tasks"](#)
- [Section 13.3, "Shutting Down Administration Server and Managed Servers"](#)
- [Section 13.4, "Backing Up Oracle Adaptive Access Manager 11g Release 1 \(11.1.1.x.x\)"](#)
- [Section 13.5, "Optional: Upgrading Oracle WebLogic Server"](#)
- [Section 13.6, "Upgrading Oracle Adaptive Access Manager Binaries to 11g Release 2 \(11.1.2.3.0\)"](#)
- [Section 13.7, "Upgrading OAAM, MDS, IAU, and OPSS Schemas"](#)
- [Section 13.8, "Extending Oracle Adaptive Access Manager 11.1.1.x.x Component Domains with OPSS Template"](#)
- [Section 13.9, "Upgrading Oracle Platform Security Services"](#)
- [Section 13.10, "Configuring OPSS Security Store"](#)

- [Section 13.11, "Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers"](#)
- [Section 13.12, "Redeploying the Applications"](#)
- [Section 13.13, "Deleting Folders"](#)
- [Section 13.14, "Restarting the Servers"](#)
- [Section 13.15, "Verifying the Upgrade"](#)

## 13.1 Upgrade Roadmap for Oracle Adaptive Access Manager

---

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Adaptive Access Manager upgrade may not be successful.

---

[Table 13–1](#) lists the steps to upgrade Oracle Adaptive Access Manager.

**Table 13–1** *Upgrade Flow*

	Task	For More Information
1	Complete the prerequisites before you begin with the upgrade process.	See, <a href="#">Performing the Required Pre-Upgrade Tasks</a>
2	Shut down all servers. This includes both Administration Server and Managed Servers.	See, <a href="#">Shutting Down Administration Server and Managed Servers</a>
3	Back up your environment.	See, <a href="#">Backing Up Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x)</a>
4	Optional - Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6.	See, <a href="#">Optional: Upgrading Oracle WebLogic Server</a>
5	Upgrade Oracle Adaptive Access Manager binaries to 11.1.2.3.0.	See, <a href="#">Upgrading Oracle Adaptive Access Manager Binaries to 11g Release 2 (11.1.2.3.0)</a>
6	Upgrade the OAAM, MDS, IAU, and OPSS Schemas using Patch Set Assistant.	See, <a href="#">Upgrading OAAM, MDS, IAU, and OPSS Schemas</a>
7	Extend your Oracle Adaptive Access Manager 11.1.1.x.x domain with the OPSS template.	See, <a href="#">Extending Oracle Adaptive Access Manager 11.1.1.x.x Component Domains with OPSS Template</a>
8	Upgrade Oracle Platform Security Services, if required.	See, <a href="#">Upgrading Oracle Platform Security Services</a>
9	Run the <code>configuresecuritystore.py</code> script to configure policy stores.	See, <a href="#">Configuring OPSS Security Store</a>
10	Start the Administration and Managed Servers.	See, <a href="#">Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers</a>
11	Redeploy the applications on Oracle Adaptive Access Manager 11.1.2.3.0 Servers.	See, <a href="#">Redeploying the Applications</a>
12	Delete the <code>tmp</code> and <code>stage</code> folders.	See, <a href="#">Deleting Folders</a>
13	Restart the servers.	See, <a href="#">Restarting the Servers</a>

**Table 13–1 (Cont.) Upgrade Flow**

	<b>Task</b>	<b>For More Information</b>
14	Verify the Oracle Adaptive Access Manager upgrade.	See, <a href="#">Verifying the Upgrade</a>

## 13.2 Performing the Required Pre-Upgrade Tasks

Before you begin with the upgrade, you must complete the following prerequisites:

- Review the *Oracle Fusion Middleware System Requirements and Specifications* and *Oracle Fusion Middleware Supported System Configurations* documents to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).
- Ensure that you are using a Java Development Kit (JDK) version that is supported and certified with Oracle Identity and Access Management 11.1.2.3.0.

You can verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

---

**Note:** For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

---

## 13.3 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Servers.

For more information about stopping the WebLogic Administration Server and the Managed Servers, see [Section 24.1.9, "Stopping the Servers"](#).

## 13.4 Backing Up Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x)

You must back up your Oracle Adaptive Access Manager 11.1.1.x.x environment before you upgrade to Oracle Adaptive Access Manager 11.1.2.3.0.

After stopping the servers, you must back up the following:

- *MW\_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Adaptive Access Manager schemas
- IAU schema, if it is part of any of your Oracle Adaptive Access Manager 11.1.1.x.x schemas
- MDS schemas

## 13.5 Optional: Upgrading Oracle WebLogic Server

Oracle Identity and Access Management 11.1.2.3.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Adaptive Access Manager environment is using Oracle WebLogic Server 10.3.5 or any earlier version, you must upgrade it to Oracle WebLogic Server 10.3.6.

---

---

**Note:** If you are already using Oracle WebLogic Server 10.3.6, ensure that you apply the mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server 10.3.6, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

---

---

For information about upgrading Oracle WebLogic Server to 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

## 13.6 Upgrading Oracle Adaptive Access Manager Binaries to 11g Release 2 (11.1.2.3.0)

To upgrade Oracle Adaptive Access Manager, you must use the Oracle Identity and Access Management 11.1.2.3.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.1.x.x Middleware Home. Your Oracle Home is upgraded from 11.1.1.x.x to 11.1.2.3.0.

For information about upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.x.x), see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 13.7 Upgrading OAAM, MDS, IAU, and OPSS Schemas

You must upgrade the following schemas using Patch Set Assistant:

- OAAM schema
- MDS schema
- OPSS schema

---

---

**Note:** If OPSS schema is not part of the source, a new OPSS schema must be created first, using 11.1.1.9.0 RCU, and only then can it be upgraded. You must create Oracle Platform Security Services (OPSS) schema because Oracle Adaptive Access Manager upgrade process involves OPSS schema policy store changes. Keys, roles, permissions, and other artifacts used by the applications must migrate to the policy store.

Run the Repository Creation utility (RCU) to create the OPSS schema. For more information, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

---

---

- IAU schema (You must upgrade Audit schema (IAU) only if it is part of your 11.1.1.x.x schemas.

---

**Note:** When upgrading schemas using Patch Set Assistant, you must select **OAAM** or **OAAM\_PARTN** as appropriate, and provide details on all screens to complete the upgrade.

---

For information about upgrading schemas using Patch Set Assistant, see [Section 24.1.4, "Upgrading Schemas Using Patch Set Assistant"](#).

## 13.8 Extending Oracle Adaptive Access Manager 11.1.1.x.x Component Domains with OPSS Template

Oracle Adaptive Access Manager 11.1.2.3.0 uses the database to store policies. This requires extending the 11.1.1.x.x Oracle Adaptive Access Manager domain to include the OPSS data source.

To do so, complete the following steps:

1. Run the following command to launch the Oracle Fusion Middleware configuration wizard:

**On UNIX:**

```
./config.sh
```

It is located in the <MW\_HOME>/<Oracle\_IDM1>/common/bin directory.

**On Windows:**

```
config.cmd
```

It is located in the <MW\_HOME>\<Oracle\_IDM1>\common\bin directory.

2. On the **Welcome** screen, select the **Extend an existing WebLogic domain** option. Click **Next**.
3. On the **Select a WebLogic Domain Directory** screen, browse to the directory that contains the WebLogic domain in which you configured the components. Click **Next**. The **Select Extension Source** screen is displayed.
4. On the **Select Extension Source** screen, select the **Oracle Platform Security Service - 11.1.1.0 [Oracle\_IDM1]** option. After selecting the domain configuration options, click **Next**.
5. The **Configure JDBC Data Sources** screen is displayed. Configure the **opssDS** data source, as required. After the test succeeds, the **Configure JDBC Component Schema** screen is displayed.
6. On the **Configure JDBC Component Schema** screen, select the **Oracle Platform Security Services** schema.  
  
You can set values for Schema Owner, Schema Password, Database and Service, Host Name, and Port. Click **Next**.  
  
The **Test JDBC Component Schema** screen is displayed. After the test succeeds, the **Select Optional Configuration** screen is displayed.
7. On the **Select Optional Configuration** screen, you can configure Managed Servers, Clusters, and Machines and Deployments and Services. Do not select

anything as you have already configured in your Oracle Identity and Access Management 11.1.1.x.x environment. Click **Next**.

8. On the **Configuration Summary** screen, review the domain configuration, and click **Extend** to start extending the domain.

Your existing Oracle Adaptive Access Manager domain is extended to support Oracle Platform Security Services (OPSS).

## 13.9 Upgrading Oracle Platform Security Services

---

---

**Note:** The upgrade steps need to be performed only if OPSS has already been configured.

---

---

After you upgrade schemas, you must upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Adaptive Access Manager to 11.1.2.3.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see [Section 24.1.7, "Upgrading Oracle Platform Security Services"](#).

## 13.10 Configuring OPSS Security Store

---

---

**Note:** You need to configure OPSS Security Store only if it was not configured during the previous installation. If it has already been configured, perform the steps to upgrade OPSS. For more information, see [Section 13.9, "Upgrading Oracle Platform Security Services"](#).

---

---

You must configure the database Security Store as it is the only security store type supported by Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For more information on configuring Oracle Platform Security Services, see "Configuring Database Security Store for an Oracle Identity and Access Management Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 13.11 Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers

---

---

**Note:** When you start the Administration Server and the Managed Servers, the Adaptive Access Manager Administration console application and the Access Manager Managed server application may start with a number of errors and exceptions. This is expected and can be ignored. These issues are resolved by the subsequent redeployment process.

---

---

The `redeploy` command is an online WLST command. Therefore, you must start the Oracle Adaptive Access Manager Administration and Managed Servers before running the `redeploy` command.

For information about starting the Administration Server and Oracle Adaptive Access Manager Managed servers, see ["Starting the Servers"](#) on page 24-11.

## 13.12 Redeploying the Applications

You must redeploy changes to the applications in the domain after upgrading Oracle Adaptive Access Manager to 11.1.2.3.0. Redeploy your 11.1.1.x.x application on the Oracle Adaptive Access Manager 11.1.2.3.0 servers.

You can redeploy the application using command line or using the WebLogic Administration console. Complete the following steps described in one of the following sections to redeploy applications:

- [Redeploying Applications Using Command Line](#)
- [Redeploying Applications Using WebLogic Administration Console](#)

### Redeploying Applications Using Command Line

To redeploy applications on Oracle Adaptive Access Manager 11.1.2.3.0 servers using command line, do the following:

1. Run the following command from the location `IAM_HOME/common/bin` to launch the WebLogic Scripting Tool (WLST):

On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

2. Connect to the Administration Server using the following command:

```
connect('weblogic-username','weblogic-password','weblogic-url')
```

For example:

```
connect('wlsuser','wlspassword','localhost:7001')
```

3. Run the following command to undeploy OAAM:

```
undeploy('oaam_admin')
```

```
undeploy('oaam_server')
```

```
undeploy('oracle.oaam.extensions')
```

---

**Note:** If you have Oracle Adaptive Access Manager Offline Server in your setup, run the `undeploy()` command to undeploy `'oaam_offline'` too.

---

For more information about using the `undeploy` command, see ["undeploy"](#) in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

4. Deploy the `oaam.extension` library application by running the following command:

```
deploy('oracle.oaam.extensions','$IAM_HOME/oaam/oaam_extensions/generic/oracle.oaam.extensions.war','oaam_admin_server1,oaam_server_server1','nostage',libraryModule='true')
```

---

---

**Note:** If you have Oracle Adaptive Access Manager Offline Server in your setup, add `oaam_offline_server1` to the list of targets while deploying `oaam.extension` library.

---

---

For more information about using the `deploy` command, see "deploy" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

5. Deploy the OAAM applications by running the following commands:

```
deploy('oaam_admin', '$IAM_HOME/oaam/oaam_admin/ear/oaam_admin.ear', 'oaam_admin_server1', 'nostage')
```

```
deploy('oaam_server', '$IAM_HOME/oaam/oaam_server/ear/oaam_server.ear', 'oaam_server_server1', 'nostage')
```

The target servers for each deployments are as follows:

- `oaam_admin` - Target: `oaam_admin_server1`
- `oaam_server` - Target: `oaam_server_server1`

---

---

**Note:** If you have Oracle Adaptive Access Manager Offline Server in your setup, deploy `'oaam_offline'` to the target `'oaam_offline_server1'` by running the `deploy()` command.

---

---

For more information about using the `deploy` command, see "deploy" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

6. Optional: If you had deployed the OAAM shared library, run the following command to redeploy it:

```
redeploy('oracle.oaam.libs')
```

7. Exit the WLST console using the `exit()` command.

### Redeploying Applications Using WebLogic Administration Console

To redeploy applications on Oracle Adaptive Access Manager 11.1.2.3.0 servers using WebLogic Administration console, do the following:

1. Log in to the WebLogic Administration console using the following URL:

```
http://admin_host:admin_port/console:
```

2. Go to the **Deployments** tab.
3. Select `oaam_admin`, `oaam_server` and `oracle.oaam.extensions` from **Deployments** and click **Delete**.
4. Deploy the following applications by clicking **Install**:

- `oracle.oaam.extensions` - Target should be `oaam_server_server1`, `oaam_admin_server1`.

---

---

**Note:** Ensure that `oracle.oaam.extensions` is deployed before you deploy other applications.

---

---

- `oaam_admin` - Target should be `oaam_admin_server1`.
- `oaam_server` - Target should be `oaam_server_server1`.

## 13.13 Deleting Folders

To deploy Oracle Adaptive Access Manager 11.1.1.x.x server content and applications in Oracle Adaptive Access Manager 11.1.2.3.0, you must delete all content of folders in the following locations:

### On UNIX:

Deleting tmp:

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_ADMIN_SERVER_NAME>/tmp
```

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_MANAGED_SERVER_NAME>/tmp
```

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_OFFLINE_SERVER_NAME>/tmp
```

Deleting stage:

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_ADMIN_SERVER_NAME>/stage
```

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_MANAGED_SERVER_NAME>/stage
```

```
<MW_Home>/user_projects/domains/domain_home/servers/<OAAM_OFFLINE_SERVER_NAME>/stage
```

### On Windows:

Deleting tmp:

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_ADMIN_SERVER_NAME>\tmp
```

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_MANAGED_SERVER_NAME>\tmp
```

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_OFFLINE_SERVER_NAME>\tmp
```

Deleting stage:

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_ADMIN_SERVER_NAME>\stage
```

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_MANAGED_SERVER_NAME>\stage
```

```
<MW_Home>\user_projects\domains\domain_home\servers\<OAAM_OFFLINE_SERVER_NAME>\stage
```

## 13.14 Restarting the Servers

To restart the Administration Server or Managed Servers, you must stop the running Administration Server or Managed Servers first before starting them again.

To stop the servers, see [Section 13.3, "Shutting Down Administration Server and Managed Servers"](#).

To start the servers, see [Section 13.11, "Starting the Administration Server and Oracle Adaptive Access Manager Managed Servers"](#).

---

---

**Note:** After all the upgrade steps are complete, check to make sure that the custom extensions (if any) are working correctly.

---

---

## 13.15 Verifying the Upgrade

Use the following URL in a web browser to verify that Oracle Adaptive Access Manager 11.1.2.3.0 is running:

`http://<oaam_host>:<oaam_port>/oaam_admin`

Assign the investigator role and verify to see the investigator UI.

---

---

## Upgrading Oracle Identity Manager 11g Release 1 (11.1.1.x.x) Environments

This chapter describes how to upgrade your existing Oracle Identity Manager 11g Release 1 (11.1.1.5.0) and 11g Release 1 (11.1.1.7.0) environments to Oracle Identity Manager 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

---

---

**Note:** This chapter refers to Oracle Identity Manager 11g Release 1 (11.1.1.5.0) and 11g Release 1 (11.1.1.7.0) environments as 11.1.1.x.x.

---

---

This chapter includes the following sections:

- [Section 14.1, "Upgrade Roadmap for Oracle Identity Manager"](#)
- [Section 14.2, "Performing the Required Pre-Upgrade Tasks"](#)
- [Section 14.3, "Upgrading Oracle Home"](#)
- [Section 14.4, "Creating Necessary Schemas and Upgrading the Existing Schemas"](#)
- [Section 14.5, "Upgrading Oracle Identity Manager Middle Tier"](#)
- [Section 14.6, "Upgrade Other Oracle Identity Manager Installed Components"](#)
- [Section 14.7, "Performing the Required Post-Upgrade Tasks"](#)
- [Section 14.8, "Verifying the Oracle Identity Manager Upgrade"](#)
- [Section 14.9, "Troubleshooting"](#)

---

---

**Note:** Oracle Identity Manager upgrade scripts from 11.1.1.x.x to 11.1.2.3.0 create application instances during the upgrade process. The application instances that are created will be based on the existing accounts and their data. For active accounts that have an IT Resource field on the process form, whose value is populated on the process form, corresponding application instances will be created for the specific Resource Object+ITResource combination.

---

---

## 14.1 Upgrade Roadmap for Oracle Identity Manager

The procedure for upgrading Oracle Identity Manager 11.1.1.x.x to 11.1.2.3.0 involves the following high-level steps:

1. **Performing the Required Pre-Upgrade Tasks:** This step involves tasks like generating the pre-upgrade report, analyzing the report and performing the necessary pre-upgrade tasks described in the report, shutting down the servers, backing up the 11.1.1.x.x environment and so on.
2. **Upgrading Oracle Home:** This step involves tasks like upgrading Oracle WebLogic Server to 10.3.6, upgrading Oracle SOA Suite to 11.1.1.9.0, and upgrading Oracle Identity Manager to 11.1.2.3.0.
3. **Creating Necessary Schemas and Upgrading the Existing Schemas:** This step involves tasks like creating necessary schemas like Oracle BI Publisher (BIP) schema and Oracle Platform Security Services (OPSS) schema using Repository Creation Utility 11.1.2.3.0, and upgrading the existing schemas using the Patch Set Assistant.
4. **Upgrading Oracle Identity Manager Middle Tier:** This step involves tasks like upgrading Oracle Identity Manager middle tier, starting the servers, patching the Oracle Identity Manager MDS metadata and so on.
5. **Upgrading Other Oracle Identity Manager Installed Components:** This step involves tasks like upgrading Oracle Identity Manager Design Console, Oracle Identity Manager Remote Manager, and configuring BI Publisher Reports.
6. **Performing the Required Post-Upgrade Tasks:** This step involves the post-upgrade tasks like enabling Oracle Identity Manager - Oracle Access Manager integration, upgrading user UDF, customizing event handlers, upgrading SOA composites and so on.

[Table 14-1](#) lists the steps to upgrade Oracle Identity Manager 11.1.1.x.x.

---

---

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Identity Manager upgrade may not be successful.

---

---

**Table 14–1 Upgrade Roadmap**

SI No	Task	For More Information
1	<p>Complete the following pre-upgrade tasks.</p> <ol style="list-style-type: none"> <li>1. Review the new features of Oracle Identity Manager 11.1.2.3.0.</li> <li>2. Review system requirements and certifications.</li> <li>3. Ensure that you are using a supported JDK version.</li> <li>4. Review the Oracle Identity Manager customizations that are lost or overwritten as part of the upgrade.</li> <li>5. Generate the pre-upgrade report by running the <code>PreUpgradeReport</code> utility.</li> <li>6. Ensure that <code>getPlatformTransactionManager ( )</code> method is not used in custom code.</li> <li>7. Empty the <code>oimProcessQueue</code> JMS queue to ensure that JMS messages are processed before you start upgrading.</li> <li>8. Complete the other pre-requisite tasks.</li> <li>9. In Oracle Identity Manager 11.1.1.x.x, if you do not have at least one reconciliation field of type <code>IT Resource</code>, then you must create one for all account type profiles.</li> <li>10. Stop all the servers. This includes the Node Manager, WebLogic Administration Server, SOA Managed Server(s), and Oracle Identity Manager Managed Server(s).</li> <li>11. Back up your existing Oracle Identity Manager 11.1.1.x.x environment.</li> </ol>	See, <a href="#">Performing the Required Pre-Upgrade Tasks</a>
2	<p>Upgrade the Oracle Home by complete the following tasks:</p> <ol style="list-style-type: none"> <li>1. Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6.</li> <li>2. Upgrade Oracle SOA suite to 11g Release 1 (11.1.1.9.0).</li> <li>3. Upgrade Oracle Identity Manager binaries to 11.1.2.3.0.</li> </ol>	See, <a href="#">Upgrading Oracle Home</a>

**Table 14–1 (Cont.) Upgrade Roadmap**

SI No	Task	For More Information
3	Create the Oracle BI Publisher (BIP) schema and Oracle Platform Security Services (OPSS) schema using the Repository Creation Utility (RCU), and upgrade your existing database schemas using the Patch Set Assistant (PSA).	See, <a href="#">Creating Necessary Schemas and Upgrading the Existing Schemas</a>
4	Upgrade the Oracle Identity Manager middle tier. This is done by running the OIM middle tier upgrade utility <code>OIMUpgrade.sh</code> or <code>OIMUpgrade.bat</code> in offline and online mode.	See, <a href="#">Upgrade Other Oracle Identity Manager Installed Components</a>
5	Upgrade other Oracle Identity Manager installed components like Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager to 11.1.2.3.0.	See, <a href="#">Upgrade Other Oracle Identity Manager Installed Components</a>
6	Complete the required post-upgrade tasks.	See, <a href="#">Performing the Required Post-Upgrade Tasks</a>
7	Verify the upgraded environment.	See, <a href="#">Verifying the Oracle Identity Manager Upgrade</a>

## 14.2 Performing the Required Pre-Upgrade Tasks

This section describes the pre-upgrade tasks that you must complete before you upgrade the Oracle Identity Manager 11.1.1.x.x environments:

- [Comparing the Features of Oracle Identity Manager 11.1.1.x.x and 11.1.2.3.0](#)
- [Reviewing System Requirements and Certification](#)
- [Ensuring that you are Using a Certified JDK Version](#)
- [Reviewing the Customizations that are Lost or Overwritten as Part of Upgrade](#)
- [Generating and Analyzing the Pre-Upgrade Report](#)
- [Ensuring That `getPlatformTransactionManager\(\)` Method is Not Used in Custom Code](#)
- [Emptying the `oimProcessQueue` JMS Queue](#)
- [Other Prerequisites](#)
- [Creating Reconciliation Field of Type IT Resource](#)
- [Shutting Down Node Manager, Administration Server and Managed Servers](#)
- [Backing Up Oracle Identity Manager 11g Release 1 \(11.1.1.x.x\)](#)

### 14.2.1 Comparing the Features of Oracle Identity Manager 11.1.1.x.x and 11.1.2.3.0

[Table 14–2](#) lists the key differences in functionality between Oracle Identity Manager 11.1.1.x.x and Oracle Identity Manager 11g Release 2 (11.1.2.3.0).

**Table 14–2 Features Comparison**

<b>Oracle Identity Manager 11.1.1.x.x</b>	<b>Oracle Identity Manager 11.1.2.3.0</b>
<p>Oracle Identity Manager 11.1.1.x.x provided separate interfaces for end user self-service and delegated administration.</p>	<p>In Oracle Identity Manager 11.1.2.3.0, the end user self-service and delegated administration consoles are unified into a single self-service console to simplify administration and self service. Oracle Identity Manager 11.1.2.3.0 uses the Alta skin which is business (mobile, cloud) friendly. OIM 11.1.2.3.0 has a new Home page, new my profile page with user friendly inbox.</p>
<p>User Interface (UI) relied on the classic UI customization model where developers would edit the back end code, deploy it to an application server, and finally validate the changes from a browser. This was required for minor changes such as changes to logos, label, font, button, etc.</p>	<p>UI customization is simplified using Sandboxing and web composer.</p>
<p>In Oracle Identity Manager 11.1.1.x.x, administrators configured request templates to control what an end user could request.</p>	<p>Most of the customizations need to be redone to match the look and feel of Oracle Identity Manager 11.1.2.3.0.</p>
<p>End users have to navigate through a series of menus to select entitlement before they can submit and access request.</p>	<p>Oracle Identity Manager 11.1.2.3.0 provides a new user interface with a shopping cart-type request model through which end users can search and browse through the catalog, and directly request any item such as roles, entitlements, or applications, without having to navigate through a series of menus.</p>
<p>An end user's access to request templates was controlled by his/her role memberships.</p>	<p>In addition to this, several business-friendly metadata such as description, audit objective, tags, owner, approver, technical glossary, and so on, can be associated to each access item, to display business-friendly and rich contextual information to a business user at the time of self service access request and access review.</p>
	<p>UDFs which are marked as searchable will automatically be part of advance search form.</p>
	<p>You can customize the search form. Attributes can be used to search catalog items. Catalog as single point for managing access.</p>

**Table 14–2 (Cont.) Features Comparison**

Oracle Identity Manager 11.1.1.x.x	Oracle Identity Manager 11.1.2.3.0
<p>In Oracle Identity Manager 11.1.1.x.x, Resource and IT resource names are named in a manner such that it is easy for the IT users to manage them. The problem with this approach is that, if a business user has to request access, the resource name will not make sense to the user. These incomprehensible Resource and IT resource names make the access request process non-intuitive.</p>	<p>Oracle Identity Manager 11.1.2.3.0 provides an abstraction entity called Application Instance. It is a combination of IT resource instance (target connectivity and connector configuration) and resource object (provisioning mechanism). Administrators can assign business friendly names to Application instances and map them to corresponding IT resources and Resource Objects.</p>
<p>Oracle Identity Manager 11.1.1.x.x had to be integrated with Oracle Identity Analytics (OIA) to leverage the advanced access review capabilities.</p>	<p>End users who request for accounts through the catalog will search for an account by providing the business friendly Application Instance Name.</p>
<p>In Oracle Identity Manager 11.1.1.x.x, authorization policies were used to control a user's access to the functions within Oracle Identity Manager. Policy administration was done through a UI that was built specifically for Oracle Identity Manager</p>	<p>Application instances are automatically created as part of the upgrade procedure. Administrators are expected to define organization publishing for these Application Instances to control who has access to request for access to the application.</p>
<p>The existing 11.1.1.x.x certification feature provides certifier selection based on User Manager, Organization Manager, Catalog Owner and Selected User.</p>	<p>In 11.1.2.3.0, the functionality of Oracle Identity Analytics is ported into Oracle Identity Governance (OIG). You can define and manage identity audit policies based on IDA rules. You can define owners and remediators for a policy, which can be a specific user, a list of users, or an OIM role. You can use preventive and detective scan capabilities which can create actionable policy violations.</p>
<p>Till Oracle Identity Manager 11.1.1.x.x, policies were implemented and customized using OIM plug-in, and pre-pop adapters implemented via plug-in framework, which required writing custom java code to extend and customize OOTB policies.</p>	<p>Oracle Identity Manager 11.1.2.3.0 has comprehensive role lifecycle management and workflow approval capabilities with direct involvement from business, featuring a business friendly User Interface. It also includes detailed Role Analytics to aid with the composition and modifications of roles.</p>
<p>In Oracle Identity Manager 11.1.1.x.x, authorization policies were used to control a user's access to the functions within Oracle Identity Manager. Policy administration was done through a UI that was built specifically for Oracle Identity Manager</p>	<p>Oracle Identity Manager 11.1.2.3.0 provides a fine grained authorization engine to help you create various admin roles. For example, by using attributes to define membership, you can restrict an administrator to managing home organization members only.</p>
<p>The existing 11.1.1.x.x certification feature provides certifier selection based on User Manager, Organization Manager, Catalog Owner and Selected User.</p>	<p>Oracle Identity Manager 11.1.2.3.0 introduces additional certifier selection where role can be used to define certifiers. All members of a certifier role can see the certification in their inbox, but the first member who 'claims' the certification will be the primary reviewer for that certification.</p>
<p>Till Oracle Identity Manager 11.1.1.x.x, policies were implemented and customized using OIM plug-in, and pre-pop adapters implemented via plug-in framework, which required writing custom java code to extend and customize OOTB policies.</p>	<p>Oracle Identity Manager 11.1.2.3.0 introduces declarative policies that enable you to define and configure various policy types that are evaluated at run time. Policy is configured via a UI/API rather than customized via Java plug-in or pre-pop adapter.</p>

**Table 14–2 (Cont.) Features Comparison**

Oracle Identity Manager 11.1.1.x.x	Oracle Identity Manager 11.1.2.3.0
Oracle Identity Manager 11.1.1.x.x had SOA based approval workflows. Request templates are provided to create various request.	Oracle Identity Manager 11.1.2.3.0 includes a number of enhancements to the request workflow.  Temporal grants allow the requester to specify the start and end date (grant duration) of the role, account and entitlements at the time of assignment.  Administrators can configure approvals by creating workflow policy rules instead of approval policies. It also supports role requests (create, modify, delete etc).Also, now enabling SOA is optional.
In Oracle Identity Manager 11.1.1.x.x, Lookup queries were supported.	In Oracle Identity Manager 11.1.2.3.0, Lookup queries are not supported.

## 14.2.2 Reviewing System Requirements and Certification

Before you start the upgrade process, review the *Oracle Fusion Middleware System Requirements and Specifications* and *Oracle Fusion Middleware Supported System Configurations* documents to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).

## 14.2.3 Ensuring that you are Using a Certified JDK Version

Ensure that you are using a Java Development Kit (JDK) version that is supported and certified with Oracle Identity and Access Management 11.1.2.3.0.

You can verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

---

**Note:** For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

---

## 14.2.4 Reviewing the Customizations that are Lost or Overwritten as Part of Upgrade

This section lists the customizations that will be lost or overwritten as part of the upgrade process.

The following customizations will be lost or overwritten as part of the Oracle Identity Manager upgrade process:

- The configuration files like `web.xml` that are directly manipulated for changing the session time out will be overwritten as part of the binary upgrade.
- The custom JARs included in the OIM Home will be lost as part of the binary upgrade.

- Oracle Identity Manager Design Console configuration settings will be lost as part of the binary upgrade.
- Oracle Identity Manager Remote Manager configuration settings will be lost as part of the binary upgrade.
- Customizations done to Email Validation Pattern will be overwritten as part of the upgrade process.
- All UI customizations will be lost as Oracle Identity Manager 11.1.2.3.0 uses a different UI model compared to Oracle Identity Manager 11.1.1.x.x.
- The following scripts will be modified as part of the Oracle Identity Manager middle tier upgrade offline.
  - Startup scripts - `startWebLogic.sh` and `startManagedWebLogic.sh` located at `DOMAIN_HOME/bin/` (on UNIX), `startWebLogic.cmd` and `startManagedWebLogic.cmd` located at `DOMAIN_HOME\bin\` (on Windows)
  - Domain environment script - `setDomainEnv.sh` located at `DOMAIN_HOME/bin/` (on UNIX), `setDomainEnv.bat` located at `DOMAIN_HOME\bin\` (on Windows)
  - Unprotected Metadata files
 

For the list of protected metadata files for which the customizations will be retained after upgrade, see [Section 24.2.1, "Protected Metadata Files for Which Customization will be Retained After Upgrade"](#).

Any manual edits done to these scripts will be overwritten. Therefore, you must revisit these after middle tier upgrade offline.
- If you have SSL configured environment, the file `ORACLE_HOME\designconsole\config\xl.policy` will be overwritten as part of the Oracle Identity Manager binary upgrade. Therefore, backup the `xl.policy` file if you have customized it, before you begin with the upgrade process.

## 14.2.5 Generating and Analyzing the Pre-Upgrade Report

You must run the pre-upgrade utility before you begin the upgrade process, and address all the issues listed as part of this report with the solution provided in the report.

The pre-upgrade utility analyzes your existing Oracle Identity Manager 11.1.1.x.x environment, and provides information about the mandatory prerequisites that you must complete before you upgrade environment. The information in the pre-upgrade report is related to the invalid approval policies, requests and event handlers that are affected by the upgrade, list of mandatory Database components that need to be installed before upgrade, cyclic groups in LDAP directory, deprecated authorization policies, and issues in creating potential application instance.

For information about generating the pre-upgrade report, and analyzing it, see [Section 24.2.2, "Generating and Analyzing Pre-Upgrade Report for Oracle Identity Manager"](#).

---



---

**Note:** It is important to address all the issues listed in the pre-upgrade report, before you can proceed with the upgrade, as upgrade might fail if the issues are not fixed.

Run this report until no pending issues are listed in the report.

---



---

## 14.2.6 Ensuring That `getPlatformTransactionManager()` Method is Not Used in Custom Code

Ensure that the method `getPlatformTransactionManager()` is not used in the custom event handler code, as this method is not available in 11.1.2.3.0.

If you are using the method `getPlatformTransactionManager()` in the custom event handler code, set the attribute `tx` to `TRUE` in the event handler XML definition.

For more information on setting the attributes in the event handler XML definition, see "Defining Custom Events Definition XML" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

## 14.2.7 Emptying the `oimProcessQueue` JMS Queue

Offline Provisioning is not supported in Oracle Identity Manager 11.1.2.3.0, as it is no longer needed on Oracle Identity Manager 11.1.2.3.0.

Empty the `oimProcessQueue` JMS queue to ensure that JMS messages are processed before you start upgrading. To do so, complete the following:

1. Shut down applications to disable accessing of Oracle Identity Manager offline provisioning by end-users, SPML, and API clients.
2. Monitor the `oimProcessQueue` JMS queue from the WebLogic Administration Console and allow Oracle Identity Manager to run, till `oimProcessQueue` JMS queue is empty.

## 14.2.8 Other Prerequisites

This is a list of checks you must run and set before you begin upgrading:

- The OOTB applications in Oracle Identity Manager are deployed in `NO_STAGE` mode. Check if `oracle.idm.uishell` is in `No Stage` mode. If `oracle.idm.uishell` is in `Stage` mode, you must re-deploy it to `NO_STAGE` mode.

Complete the following steps to change the mode to `No Stage`:

1. Set the `WL_HOME` and `OIM_HOME`.
2. Undeploy `oracle.idm.uishell` by running the following command:

```
java -cp $WL_HOME/server/lib/weblogic.jar weblogic.Deployer
-adminurl t3://localhost:8005 -username weblogic -password
weblogic1 -undeploy -name oracle.idm.uishell
```

3. Deploy `oracle.idm.uishell` in stage mode by running the following command:

```
java -cp $WL_HOME/server/lib/weblogic.jar weblogic.Deployer
-adminurl t3://localhost:8005 -username weblogic -password
weblogic1 -deploy -name oracle.idm.uishell -source $OIM_
HOME/modules/oracle.idm.uishell_11.1.1/oracle.idm.uishell.war
-nostage -library -targets AdminServer,$OIM_SERVER_NAME
```

- In case of a migrated, upgraded, or restored database in the Oracle Identity Manager environment, you must synchronize all the Oracle Identity Manager Schema Privileges (SYSTEM and OBJECT Grants) from the source to the target (restored) schema by doing the following:
  1. Capture the OIM Database Schema user constituent grants from the source schema by executing the following SQLs as `SYS` database user:

- SELECT DBMS\_METADATA.GET\_GRANTED\_DDL ('SYSTEM\_GRANT', '<OIM\_Schema\_Name>') FROM DUAL;
- SELECT DBMS\_METADATA.GET\_GRANTED\_DDL ('OBJECT\_GRANT', '<OIM\_Schema\_Name>') FROM DUAL;

2. In the schema restoration phase prior to schema upgrade, execute the grants output of the SQLs captured in step-1, as post schema restoration step.
3. Recompile any INVALID objects in the OIM schema using the following steps:

a. Identify INVALID schema objects as SYS user by running the following SQL:

```
SELECT owner,object_type,object_name,status FROM dba_objects WHERE
status = 'INVALID' AND owner in ('<OIM_Schema_Name1>') ORDER BY
owner, object_type, object_name;
```

b. Compile the INVALID schema objects using any appropriate method. The following is an example of compiling INVALID schema objects by executing the method UTL\_RECOMP as SYS user for the OIM schema:

```
BEGIN
UTL_RECOMP.recomp_serial('<OIM_SCHEMA_NAME>');
END
```

---



---

**Note:** For information on schema backup and restoration using Data Pump Client Utility for Oracle Identity Manager 11g Release 1, see My Oracle Support document ID 1359656.1.

For information on schema backup and restoration using Data Pump Client Utility for Oracle Identity Manager 11g Release 2, see My Oracle Support document ID 1492129.1.

---



---

## 14.2.9 Creating Reconciliation Field of Type IT Resource

All account reconciliation Field Mapping configurations must have at least one Reconciliation field of type `ITResource` defined. This can be done by adding a mapping from the Oracle Identity Manager Design Console. Complete the following steps for those resource objects which do not have `ITResource` filed in reconciliation field mapping:

1. Create reconciliation field of type `IT Resource` by doing the following:
  - a. Log in to the Oracle Identity Manager Design Console by running the following command from the location `ORACLE_HOME/designconsole/`:
    - On UNIX: `./xlclient.sh`
    - On Windows: `xlclient.cmd`
  - b. Expand **Resource Management**.
  - c. Click **Resource Objects**.
  - d. Search for and select the Resource Object that you wish to modify.
  - e. Go to the **Object Reconciliation** tab.
  - f. Click **Add Field** under **Reconciliation Fields** tab.
  - g. Enter the Field Name, and select **IT Resource** as the **Field Type**.
  - h. Click Save icon.

2. Define mapping for the field `ITResource` by doing the following:
  - a. On the Oracle Identity Manager Design Console, expand **Process Management** on the left navigation pane.
  - b. Click **Process Definition**.
  - c. Go to the **Reconciliation Field Mapping** tab in the **Process Definition** form.
  - d. Search for the Resource Object.
  - e. Define mapping for the field **IT Resource**.
  - f. Save the form.

---

**Note:** This step is required if you are using connector for account reconciliation or if you wish to use connector for account reconciliation after you upgrade to 11.1.2.3.0.

---

## 14.2.10 Shutting Down Node Manager, Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Managed Servers, Administration Server, and the Node Manager.

---

**Note:** When shutting down the servers, the following error message might be displayed:

```
** SOA specific environment is already set. Skipping ...
*****
OIM specific environment is already set. Skipping ...
The input line is too long.
The syntax of the command is incorrect.
```

It is recommended that you open a new command prompt and then run the commands for shutting down the servers.

---

**Note:** If you are upgrading highly available environment, you must shut down the servers on all of the hosts.

---

For information about stopping the servers, see [Section 24.1.9, "Stopping the Servers"](#).

## 14.2.11 Backing Up Oracle Identity Manager 11g Release 1 (11.1.1.x.x)

You must back up your old Oracle Identity Manager 11.1.1.x.x environment before you upgrade to Oracle Identity Manager 11g Release 2 (11.1.2.3.0).

After stopping the servers, back up the following:

- `MW_HOME` directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Identity Manager schemas
- MDS schema

- ORASDPM schema
- SOAINFRA schemas

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

---

---

**Note:** If you are upgrading highly available environment, you must back up the Oracle Home directories and the domain home directories on all of the hosts.

---

---

## 14.3 Upgrading Oracle Home

This section describes the tasks to be completed to upgrade the existing Oracle home.

---

---

**Note:** Before you begin with the upgrade process, make sure that you have read and write permission to the domain including the `/security/SerializedSystemIni.dat` file.

---

---

This section includes the following topics:

- [Upgrading Oracle WebLogic Server to 10.3.6](#)
- [Upgrading Oracle SOA Suite to 11.1.1.9.0](#)
- [Upgrading Oracle Identity Manager Binaries to 11.1.2.3.0](#)

### 14.3.1 Upgrading Oracle WebLogic Server to 10.3.6

Oracle Identity and Access Management 11.1.2.3.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Identity Manager environment is using Oracle WebLogic Server 10.3.5 or any earlier version, you must upgrade it to Oracle WebLogic Server 10.3.6.

---

---

**Note:** If you are already using Oracle WebLogic Server 10.3.6, ensure that you apply the mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server 10.3.6, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

---

---

For information about upgrading Oracle WebLogic Server, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

### 14.3.2 Upgrading Oracle SOA Suite to 11.1.1.9.0

Oracle Identity Manager 11.1.2.3.0 is certified with Oracle SOA Suite 11.1.1.9.0. Therefore, you must upgrade Oracle SOA Suite to 11.1.1.9.0 if you are using any earlier version.

For information about upgrading Oracle SOA Suite, see [Section 24.2.3, "Upgrading Oracle SOA Suite to 11g Release 1 \(11.1.1.9.0\)"](#).

### 14.3.3 Upgrading Oracle Identity Manager Binaries to 11.1.2.3.0

To upgrade Oracle Identity Manager binaries to 11.1.2.3.0, you must use the Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) Installer. During the procedure, point the Middleware Home to your existing 11.1.1.x.x Middleware Home. Your Oracle Home is upgraded from 11.1.1.x.x to 11.1.2.3.0.

---



---

**Note:** Before upgrading the Oracle Identity Manager binaries to 11g Release 2 (11.1.2.3.0), you must ensure that the OPatch version in *ORACLE\_HOME* and *MW\_HOME/oracle\_common* is 11.1.0.10.3. Different OPatch version might cause patch application failure. If you have upgraded opatch to a newer version, you will have to roll back to version 11.1.0.10.3.

---



---

For information about upgrading Oracle Identity Manager 11g Release 1 (11.1.1.x.x), see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

After the binary upgrade, check the installer logs at the following location:

- On UNIX: *ORACLE\_INVENTORY\_LOCATION*/logs

To find the location of the Oracle Inventory directory on UNIX, check the file *ORACLE\_HOME/oraInst.loc*.

- On Windows: *ORACLE\_INVENTORY\_LOCATION*\logs

The default location of the Oracle Inventory Directory on Windows is C:\Program Files\Oracle\Inventory\logs.

The following install log files are written to the log directory:

- installDATE-TIME\_STAMP.log
- installDATE-TIME\_STAMP.out
- installActionsDATE-TIME\_STAMP.log
- installProfileDATE-TIME\_STAMP.log
- oraInstallDATE-TIME\_STAMP.err
- oraInstallDATE-TIME\_STAMP.log

## 14.4 Creating Necessary Schemas and Upgrading the Existing Schemas

This section describes the tasks to be completed to upgrade Database schemas.

This section includes the following topics:

- [Creating Necessary Database Schemas](#)
- [Upgrading Existing Schemas](#)

### 14.4.1 Creating Necessary Database Schemas

You must create the following database schemas using Repository Creation Utility (RCU) 11.1.1.9.0.

- Oracle Platform Security Store (OPSS) schema
- Oracle BI Publisher (BIP) schema

Oracle Identity Manager upgrade process involves OPSS schema policy store changes. Keys, roles, permissions, and other artifacts used by the applications must migrate to the policy store.

For more information about creating schemas, see [Section 24.1.3, "Creating Database Schemas Using Repository Creation Utility"](#).

---



---

**Note:** When you create schemas using Repository Creation Utility, select only Oracle Platform Security Store (OPSS) and Oracle BI Publisher (BIP) schemas on the **Select Components** screen.

Do not select any other schema.

---



---

## 14.4.2 Upgrading Existing Schemas

You must upgrade the existing Oracle Identity Manager (OIM) schema using Patch Set Assistant (PSA). When you select the Oracle Identity Manager Schema, it automatically selects all dependent schemas and upgrades them too.

For information about upgrading schemas using the Patch Set Assistant, see [Upgrading Schemas Using Patch Set Assistant](#).

After you upgrade schemas, verify the upgrade by checking the version numbers of the schemas as described in [Version Numbers After Upgrading Schemas](#).

### 14.4.2.1 Version Numbers After Upgrading Schemas

Run `select version,status,upgraded from schema_version_registry where owner=<SCHEMA_NAME>;` and ensure that the version numbers are upgraded, as listed in [Table 14–3](#):

**Table 14–3 Component Version Numbers After Upgrading the Schemas**

Component	Version No.
OPSS	11.1.1.9.0
MDS	11.1.1.9.0
Oracle Identity Manager	11.1.2.3.0
ORASDPM	11.1.1.9.0
SOAINFRA	11.1.1.9.0 (Make sure that you have upgraded SOA schemas as described in <a href="#">Section 24.1.4, "Upgrading Schemas Using Patch Set Assistant"</a> )

## 14.5 Upgrading Oracle Identity Manager Middle Tier

To upgrade Oracle Identity Manager middle tier, you must run the middle tier upgrade utility `OIMUpgrade` in offline and online mode. For more information about upgrading the Oracle Identity Manager middle tier, see [Section 24.2.4, "Upgrading Oracle Identity Manager Middle Tier"](#).

## 14.6 Upgrade Other Oracle Identity Manager Installed Components

After you upgrade the Oracle Identity Manager middle tier, you must upgrade the other Oracle Identity Manager installed components like Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager to 11.1.2.3.0.

For more information about upgrading Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager, see [Section 24.2.5, "Upgrading Other Oracle Identity Manager Installed Components"](#).

## 14.7 Performing the Required Post-Upgrade Tasks

After you upgrade Oracle Identity Manager 11.1.1.x.x to 11.1.2.3.0, you must perform the following post-upgrade tasks described in [Section 24.2.6, "Performing Oracle Identity Manager Post-Upgrade Tasks"](#):

- [After You Upgrade](#)
- [Enabling Oracle BI Publisher](#)
- [Reviewing Performance Tuning Recommendations](#)
- [Validating the Database Objects](#)
- [Impact of Removing Approver-Only Attribute in Request Data Set](#)
- [Changes to Request API After Upgrading to Oracle Identity Manager 11g Release 2 \(11.1.2.3.0\)](#)
- [Verifying the Compatibility of Oracle Identity Manager Integrated with Oracle Access Manager](#)
- [Running the Entitlement List Schedule](#)
- [Running the Evaluate User Policies Scheduled Task](#)
- [Running Catalog Synchronization](#)
- [UMS Notification Provider](#)
- [Upgrading User UDF](#)
- [Upgrading Application Instances](#)
- [Re XIMDD](#)
- [Re SPML-DSML](#)
- [Customizing Event Handlers](#)
- [Upgrading SOA Composites](#)
- [Authorization Policy Changes](#)
- [Creating Password Policies](#)
- [Creating PeopleSoft Enterprise HRMS Reconciliation Profile](#)
- [Reviewing OIM Data Purge Job Parameters](#)
- [Migrating Customized Oracle Identity Manager Reports Built on BI Publisher 10g to BI Publisher 11g](#)
- [Reviewing Connector Certification](#)
- [Verifying the Functionality of Connectors](#)
- [Updating the Provider URL For ForeignJNDIProvider-SOA](#)

- [Rebuilding the Indexes of Oracle Identity Manager Table to Change to Reverse Type](#)
- [Reviewing System Property](#)
- [Updating the URI of the Human Task Service Component with Oracle HTTP Server Details](#)
- [Migrating Approval Policies to Approval Workflow Rules](#)
- [Disabling Oracle SOA Suite Server](#)
- [Adjusting the Width of UDF Components](#)

## 14.8 Verifying the Oracle Identity Manager Upgrade

To verify your Oracle Identity Manager upgrade, perform the following steps:

1. Verify that Oracle Identity Manager 11.1.2.3.0 is running using the following URL:

`http://oim_host:oim_port/sysadmin`

`http://oim_host:oim_port/identity`

where

*oim\_host* is the host on which Oracle Identity Manager is running.

*oim\_port* is the port number.

2. Verify that Oracle BI Publisher 11.1.1.9.0 is running using the following URLs:

`http://bip_host:bip_port/xmlpserver`

where

*bip\_host* is the host on which Oracle BI Publisher is running.

*bip\_port* is the port number. The default HTTP port for BI Publisher is 9704, if not changed during upgrade.

3. Use Fusion Middleware Control to verify that Oracle Identity Manager and any other Oracle Identity Management components are running in the Oracle Fusion Middleware environment.

## 14.9 Troubleshooting

For the list of common issues that you might encounter during the Oracle Identity Manager upgrade process, and their workaround, see [Section 25.1, "Troubleshooting Oracle Identity Manager Upgrade Issues"](#).

For the list of known issues related to upgrade, and their workaround, see "Upgrade and Migration Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes for Identity Management*.

---

---

## Upgrading Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) Environment

This chapter describes how to upgrade your existing Oracle Entitlements Server 11g Release 1 (11.1.1.5.0) environment to Oracle Entitlements Server 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

This chapter includes the following sections:

- [Section 15.1, "Upgrading Oracle Entitlements Server Administration Server"](#)
- [Section 15.2, "Upgrading Oracle Entitlements Server Client Server"](#)

### 15.1 Upgrading Oracle Entitlements Server Administration Server

This section contains the following topics:

- [Section 15.1.1, "Upgrade Roadmap for Oracle Entitlements Server Administration Server"](#)
- [Section 15.1.2, "Performing the Required Pre-Upgrade Tasks"](#)
- [Section 15.1.3, "Shutting Down Administration Server and Managed Servers"](#)
- [Section 15.1.4, "Backing Up Oracle Entitlements Server 11g Release 1 \(11.1.1.5.0\)"](#)
- [Section 15.1.5, "Upgrading Oracle WebLogic Server to 10.3.6"](#)
- [Section 15.1.6, "Upgrading Oracle Entitlements Server Administration Server 11g Release 2 \(11.1.2.3.0\)"](#)
- [Section 15.1.7, "Creating Oracle Platform Security Service Schema"](#)
- [Section 15.1.8, "Executing R2\\_Upgrade.sql"](#)
- [Section 15.1.9, "Creating New Oracle Entitlements Server Domain"](#)
- [Section 15.1.10, "Exporting Encryption Key"](#)

- [Section 15.1.11, "Re-Associating Policy Stores"](#)
- [Section 15.1.12, "Deleting all py.class Files"](#)
- [Section 15.1.13, "Upgrading Oracle Platform Security Services"](#)
- [Section 15.1.14, "Starting the Administration Server and Oracle Entitlements Server Managed Servers"](#)
- [Section 15.1.15, "Redeploying APM"](#)
- [Section 15.1.16, "Verifying the Upgrade"](#)

## 15.1.1 Upgrade Roadmap for Oracle Entitlements Server Administration Server

---

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Entitlements Server Administration Server upgrade may not be successful.

---

[Table 15–1](#) lists the steps to upgrade Oracle Entitlements Server Administration Server upgrade.

**Table 15–1 Upgrade Flow**

Task No.	Task	For More Information
1	Review system requirements and certifications.	See, <a href="#">Performing the Required Pre-Upgrade Tasks</a>
2	Shut down all servers. This includes both Administration Server and Managed Servers.	See, <a href="#">Shutting Down Administration Server and Managed Servers</a>
3	Back up your environment.	See, <a href="#">Backing Up Oracle Entitlements Server 11g Release 1 (11.1.1.5.0)</a>
4	Upgrade Oracle WebLogic Server 10.3.5 to Oracle WebLogic Server 10.3.6.	See, <a href="#">Upgrading Oracle WebLogic Server to 10.3.6</a>
5	Upgrade 11.1.1.5.0 Oracle Home to 11.1.2.3.0.	See, <a href="#">Upgrading Oracle Entitlements Server Administration Server 11g Release 2 (11.1.2.3.0)</a>
6	Create new Oracle Platform Security Services schema.	See, <a href="#">Creating Oracle Platform Security Service Schema</a>
8	Execute R2_Upgrade.sql	See, <a href="#">Executing R2_Upgrade.sql</a>
9	Create new Oracle Entitlements Server domain.	See, <a href="#">Creating New Oracle Entitlements Server Domain</a>
10	Using the <code>exportEncryptionKey()</code> , extract the encryption key.	See, <a href="#">Exporting Encryption Key</a>
11	Run the <code>configuresecuritystore.py</code> script to re-associate policy stores.	See, <a href="#">Re-Associating Policy Stores</a>
12	Delete all the <code>py.class</code> files in the newly installed Oracle Entitlements Server home.	See, <a href="#">Deleting all py.class Files</a>
13	Upgrade Oracle Platform Security Services.	See, <a href="#">Upgrading Oracle Platform Security Services</a>

**Table 15–1 (Cont.) Upgrade Flow**

Task No.	Task	For More Information
14	Start the Administration Server and Oracle Entitlements Server Managed servers.	See, <a href="#">Starting the Administration Server and Oracle Entitlements Server Managed Servers</a>
15	Redeploy APM.	See, <a href="#">Redeploying APM</a>
16	Verify the Oracle Entitlements Server upgrade.	See, <a href="#">Verifying the Upgrade</a>

## 15.1.2 Performing the Required Pre-Upgrade Tasks

Before you begin with the upgrade, you must complete the following prerequisites:

- Review the *Oracle Fusion Middleware System Requirements and Specifications* and *Oracle Fusion Middleware Supported System Configurations* documents to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).
- Ensure that you are using a Java Development Kit (JDK) version that is supported and certified with Oracle Identity and Access Management 11.1.2.3.0.

You can verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

---

**Note:** For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

---

## 15.1.3 Shutting Down Administration Server and Managed Servers

The upgrade process involves changes to the binaries and to the schema. Therefore, before you begin the upgrade process, you must shut down the Administration Server and Managed Servers.

For information about stopping the servers, see ["Stopping the Servers"](#) on page 24-13.

## 15.1.4 Backing Up Oracle Entitlements Server 11g Release 1 (11.1.1.5.0)

You must back up your Oracle Entitlements Server 11.1.1.5.0 environment before you upgrade to Oracle Entitlements Server 11.1.2.3.0.

After stopping the servers, back up the following:

- *MW\_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Oracle Entitlements Server schemas

## 15.1.5 Upgrading Oracle WebLogic Server to 10.3.6

Oracle Identity and Access Management 11.1.2.3.0 is certified with Oracle WebLogic Server 11g Release 1 (10.3.6). Therefore, if your existing Oracle Entitlements Server environment is using Oracle WebLogic Server 10.3.5 or any earlier version, you must upgrade it to Oracle WebLogic Server 10.3.6.

---

---

**Note:** If you are already using Oracle WebLogic Server 10.3.6, ensure that you apply the mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server 10.3.6, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

---

---

---

---

**Note:**

- If you upgrade Oracle WebLogic Server from 10.3.5 to 10.3.6, `weblogic.policy` will be overwritten. Hence, you must backup/restore some of the policies in `weblogic.policy`.

After the upgrade procedure, add the following WebLogic Server SM policy:

```
grant codeBase "file:${oes.client.home}/-" {
permission java.security.AllPermission;
};
```

In addition, if you had added any policies in 11.1.1.5.0, these policies must be backed up and restored after upgrading to 11.1.2.3.0.

---

---

For information about upgrading to Oracle WebLogic Server 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

## 15.1.6 Upgrading Oracle Entitlements Server Administration Server 11g Release 2 (11.1.2.3.0)

To upgrade Oracle Entitlements Server Administration Server, you must use the Oracle Identity and Access Management 11.1.2.3.0 Installer. During the procedure, point the Middleware Home to your existing 11.1.1.5.0 Middleware Home. Your Oracle Home is upgraded from 11.1.1.5.0 to 11.1.2.3.0.

For information about upgrading Oracle Entitlements Server Administration Server 11g Release 1 (11.1.1.5.0), see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 15.1.7 Creating Oracle Platform Security Service Schema

---



---

**Note:** You must perform the following task only if your policy store is database.

---



---

Oracle Entitlements Server 11.1.1.5.0 schema is bound with APM. From Oracle Entitlements Server 11.1.2 release onwards, Oracle Entitlements Server security store relies on Oracle Platform Security Services for database. In order to access the Oracle Platform Security Services database, you need to create OPSS schema.

To create Oracle Platform Security Store (OPSS) schema, run the Repository Creation utility (RCU) 11.1.1.9.0. For more information, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

## 15.1.8 Executing R2\_Upgrade.sql

Complete the following steps to migrate data from old store to new store.

1. Log in to the database as SYS.
2. Go to the following path:

**On UNIX:**

<IAM\_HOME>/oes/upgrade/sql

**ON Windows:**

<IAM\_HOME>\oes\upgrade\sql

3. Run the following SQL script. Note that when you run this script, you must provide the 11.1.2.3.0 opss schema and 11.1.1.x.x APM schema details.

R2\_Upgrade.sql

This SQL script copies the user data from Oracle Entitlements Server 11.1.1.5.0 to Oracle Platform Security Services.

---



---

**Note:** In order to execute the R2\_Upgrade.sql command, you need to install a database client or execute the script in another computer that has a database client installed on it.

---



---

## 15.1.9 Creating New Oracle Entitlements Server Domain

Oracle Entitlements Server 11.1.2.3.0 Administration applications requires a JRF domain. But Oracle Entitlements Server 11.1.1.5.0 does not support JRF. Therefore, in order to deploy Oracle Entitlements Server 11.1.2.3.0 applications, you must create a new Oracle Entitlements Server domain.

For more information, see "Configuring Oracle Entitlements Server in a New WebLogic Domain" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 15.1.10 Exporting Encryption Key

Credential data are encrypted and stored in the database. The encryption key is domain specific. Since you are moving to Oracle Entitlements Server 11.1.2.3.0 domain

from Oracle Entitlements Server 11.1.1.5.0 domain, you must export the key to a keyfile and then import the key to the Oracle Entitlements Server 11.1.2.3.0 domain.

You must run the `exportEncryptionKey()` command to extract the encryption key from Oracle Entitlements Server 11.1.1.5.0 domain's bootstrap wallet.

Run the following command:

**On UNIX:**

1. Move from your present working directory to the `<MW_HOME>/oracle_common/common/bin` directory by running the following command on the command line:

```
cd <MW_HOME>/oracle_common/common/bin
```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
./wlst.sh
```

3. At the WLST prompt, run the following command:

```
exportEncryptionKey(jpsConfigFile="<domainidir>/config/fmwconfig/jps-config.xml",keyFilePath="/tmp/key",keyFilePassword="<password>")
```

where

`<domainidir>` is the complete path of the Oracle Entitlements Server 11.1.1.5.0 domain location.

`<password>` is the key file password.

**On Windows:**

1. Move from your present working directory to the `<MW_HOME>\oracle_common\common\bin` directory by running the following command on the command line:

```
cd <MW_HOME>\oracle_common\common\bin
```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
wlst.cmd
```

3. At the WLST prompt, run the following command:

```
exportEncryptionKey(jpsConfigFile="<domainidir>\config\fmwconfig\jps-config.xml",keyFilePath="C:\\tmp\key",keyFilePassword="<password>")
```

Where

`<domainidir>` is the complete path of the Oracle Entitlements Server 11.1.1.5.0 domain location.

`<password>` is the key file password.

## 15.1.11 Re-Associating Policy Stores

You must re-associate policy stores to make the Oracle Entitlements Server 11.1.2.3.0 domain uptake the security store which is based on the Oracle Platform Security Services schema. Run the `configuresecuritystore.py` script to re-associate policy stores as follows:

### 15.1.11.1 Policy Store is DB

If the policy store in 11.1.1.5.0 is DB, perform the following steps to re-associate to DB based policy store and import the encryption key to the 11.1.2.3.0 domain.

**On UNIX:**

Run the following WLST command:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <domaindir> -m join -j
<OES_11.1.1.5.0 jpsroot> -f <OES_11.1.1.5.0 farmname> -p <OPSS schema
password> -t <policy store type> -k <keyFilePath> -w <keyFilePassword>
--create_diagnostic_data
```

For example:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <MW_HOME>/user_
projects/domains/<oes_domain> -m join -j cn=jpsroot -f <oes_domain> -p
welcome1 -t DB_ORACLE -k /tmp/key -w myKeyPwd --create_diagnostic_data
```

**On Windows:**

Run the following WLST command:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir> -m join -j
<OES 11.1.1.5.0 jpsroot> -f <OES 11.1.1.5.0 farmname> -p <OPSS schema
password> -t <policy store type> -k <keyFilePath> -w <keyFilePassword>
--create_diagnostic_data
```

For example:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <MW_HOME>\user_
projects\domains\<oes_domain> -m join -j cn=jpsroot -f oes_domain -p
welcome1 -t DB_ORACLE -k C:\tmp\key -w myKeyPwd --create_diagnostic_data
```

---

**Note:** For help on the command, run the following:

On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <domaindir>
-help
```

On Windows:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir>
-help
```

---

Table 15–2 describes the parameters you need to specify on the command line.

**Table 15–2 Parameters for Reassociating Policy Stores**

Parameter	Description
MW_HOME	Specify the absolute path to the Oracle Middleware home. For example: On UNIX: /scratch/oracle/Middleware On Windows: C:\oracle\Middleware

**Table 15–2 (Cont.) Parameters for Reassociating Policy Stores**

Parameter	Description
IAM_HOME	Specify the absolute path to the Oracle Identity and Access Manager Home. For example: On UNIX: /scratch/oracle/Middleware/Oracle_IDM1 On Windows: C:\oracle\Middleware\Oracle_IDM1
domaindir	Specify the path to the Identity and Access Manager's domain location. The following example shows the complete path: On UNIX, it is located in the <MW_HOME>/user_projects/domains/base_domain directory. On Windows, it is located in the <MW_HOME>\user_projects\domains\base_domain directory.
-m	The following are the two options available for the argument -m: <ul style="list-style-type: none"> <li>■ create -m create option creates a new security store. This option is applicable for fresh installation.</li> <li>■ join -m join option uses an existing database security store for the domain. Since this is an upgrade, you must use -m join option while running the configureSecurityStore.py command.</li> </ul>
OPSS_schema_password	Specify the password of OPSS schema.
-t	Specify the policy store type. For example: DB_ORACLE, DB_DERBY, or OID.
-k	Specify the path to the KeyFile.
-w	Specify the KeyFile password.

### 15.1.11.2 Policy Store is OID

If the policy store in 11.1.1.5.0 is OID, perform the following steps to re-associate to OID based policy store and import the encryption key to the 11.1.2.3.0 domain:

1. Remove the py.class files from the oracle\_common directory by running the following command from the location *MW\_HOME*/oracle\_common:

```
find . -name "*py*class" | xargs rm
```

2. Run the following WLST command to re-associate the policy store:

#### On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_HOME>/common/tools/configureSecurityStore.py -d <domaindir> -m join -j cn=reassociate_rlps1_oes_domain -f <OES_11.1.1.5.0 farmname> -t OID -a cn=orcladmin -p <OPSS schema password> -l ldap://oim.example.com:18686 --create_diagnostic_data
```

#### For example:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_HOME>/common/tools/configureSecurityStore.py -d <MW_HOME>/user_projects/domains/<oes_domain> -m join -j cn=jpsroot -f <oes_domain> -t OID -a cn=orcladmin -p welcome1 -l ldap://oim.example.com:18686 --create_diagnostic_data
```

#### On Windows:

Run the following WLST command:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir> -m join -j
cn=reassociate_r1ps1_oes_domain -f <OES 11.1.1.5.0 farmname> -t OID -a
cn=orcladmin -p <OPSS schema password> -l ldap://oim.example.com:18686
--create_diagnostic_data
```

For example:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <MW_HOME>\user_
projects\domains\<oes_domain> -m join -j cn=jpsroot -f oes_domain -t
OID -a cn=orcladmin -p welcome1 -l ldap://oim.example.com:18686
--create_diagnostic_data
```

---

**Note:** For help on the command, run the following:

On UNIX:

```
<MW_HOME>/oracle_common/common/bin/wlst.sh <IAM_
HOME>/common/tools/configureSecurityStore.py -d <domaindir>
-help
```

On Windows:

```
<MW_HOME>\oracle_common\common\bin\wlst.cmd <IAM_
HOME>\common\tools\configureSecurityStore.py -d <domaindir>
-help
```

---

Table 15–3 describes the parameters you need to specify on the command line.

**Table 15–3 Parameters for Reassociating Policy Stores**

Parameter	Description
MW_HOME	Specify the path to the Oracle Identity and Access Manager's Middleware Home. For example: On UNIX: /oracle/Middleware On Windows: C:\oracle\Middleware
IAM_HOME	Specify the path to the Oracle Identity and Access Manager Home. The following example shows the complete path: On UNIX, it is located in the /oracle/Middleware/Oracle_IDM1 directory. On Windows, it is located in the \oracle\Middleware\Oracle_IDM1 directory.
domaindir	Specify the path to the Identity and Access Manager's domain location. The following example shows the complete path: On UNIX, it is located in the <MW_HOME>/user_projects/domains/base_domain directory. On Windows, it is located in the <MW_HOME>\user_projects\domains\base_domain directory.

**Table 15–3 (Cont.) Parameters for Reassociating Policy Stores**

Parameter	Description
-m	The following are the two options available for the argument -m: <ul style="list-style-type: none"> <li>■ create -m create option creates a new security store. This option is applicable for fresh installation.</li> <li>■ join -m join option uses an existing database security store for the domain. Since this is an upgrade, you must use -m join option while running the <code>configureSecurityStore.py</code> command.</li> </ul>
OPSS_schema_password	Specify the password of OPSS schema.
-k	Specify the path to the <code>KeyFile</code> .
-f	Specify the security store farm name.
-j	Specify the distinguished name of <code>jpsroot</code> .
-t	Specify the policy store type. For example: <code>DB_ORACLE</code> , <code>DB_DERBY</code> , or <code>OID</code> .
-a	Specify the administrator username for <code>OID</code> .
-l	Specify the url for <code>OID</code> .

### 15.1.12 Deleting all `py.class` Files

Delete all the files with postfix `py.class` in the newly installed Oracle Entitlements Server home.

### 15.1.13 Upgrading Oracle Platform Security Services

After you upgrade schemas, you must upgrade Oracle Platform Security Services (OPSS) of the new Oracle Entitlements Server domain.

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Entitlements Server to 11.1.2.3.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see [Section 24.1.7, "Upgrading Oracle Platform Security Services"](#)

### 15.1.14 Starting the Administration Server and Oracle Entitlements Server Managed Servers

After the upgrade is complete, start the WebLogic Administration Server, the Administration Server for the domain that contains Oracle Entitlements Server, and the Oracle Entitlements Server Managed Server. For more information, see [Section 24.1.8, "Starting the Servers"](#).

### 15.1.15 Redeploying APM

To get the latest APM policies into the policy store, you must redeploy the APM applications.

Complete the following steps to redeploy APM:

**On UNIX:**

1. Move from your present working directory to the <MW\_HOME>/wlserver\_10.3/common/bin directory by running the following command on the command line:

```
cd <MW_HOME>/wlserver_10.3/common/bin
```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
./wlst.sh
```

3. Connect to the Administration Server using the following command:

```
connect('weblogic-username','weblogic-password','weblogic-url')
```

4. At the WLST prompt, run the following command:

```
redeploy(appName='oracle.security.apm')
```

5. Exit the WLST console using the exit() command.

**On Windows:**

1. Move from your present working directory to the <MW\_HOME>\wlserver\_10.3\common\bin by running the following command on the command line:

```
cd <MW_HOME>\wlserver_10.3\common\bin
```

2. Run the following command to launch the WebLogic Scripting Tool (WLST):

```
wlst.cmd
```

3. Connect to the Administration Server using the following command:

```
connect('weblogic-username','weblogic-password','weblogic-url')
```

4. At the WLST prompt, run the following command:

```
<domaindir>\serverConfig\redeploy(appName='oracle.security.apm')
```

where

<domaindir> is the complete path to the Oracle Entitlements Server 11.1.2.3.0 domain.

**For example:**

```
<MW_HOME>\user_projects\domains\<oes_domain>\serverConfig\
redeploy(appName='oracle.security.apm')
```

5. Exit the WLST console using the exit() command.

**15.1.16 Verifying the Upgrade**

To verify the Oracle Entitlements Server upgrade, do the following:

- Log in to LDAP or database and verify the schema version in the Policy Store. The OPSS schema version should be 11.1.1.9.0.
- The application MAPI works with both old and new functionality.

Create a new policy to see if CRUD operations on the policy store artifacts, using their entity managers, are working.

For more information, see "Creating Fine Grained Elements for a Simple Policy" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*.

- The Application Runtime Authorization continues working.

To verify, create an authorization, as mentioned in "Using the PEP API" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*, and see if it works correctly.

## 15.2 Upgrading Oracle Entitlements Server Client Server

This section contains the following topics:

- [Section 15.2.1, "Upgrade Roadmap for Oracle Entitlements Server Client Server"](#)
- [Section 15.2.2, "Stopping all Security Module Instances"](#)
- [Section 15.2.3, "Upgrading Oracle Entitlements Server Client 11g Release 2 \(11.1.2.3.0\)"](#)
- [Section 15.2.4, "Changing Username and Password for the New Schemas"](#)
- [Section 15.2.5, "Starting the Security Modules"](#)
- [Section 15.2.6, "Verifying the Upgrade"](#)

### 15.2.1 Upgrade Roadmap for Oracle Entitlements Server Client Server

---

**Note:** If you do not follow the exact sequence provided in this task table, your Oracle Entitlements Server Client Server upgrade may not be successful.

---

[Table 15–4](#) lists the steps for upgrading Oracle Entitlements Server Client Server upgrade.

**Table 15–4 Upgrade Flow**

SI. No.	Task	For More Information
1	Shut down all security modules. This includes shutting down the Administration Server and Managed Servers too.	See, <a href="#">Stopping all Security Module Instances</a>
2	Upgrade 11.1.1.5.0 Oracle Home to 11.1.2.3.0.	See, <a href="#">Upgrading Oracle Entitlements Server Client 11g Release 2 (11.1.2.3.0)</a>
3	Change the username and password.	See, <a href="#">Changing Username and Password for the New Schemas</a>
4	Start the security modules.	See, <a href="#">Starting the Security Modules</a>
5	Verify the Oracle Entitlements Server Client Server upgrade.	See, <a href="#">Verifying the Upgrade</a>

### 15.2.2 Stopping all Security Module Instances

Bring down all security module instances, Administration Server, and Managed Servers.

The security module instances shuts down when the Administration Server and Managed Servers are shut down.

To stop the servers, see [Section 15.1.3, "Shutting Down Administration Server and Managed Servers"](#).

## 15.2.3 Upgrading Oracle Entitlements Server Client 11g Release 2 (11.1.2.3.0)

To upgrade Oracle Entitlements Server Client Server, you must use the 11.1.2.3.0 installer. During the procedure, point the Middleware Home to your existing 11.1.1.5.0 Oracle Entitlements Server Middleware Home. This upgrades your Middleware Home and Oracle Home from 11.1.1.5.0 to 11.1.2.3.0.

This section contains the following topics:

- [Prerequisites](#)
- [Obtaining the Software](#)
- [Installing Oracle Entitlements Server Client Server 11g Release 2 \(11.1.2.3.0\)](#)
- [Verifying the Installation](#)

### 15.2.3.1 Prerequisites

You must install and configure Oracle Entitlements Server Administration Server, as described in [Section 15.1.6, "Upgrading Oracle Entitlements Server Administration Server 11g Release 2 \(11.1.2.3.0\)"](#).

### 15.2.3.2 Obtaining the Software

For more information on obtaining Oracle Fusion Middleware 11g software, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

### 15.2.3.3 Installing Oracle Entitlements Server Client Server 11g Release 2 (11.1.2.3.0)

For more information on installing Oracle Entitlements Server Client Server 11.1.2.3.0, see "Installing Oracle Entitlements Server Client" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

### 15.2.3.4 Verifying the Installation

To verify that your Oracle Entitlements Server Client install was successful, go to your Oracle Home directory which you specified during installation and verify that the Oracle Entitlements Server Client installation files are created.

## 15.2.4 Changing Username and Password for the New Schemas

If Oracle Entitlements Server client is running in a controlled-pull mode or in an uncontrolled mode, the `jps-config.xml` of the Security Module instance must be changed to reflect the schema changes done during the Administration Server upgrade.

Before running the `oessmconfig.sh` command, you need to modify `jps-config.xml` of the controlled-pull or uncontrolled security module.

---

**Note:** For Java, RMI and Web Service security modules, `jps-config.xml` is located at:

```
<OES_CLIENT_HOME>/oes_sm_instances/<SM_NAME>/config
```

For Oracle WebLogic Server security module, `jps-config.xml` is located at:

```
<WLS_DOMAIN_HOME>/config/oeswlsmconfig/<SERVER_NAME>
```

---

---

---

**Note:** For controlled-push security module, you do not have to add any parameters to the `pdp.service` instance.

---

---

### Controlled-Pull Security Module

For controlled-pull security module, add the following to the `pdp.service` instance:

```
<property name="oracle.security.jps.runtime.pd.client.SMinstanceType"
value="<sm_type>" />
```

Replace "`<sm_type>`" with the actual type.

For example:

```
"java"
```

### Uncontrolled Security Module

For uncontrolled security module, add the following to the `pdp.service` instance:

```
<property
name="oracle.security.jps.runtime.pd.client.policyDistributionMode"
value="non-controlled" />

<property name="oracle.security.jps.runtime.pd.client.sm_name" value="<sm_
name>" />

<property name="oracle.security.jps.runtime.pd.client.SMinstanceType"
value="<sm_type>" />
```

Replace "`<sm_name>`" "`<sm_type>`" with the actual values.

Do the following to change the username and password of the new schemas:

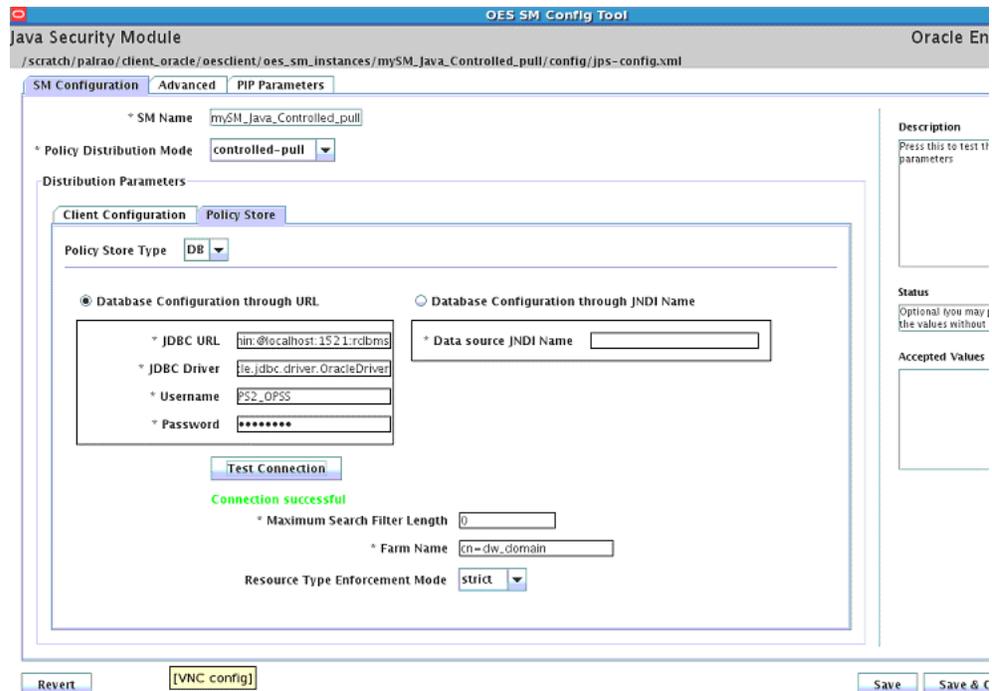
1. Go to the following path:  
On UNIX, `<CLIENT_HOME>/oesclient/oesm/enroll/bin`  
On Windows, `<CLIENT_HOME>\oesclient\oesm\enroll\bin`
2. Run the following command:  
On UNIX:  

```
./oesmconfig.sh -jpsconfig <path to the jps-config.xml>
```

  
On Windows:  

```
oesmconfig.cmd -jpsconfig <path to the jps-config.xml>
```
3. A Graphic User Interface displays. See [Figure 15-1](#).
4. Click **SM Configuration**.
5. Click the **Policy Store** sub-tab.
6. Enter the new schema user name and password.
7. Click **Test Connection**
8. When you get the successful security module test message, click **Save & Close**.

Figure 15–1 Java Security Module



## 15.2.5 Starting the Security Modules

You must start the security modules by starting the Administration Server and Managed Servers.

To start the servers, see [Section 15.1.14, "Starting the Administration Server and Oracle Entitlements Server Managed Servers"](#).

---

**Note:** When starting the Oracle Service Bus Security Module, you must use the parameter `-Doracle.oes.osbresource.converter.distinguishtransportprivilege=false` while running the script.

---

## 15.2.6 Verifying the Upgrade

To verify, create an authorization, as mentioned in "Using the PEP API" in the *Oracle Fusion Middleware Developer's Guide for Oracle Entitlements Server*, and see if it works correctly.

The Application Runtime Authorization continues working.



---

---

## Upgrading Oracle Identity Manager 9.1.x.x Environments

This chapter describes how to upgrade Oracle Identity Manager 9.1.x.x to Oracle Identity Manager 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

Upgrading Oracle Identity Manager 9.1.x.x to Oracle Identity Manager 11.1.2.3.0 involves two major tasks:

- Upgrading Oracle Identity Manager 9.1.x.x to Oracle Identity Manager 11g Release 2 (11.1.2.2.0)
- Upgrading Oracle Identity Manager 11g Release 2 (11.1.2.2.0) to Oracle Identity Manager 11g Release 2 (11.1.2.3.0)

This chapter includes the following sections:

- [Section 16.1, "Upgrade Roadmap for Oracle Identity Manager"](#)
- [Section 16.2, "Feature Comparison"](#)
- [Section 16.3, "Reviewing System Requirements and Certification"](#)
- [Section 16.4, "Upgrading Oracle Identity Manager 9.1.x.x to 11.1.2.2.0"](#)
- [Section 16.5, "Upgrading Oracle Identity Manager 11.1.2.2.0 to 11.1.2.3.0"](#)

### 16.1 Upgrade Roadmap for Oracle Identity Manager

[Table 16–1](#) lists the tasks to be completed to upgrade Oracle Identity Manager 9.1.x.x to 11.1.2.3.0.

**Table 16–1 Roadmap for Upgrading Oracle Identity Manager 9.1.x.x to 11.1.2.3.0**

SI No	Task	For More Information
1	Review the changes in the features of Oracle Identity Manager 11.1.2.3.0.	See, <a href="#">Feature Comparison</a>
2	Review system requirements and certifications.	See, <a href="#">Reviewing System Requirements and Certification</a>
3	Upgrade Oracle Identity Manager 9.1.x.x environments to Oracle Identity Manager 11g Release 2 (11.1.2.2.0).	See, <a href="#">Upgrading Oracle Identity Manager 9.1.x.x to 11.1.2.2.0</a>
4	Upgrade Oracle Identity Manager 11g Release 2 (11.1.2.2.0) to Oracle Identity Manager 11g Release 2 (11.1.2.3.0).	See, <a href="#">Upgrading Oracle Identity Manager 11.1.2.2.0 to 11.1.2.3.0</a>

## 16.2 Feature Comparison

[Table 16–2](#) lists key differences in functionality between Oracle Identity Manager 9.1.x.x and Oracle Identity Manager 11.1.2.3.0.

**Table 16–2 Features Comparison**

Oracle Identity Manager 9.1.x.x	Oracle Identity Manager 11.1.2.3.0
The Oracle Identity Manager 9.1.x.x User Interface is built on the struts framework. It provides basic self service interfaces.	Oracle Identity Manager 11.1.2.3.0 uses Alta skin which is business (mobile, cloud) friendly. Oracle Identity Manager 11.1.2.3.0 has new Home page, and new my profile page with user-friendly inbox.  Most of the UI customizations need to be re done post upgrade, to match the look and feel of 11.1.2.3.0.
Oracle Identity Manager 9.1.x.x provides basis self service capabilities such as password reset and account request.	Oracle Identity Manager 11.1.2.3.0 provides a new user interface with a shopping cart-type request model through which end users can search and browse through the catalog and directly request any item such as roles, entitlements, or applications without having to navigate through a series of menus.  In addition to this, several business-friendly metadata such as description, audit objective, tags, owner, approver, and technical glossary and so on can be associated to each access item, to display business-friendly and rich contextual information to a business user at the time of self service access request and access review.  UDFs which are marked as searchable will automatically be part of advance search form.  You can customize the search form. Attributes can be used to search catalog items. Catalog is the single point for managing access.

**Table 16–2 (Cont.) Features Comparison**

Oracle Identity Manager 9.1.x.x	Oracle Identity Manager 11.1.2.3.0
<p>Oracle Identity Manager 9.1.x.x provides Identity Attestation to periodically review a user's access. For advanced access review capabilities such as role or data owner certification, OIM 9.1.x.x had to be integrated with Oracle Identity Analytics (OIA).</p>	<p>OIA functionality is now ported into Oracle Identity Governance (OIG). Customers can define and manage identity audit policies based on IDA rules. Customers can define owners and remediators for a policy, which can be a specific user, a list of users or an OIM role.</p>
<p>In Oracle Identity Manager 9.1.0.x, users are assigned to organizations by specifying an organization name in the Organization attribute of the user details. This is a static organization membership. A user can only be a member of one organization.</p>	<p>Customers can use preventive and detective scan capabilities which can create actionable policy violations.</p> <p>Oracle Identity Manager 11.1.2.3.0 has comprehensive role lifecycle management and workflow approval capabilities with direct involvement from business, featuring a business friendly UI.</p> <p>It also includes detailed Role Analytics to aid with the composition and modifications of roles.</p> <p>In Oracle Identity Manager 11.1.2.3.0, in addition to the existing feature, you can dynamically assign users to organizations based on user-membership rules, which you can define in the Members tab of the organization details page.</p>
<p>In Oracle Identity Manager 9.1.x.x Resource and IT resource names are named in a manner such that it is easy for the IT users to manage them. The problem with this approach is that if a business user has to request access, the resource name will not make sense to the user. These incomprehensible Resource and IT resource names make the access request process non intuitive.</p>	<p>All users who satisfy the user-membership rule are dynamically associated with the organization, irrespective of the organization hierarchy the users statically belong to. With this new capability, a user can gain membership of one home organization via static membership and multiple secondary organizations via user-membership rules that are dynamically evaluated.</p> <p>Oracle Identity Manager 11.1.2.3.0 provides an abstraction entity called Application Instance. It is a combination of IT resource instance (target connectivity and connector configuration) and resource object (provisioning mechanism). Administrators can assign business friendly names to Application instances and map them to corresponding IT resources and Resource Objects.</p> <p>End users who request for accounts through the catalog will search for an account by providing the business friendly Application Instance Name.</p> <p>Application instances are automatically created as part of the Upgrade procedure. Administrators are expected to define organization publishing for these Application Instances to control who has access to request for access to the application.</p>

**Table 16–2 (Cont.) Features Comparison**

Oracle Identity Manager 9.1.x.x	Oracle Identity Manager 11.1.2.3.0
In Oracle Identity Manager 9.1.x.x, policies are implemented and customized using OIM plug-in and pre-pop adapters implemented via plug-in framework, which required writing custom java code to extend and customize OOTB policies	Oracle Identity Manager 11.1.2.3.0 has introduced declarative policies that enable customers to define and configure various policy types that are evaluated at run time. Policy is configured via a UI/API rather than customized via Java plug-in or pre-pop adapter.

## 16.3 Reviewing System Requirements and Certification

Before you start the upgrade process, you must read the system requirements and certification document to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).

## 16.4 Upgrading Oracle Identity Manager 9.1.x.x to 11.1.2.2.0

In order to upgrade Oracle Identity Manager 9.1.x.x environments to 11g Release 2 (11.1.2.3.0), you must first upgrade to 11g Release 2 (11.1.2.2.0). For information about upgrading Oracle Identity Manager 9.1.x.x to Oracle Identity Manager 11.1.2.2.0, see "Upgrading Oracle Identity Manager 9.1.x.x Environments" in the *Upgrade Guide for Oracle Identity and Access Management* for 11g Release 2 (11.1.2.2.0).

## 16.5 Upgrading Oracle Identity Manager 11.1.2.2.0 to 11.1.2.3.0

After you upgrade Oracle Identity Manager 9.1.x.x to 11.1.2.2.0, you must upgrade Oracle Identity Manager 11.1.2.2.0 to 11.1.2.3.0. For information about upgrading Oracle Identity Manager 11.1.2.2.0 to 11.1.2.3.0, see [Chapter 10, "Upgrading Oracle Identity Manager 11g Release 2 \(11.1.2.x.x\) Environments"](#).

# Part V

---

## Upgrading Oracle Identity and Access Management High Availability Environments

This part includes the following chapters:

- Chapter 17, "Upgrading Oracle Access Management Highly Available Environments"
- Chapter 18, "Upgrading Oracle Access Management Multi-Data Center Environments"
- Chapter 19, "Upgrading Oracle Adaptive Access Manager Highly Available Environments"
- Chapter 20, "Upgrading Oracle Identity Manager Highly Available Environments"
- Chapter 21, "Upgrading Oracle Entitlements Server Highly Available Environments"
- Chapter 22, "Upgrading Oracle Privileged Account Manager Highly Available Environments"
- Chapter 23, "Upgrading OIM-OAM Integrated Highly Available Environments"
- Chapter 18, "Upgrading Oracle Access Management Multi-Data Center Environments"



---

---

## Upgrading Oracle Access Management Highly Available Environments

This chapter describes how to upgrade Oracle Access Management highly available environments to Oracle Access Management 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0). For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

If you wish to upgrade Oracle Access Management multi-data center environments, refer to [Chapter 18, "Upgrading Oracle Access Management Multi-Data Center Environments"](#).

---

---

---

---

**Note:** Before you proceed, check if your existing Oracle Access Management version is supported for high availability upgrade. For more information on supported starting points for high availability upgrade, see [Section 3.3, "Supported Starting Points for Oracle Identity and Access Management Manual Upgrade"](#).

---

---

This chapter includes the following sections:

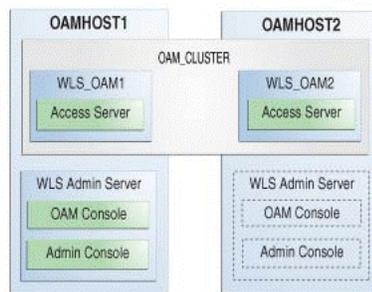
- [Section 17.1, "Understanding Oracle Access Management High Availability Upgrade Topology"](#)
- [Section 17.2, "Upgrade Roadmap"](#)
- [Section 17.3, "Shutting Down Administration Server and Managed Servers on OAMHOST1 and OAMHOST2"](#)
- [Section 17.4, "Backing Up the Existing Environment"](#)
- [Section 17.5, "Upgrading OAMHOST1 to 11.1.2.3.0"](#)
- [Section 17.6, "Updating Component Versions on OAMHOST1"](#)
- [Section 17.7, "Updating Binaries of WebLogic Server and Access Manager on OAMHOST2"](#)

- [Section 17.8, "Replicating Domain Configuration on OAMHOST2"](#)
- [Section 17.9, "Redeploying Access Manager Server Applications and Shared Libraries on OAMHOST1"](#)
- [Section 17.10, "Starting Administration Server and Managed Servers on OAMHOST1 and OAMHOST2"](#)

## 17.1 Understanding Oracle Access Management High Availability Upgrade Topology

Figure 17–1 shows the Oracle Access Management cluster set up that can be upgraded to 11.1.2.3.0 by following the procedure described in this chapter.

**Figure 17–1 Oracle Access Management High Availability Upgrade Topology**



On OAMHOST1, the following installations have been performed:

- An Oracle Access Management Access Manager instance has been installed in the WLS\_OAM1 Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the active Administration Server.

On OAMHOST2, the following installations have been performed:

- An Oracle Access Management Access Manager instance has been installed in the WLS\_OAM2 Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on OAMHOST1 becomes unavailable.

The instances in the WLS\_OAM1 and WLS\_OAM2 Managed Servers on OAMHOST1 and OAMHOST2 are configured in a cluster named OAM\_CLUSTER.

## 17.2 Upgrade Roadmap

Table 17–1 lists the steps to upgrade Oracle Access Management high availability environment illustrated in Figure 17–1 to 11.1.2.3.0.

**Table 17–1 Oracle Access Management High Availability Upgrade Roadmap**

Task No	Task	For More Information
1	Review the Oracle Access Management high availability upgrade topology, and identify OAMHOST1 and OAMHOST2 on your setup.	See, <a href="#">Understanding Oracle Access Management High Availability Upgrade Topology</a>
2	Shut down the Administration Server and all the Managed Servers on OAMHOST1 and OAMHOST2.	See, <a href="#">Shutting Down Administration Server and Managed Servers on OAMHOST1 and OAMHOST2</a>
3	Back up the existing environment.	See, <a href="#">Backing Up the Existing Environment</a>
4	Upgrade OAMHOST1 to 11.1.2.3.0. This is the host with active Administration Server running on it.	See, <a href="#">Upgrading OAMHOST1 to 11.1.2.3.0</a>
5	If your starting point is Oracle Access Manager 11g Release 1 (11.1.1.5.0), you must upgrade the OAM packages to 11.1.2.3.0 on OAMHOST1.	See, <a href="#">Updating Component Versions on OAMHOST1</a>
6	Update the binaries of Oracle WebLogic Server and Access Manager on OAMHOST2.	See, <a href="#">Updating Binaries of WebLogic Server and Access Manager on OAMHOST2</a>
7	If your starting point is Oracle Access Manager 11.1.1.5.0, after you upgrade OAMHOST1, you must replicate the configurations on OAMHOST2 by packing the domain on OAMHOST1 and unpacking it on OAMHOST2.	See, <a href="#">Replicating Domain Configuration on OAMHOST2</a>
8	If you are upgrading Oracle Access Manager 11.1.1.5.0 environments, redeploy Access Manager Server applications and shared libraries on OAMHOST1 to target them to OAM_CLUSTER.	See, <a href="#">Redeploying Access Manager Server Applications and Shared Libraries on OAMHOST1</a>
9	Start the WebLogic Administration Server and the Managed Servers on OAMHOST1 and OAMHOST2.	See, <a href="#">Starting Administration Server and Managed Servers on OAMHOST1 and OAMHOST2</a>

## 17.3 Shutting Down Administration Server and Managed Servers on OAMHOST1 and OAMHOST2

Before you begin the upgrade process, you must stop the WebLogic Administration Server and all of the Access Manager Managed Servers on OAMHOST1 and OAMHOST2 in the following order:

1. Stop the Access Manager Managed Servers on both OAMHOST1 and OAMHOST2.
2. Stop the WebLogic Administration Server on OAMHOST1.

For information about stopping the Managed Server, see [Section 24.1.9.1, "Stopping the Managed Server\(s\)"](#).

For information about stopping the Administration Server, see [Section 24.1.9.2, "Stopping the WebLogic Administration Server"](#).

## 17.4 Backing Up the Existing Environment

After stopping all the servers, you must back up the following before proceeding with the upgrade process:

- `MW_HOME` directory (Middleware home directory), including the Oracle Home directories inside Middleware home on both `OAMHOST1` and `OAMHOST2`.
- Oracle Access Management Domain Home directory on both `OAMHOST1` and `OAMHOST2`.
- Following Database schemas:
  - Oracle Access Manager schema
  - MDS schema
  - Audit and any other dependent schema

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

## 17.5 Upgrading OAMHOST1 to 11.1.2.3.0

In order to upgrade the Oracle Access Management high availability environment to 11.1.2.3.0, you must first upgrade `OAMHOST1` which has the active Administration Server. The following are some of the important tasks involved in upgrading `OAMHOST1` to 11.1.2.3.0:

- Upgrading Oracle WebLogic Server to 10.3.6 if you are using a previous version.
- Upgrading Oracle Access Management binaries to 11.1.2.3.0.
- Upgrading the database schemas.
- Copying the modified domain mbean configurations.
- Upgrading the system configuration.

The procedure to upgrade `OAMHOST1` depends on your starting point.

- If your starting point is Oracle Access Management 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0), follow the instructions described in [Chapter 8, "Upgrading Oracle Access Management 11g Release 2 \(11.1.2.x.x\) Environments"](#) to upgrade `OAMHOST1` to 11.1.2.3.0.
- If your starting point is Oracle Access Manager 11g Release 1 (11.1.1.5.0), follow the instructions described in [Chapter 12, "Upgrading Oracle Access Manager 11g Release 1 \(11.1.1.x.x\) Environments"](#) to upgrade `OAMHOST1` to 11.1.2.3.0.

## 17.6 Updating Component Versions on OAMHOST1

If your starting point is Oracle Access Manager 11g Release 1 (11.1.1.5.0) and if you are using Oracle Access Manager - Oracle Adaptive Access Manager integrated setup, you must upgrade the following packages from 11g Release 1 (11.1.1.5.0) to 11g Release 2 (11.1.2.3.0):

- `oracle.dogwood.top`
- `oracle.oam.server`
- `oracle.idm.oinav`
- `oracle.sdp.client`

- oracle.oaam.suite
- oracle.oaam.oaam\_admin
- oracle.oaam.oaam\_server
- oracle.oaam.oaam\_offline

---

**Note:** If your starting point is Access Manager 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0) or 11g Release 2 (11.1.2), skip this task.

---

To upgrade the packages, you must run the domain updater utility (com.oracle.cie.domain-update\_1.0.0.0.jar) on OAMHOST1 which updates the domain-info.xml. OAMHOST1 is the host on which Administration Server is running.

To upgrade the necessary Oracle Access Manager packages to 11.1.2.3.0, complete the following steps on OAMHOST1:

1. Go to the directory `$ORACLE_HOME/oaam/upgrade`. The domain updater utility com.oracle.cie.domain-update\_1.0.0.0.jar file is located in this directory.
2. Upgrade the packages using the following command:

```
java -cp MW_
HOME/utills/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
_1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
<package_name>:11.1.1.5.0, :11.1.2.3.0
```

In this command, `<DOMAIN_HOME>` refers to the absolute path to the Oracle Access Management domain, and `<package_name>` refers to the package that you are upgrading.

Run this command for all of the following packages:

- oracle.dogwood.top
- oracle.oam.server
- oracle.idm.oimnav
- oracle.sdp.client
- oracle.oaam.suite
- oracle.oaam.oaam\_admin
- oracle.oaam.oaam\_server
- oracle.oaam.oaam\_offline

## 17.7 Updating Binaries of WebLogic Server and Access Manager on OAMHOST2

After you upgrade the Access Manager environment on OAMHOST1, you must update the binaries of Oracle WebLogic Server on OAMHOST2 (if you are using any previous version). Also, you must update the binaries of Oracle Access Manager to 11.1.2.3.0 on OAMHOST2 using the Oracle Identity and Access Management 11.1.2.3.0 installer.

For information about upgrading Oracle WebLogic Server to 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

For information about upgrading Oracle Access Manager binaries to 11.1.2.3.0, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 17.8 Replicating Domain Configuration on OAMHOST2

This step is applicable if you are upgrading Oracle Access Manager 11g Release 1 (11.1.1.5.0) to 11.1.2.3.0.

After you upgrade Oracle Access Manager 11.1.1.5.0 to 11.1.2.3.0 on OAMHOST1, you must replicate the configurations on OAMHOST2. This task involves packing the upgraded domain on OAMHOST1 and unpacking it on OAMHOST2.

---

---

**Note:** Make sure that the Managed Servers are stopped before you perform this step. Do not start the Managed Servers until you complete this task.

---

---

To do this, complete the following steps:

1. On OAMHOST1, run the following command from the location `$MW_HOME/oracle_common/common/bin` to pack the upgraded domain:

**On UNIX:**

```
sh pack.sh -domain=<Location_of_OAM_domain> -template=<Location_where_domain_configuration_jar_to_be_created> -template_name="OAM Domain" -managed=true
```

**On Windows:**

```
pack.cmd -domain=<Location_of_OAM_domain> -template=<Location_where_domain_configuration_jar_needs_to_be_created> -template_name="OAM Domain" -managed=true
```

2. Copy the domain configuration jar file created by the pack command on OAMHOST1 to any accessible location on OAMHOST2.
3. On OAMHOST2, run the following command from the location `$MW_HOME/oracle_common/common/bin` to unpack the domain:

**On UNIX:**

```
sh unpack.sh -domain=<Location_of_OAM_domain> -template=<Location_on_OAMHOST2_where_you_copied_jar_file_created_by_pack_command> -overwrite_domain=true
```

**On Windows:**

```
unpack.cmd -domain=<Location_of_OAM_domain> -template=<Location_on_OAMHOST2_where_you_copied_jar_file_created_by_pack_command> -overwrite_domain=true
```

## 17.9 Redeploying Access Manager Server Applications and Shared Libraries on OAMHOST1

If you are upgrading Oracle Access Manager 11.1.1.5.0 on OAMHOST1, then you must redeploy Access Manager server applications and shared libraries, and target the applications and shared libraries to OAM\_CLUSTER, for the following reasons:

- To uptake new shared libraries that Access Manager server applications are dependent on.
- To uptake newer versions of Access Manager Administration and Managed Server applications.

For information about redeploying Access Manager server applications and shared libraries, see [Section 12.13, "Redeploying Access Manager Server Applications and Shared Libraries"](#).

---

**Note:** ■ Before you run the `redeployOAM` command, ensure that the Access Manager Managed Server(s) are in `RUNNING` state and not in the `ADMIN` state.

If the servers are in `ADMIN` state, do the following:

1. Log in to the WebLogic Administration Server using the following URL:  
`http://host:port/console`
  2. Click Deployments.
  3. Click **oam\_server(11.1.2.0.0)** on the **Summary of Deployments** page.
  4. Click *OAM\_SERVER* on the **Summary of Servers** page.
  5. Go to the **Control** tab and click **RESUME**.
- If you had redeployed Access Manager server applications and shared libraries as part of [Section 17.5, "Upgrading OAMHOST1 to 11.1.2.3.0"](#), skip this task.
- 

## 17.10 Starting Administration Server and Managed Servers on OAMHOST1 and OAMHOST2

Start the WebLogic Administration Server and the Access Manager Managed Servers on OAMHOST1 and OAMHOST2 in the following order:

1. Start the WebLogic Administration Server on OAMHOST1.
2. Start the Access Manager Managed Servers on OAMHOST1 and OAMHOST2.

For more information about starting the WebLogic Administration Server, see [Section 24.1.8.2, "Starting the WebLogic Administration Server"](#).

For more information about starting the Managed Servers, see [Section 24.1.8.3, "Starting the Managed Server\(s\)"](#).



---

---

## Upgrading Oracle Access Management Multi-Data Center Environments

This chapter describes how to upgrade Oracle Access Management deployed across multi-data centers (MDC), to 11g Release 2 (11.1.2.3.0).

---

---

**Note:** To upgrade Oracle Access Management MDC environments to 11.1.2.3.0, ensure that all of the data centers (DC) are at the same Patch Set level.

---

---

When you plan to upgrade to 11.1.2.3.0, you can choose to have zero down time by stopping the data center that needs to be upgraded, and routing all the traffic to the other data centers. Once the upgrade has been completed on one data center, it can start and function as an independent data center. You can then redirect all the traffic to the upgraded data center, provided all of the non-upgraded data centers are removed from the load balancer (LBR). Only when the remaining data centers individually upgraded to the level of the first data center, they can participate in MDC.

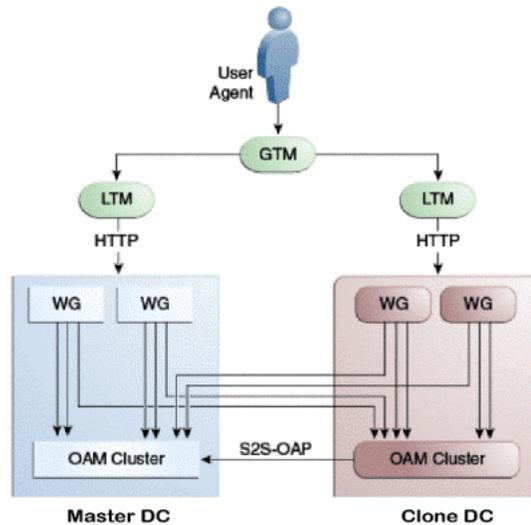
This section includes the following sections:

- [Understanding Oracle Access Management Multi-Data Center Topology](#)
- [Upgrade Roadmap](#)
- [Backing Up the Existing Environment](#)
- [Enabling Write Permission to Master and Clones \(if Necessary\)](#)
- [Disabling and Deleting All Replication Agreements Between Master and Clone](#)
- [Redirecting Traffic to Clone Data Center](#)
- [Upgrading OAM on Master Data Center](#)
- [Redirecting Traffic to Master Data Center](#)
- [Upgrading OAM on Clone Data Center](#)
- [Freezing all Changes to Master and Clones \(if Necessary\)](#)
- [Syncing Access Metadata](#)
- [Creating Replication Agreement](#)
- [Bringing up the Master and Clone Data Centers Online](#)
- [Troubleshooting](#)

## 18.1 Understanding Oracle Access Management Multi-Data Center Topology

Figure 18–1 illustrates the Oracle Access Management multi-data center topology.

**Figure 18–1 Oracle Access Management in MDC Setup**



This is a sample topology that illustrates Oracle Access Management in a multi-data center setup. This figure shows a Master data center and a Clone data center, each of them including a full Access Manager installation. In this topology, GTM refers to the global load balancer, LTM refers to the local load balancer, and WG refers to the WebGate. The S2S OAP is the Oracle Access Protocol.

The procedure in this chapter describes how to upgrade Oracle Access Management in a MDC setup similar to Figure 18–1.

## 18.2 Upgrade Roadmap

Table 18–1 lists the steps to upgrade Oracle Access Management deployed across multi-data centers, to 11.1.2.3.0.

**Table 18–1 Upgrade Roadmap**

Task No	Task	For More Information
1	Review the Oracle Access Management multi-data center topology.	See, <a href="#">Understanding Oracle Access Management Multi-Data Center Topology</a>
2	Back up your existing environment.	See, <a href="#">Backing Up the Existing Environment</a>
3	Enable write permission to Master and Clone data centers, if not already done.	See, <a href="#">Enabling Write Permission to Master and Clones (if Necessary)</a>
4	Disable and delete all replication agreements between Master and Clone data centers.	See, <a href="#">Disabling and Deleting All Replication Agreements Between Master and Clone</a>

**Table 18–1 (Cont.) Upgrade Roadmap**

<b>Task No</b>	<b>Task</b>	<b>For More Information</b>
5	Redirect the traffic to the Clone data center.	See, <a href="#">Redirecting Traffic to Clone Data Center</a>
6	Upgrade Oracle Access Management on Master data center.	See, <a href="#">Upgrading OAM on Master Data Center</a>
7	Redirect the traffic to the Master data center.	See, <a href="#">Redirecting Traffic to Master Data Center</a>
8	Upgrade Oracle Access Management on Clone data center.	See, <a href="#">Upgrading OAM on Clone Data Center</a>
9	Freeze all changes to the Master and Clones, if required.	See, <a href="#">Freezing all Changes to Master and Clones (if Necessary)</a>
10	Sync the access UDM data by exporting the access store data from Master data center and importing it on the Clone data center.	See, <a href="#">Syncing Access Metadata</a>
11	Create the replication agreement again.	See, <a href="#">Creating Replication Agreement</a>
12	Bring up the Master and Clone data centers online.	See, <a href="#">Bringing up the Master and Clone Data Centers Online</a>

### 18.3 Backing Up the Existing Environment

After stopping all the servers, you must back up the following on every data center before proceeding with the upgrade process:

- *MW\_HOME* directory (Middleware home directory), including the Oracle Home directories inside Middleware home.
- Oracle Access Management Domain Home directory on all OAM hosts.
- Following Database schemas:
  - Oracle Access Manager schema
  - Audit and any other dependent schema

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

### 18.4 Enabling Write Permission to Master and Clones (if Necessary)

Before you start the upgrade, you must enable modifications to the system and policy configurations on both Master and Clones. To do this, run the following command on Master and Clone data centers:

```
SetMultiDataCenterWrite(WriteEnableFlag="true")
```

### 18.5 Disabling and Deleting All Replication Agreements Between Master and Clone

Disable all replication agreements between Master and Clone by running the following command:

```
PUT http://oam1.example.com/oam/services/rest/_
replication/201312040602298762 HTTP/1.1 Content-Type: application/json
{"enabled":"false","pollInterval":"60","replicaType":"clone"}
```

After you disable the replication agreements, delete them by running the following command:

```
DELETE http://oam1.example.com/oam/services/rest/_replication/
201312040602298762 HTTP/1.1
```

## 18.6 Redirecting Traffic to Clone Data Center

An in-line upgrade procedure is used to upgrade the Master data center which requires downtime. Therefore, all traffic must be rerouted to the Clone data centers (also referred to as, the backup data centers or the secondary data centers). Consult your network infrastructure team or refer to the network infrastructure documentation to accomplish the traffic re-routing.

## 18.7 Upgrading OAM on Master Data Center

Upgrade Oracle Access Management on the Master data center by following the instructions described in [Chapter 17, "Upgrading Oracle Access Management Highly Available Environments"](#).

## 18.8 Redirecting Traffic to Master Data Center

An in-line upgrade procedure is used to upgrade the Clone data center which requires downtime. Therefore, all traffic must be rerouted to the Master data center. Consult your network infrastructure team or refer to the network infrastructure documentation to accomplish the traffic re-routing.

## 18.9 Upgrading OAM on Clone Data Center

Upgrade the Oracle Access Management on Clone data center(s) by following the instructions described in [Chapter 17, "Upgrading Oracle Access Management Highly Available Environments"](#).

## 18.10 Freezing all Changes to Master and Clones (if Necessary)

After you upgrade Oracle Access Management on all of the Clone data center(s), it is recommended that you freeze the changes to the Master and the Clone data center(s). This is to avoid any inadvertent writes. To do this, run the following command on the Master and the Clone data center(s):

```
SetMultiDataCenterWrite(WriteEnableFlag="false")
```

## 18.11 Syncing Access Metadata

This step is required for OAM metadata stored in Unified Data Model (UDM) to be synced from Master to Clone. This can be achieved using the WLST commands - `exportAccessStore` and `importAccessStore`. These commands need to be executed after you upgrade all of the data centers and before creating the new replication agreement. This exports the UDM artifacts created till that point, from the Master data center and imports them in the Clone data center(s).

To sync the UDM metadata, complete the following steps:

1. Run the following WLST command on the Master data center to create a ZIP file containing the UDM metadata:

```
exportAccessStore(toFile="/master/location/dclmetadata.zip",
namePath="/")
```

2. Copy `dclmetadata.zip` to each of the upgraded Clone data centers.

3. Run the following WLST command on the each of the Clone data centers to import the UDM metadata:

```
importAccessStore(fromFile="/clone/location/dclmetadata.zip",
namePath="/")
```

## 18.12 Creating Replication Agreement

Create the replication agreement again by running the following command:

---



---

**Note:** Ensure that Master & Clone data centers REST endpoints are up and running, before you run this command.

---



---

```
curl -u <repluser> -H 'Content-Type: application/json' -X POST
'https://supplier.example.com/oam/services/rest/_replication/setup' -d
'{"name": "DC12DC2",
"source": "DC1", "target": "DC2", "documentType": "ENTITY"}'
```

For more information about creating the replication agreement, see "Creating the Replication Agreement" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

## 18.13 Bringing up the Master and Clone Data Centers Online

After successful upgrade, both Master and Clone data centers can be brought up online. Traffic can be routed to both data centers based on existing routing rules. Consult your network infrastructure team or refer to the network infrastructure documentation to accomplish the traffic re-routing.

## 18.14 Troubleshooting

This section describes troubleshooting methods for some of the common problems that might occur during the upgrade process.

---



---

**Note:** For information about the issues that you might encounter during the upgrade process, and their workaround, see *Oracle Fusion Middleware Release Notes*.

---



---

This section contains the following topic:

- [Multi-Data Centre Feature Not Working After Upgrade](#)

## 18.14.1 Multi-Data Centre Feature Not Working After Upgrade

If you had enabled Multi-Data Centre (MDC) feature in your 11.1.2.x.x setup, you must re-register the MDC partners and enable the MDC functionality that is added in 11.1.2.3.0. To do this, complete the following steps post-upgrade:

1. In each Data Centre (DC), remove the MDC partners by running the following WebLogic Scripting Tool (WLST) command:

```
removePartnerForMultiDataCentre="( <cluster_ID>")
```

For example:

```
removePartnerForMultiDataCentre("cluster1")
```

You must run this command for each of the MDC partners. For more information about using the `removePartnerForMultiDataCentre()` command, see "removePartnerForMultiDataCentre" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

2. In 11.1.2.3.0, fail over for the MDC partners are supported. Therefore, you must specify the primary and secondary servers for each of the MDC partners using the Access Manager console. To do this, complete the following steps:

- a. Log in to the Access Manager 11.1.2.3.0 console using the following URL:

```
http://oam_admin_server_host:oam_admin_server_port/oamconsole
```

- b. Navigate to **SSO Agents**.

- c. Modify the **Primary Server** and **Secondary Server** for each of the MDC partners.

3. Add the modified MDC partners to the respective Data Centres using the following command:

```
addPartnerForMultiDataCentre(propfile= "../MDC_
properties/partnerInfo.properties")
```

While running this command, make sure you use the updated `partnerInfo.properties` file. You must run this command for each of the MDC partners. For more information about using the `addPartnerForMultiDataCentre()` command, see "addPartnerForMultiDataCentre" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

4. Verify that the **MultiDataCenterPartners** section in each of the MDC partner profile contains the following settings instead of the Hostname and Port:

```
<Setting Name="PrimaryHostPort" Type="xsd:string">
<Setting Name="SecondaryHostPort" Type="xsd:string">
```

---

---

## Upgrading Oracle Adaptive Access Manager Highly Available Environments

This chapter describes how to upgrade Oracle Adaptive Access Manager highly available environments to 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

---

---

**Note:** Before you proceed, check if your existing Oracle Adaptive Access Manager version is supported for high availability upgrade. For more information on supported starting points for high availability upgrade, see [Section 3.3, "Supported Starting Points for Oracle Identity and Access Management Manual Upgrade"](#).

---

---

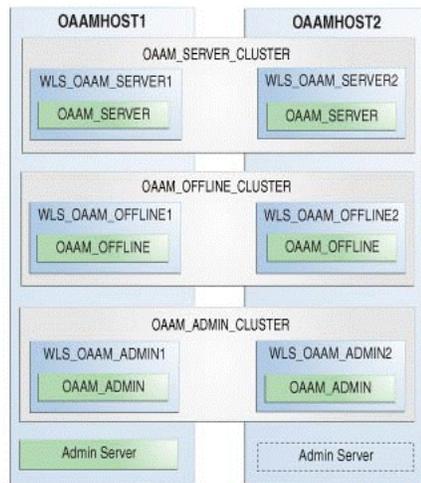
This chapter includes the following sections:

- [Section 19.1, "Understanding Oracle Adaptive Access Manager High Availability Upgrade Topology"](#)
- [Section 19.2, "Upgrade Roadmap"](#)
- [Section 19.3, "Shutting Down Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2"](#)
- [Section 19.4, "Backing Up the Existing Environment"](#)
- [Section 19.5, "Updating Binaries of WebLogic Server and Oracle Adaptive Access Manager on OAAMHOST2"](#)
- [Section 19.6, "Upgrading OAAMHOST1 to 11.1.2.3.0"](#)
- [Section 19.7, "Updating Component Versions on OAAMHOST1"](#)
- [Section 19.8, "Replicating Domain Configuration on OAAMHOST2"](#)
- [Section 19.9, "Starting Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2"](#)

## 19.1 Understanding Oracle Adaptive Access Manager High Availability Upgrade Topology

Figure 19–1 shows the Oracle Adaptive Access Manager cluster set up that can be upgraded to 11.1.2.3.0 by following the procedure described in this chapter.

**Figure 19–1 Oracle Adaptive Access Manager High Availability Upgrade Topology**



The host OAAMHOST1 contains the following:

- An Oracle Adaptive Access Manager Managed Server WLS\_OAAM\_SERVER1 that hosts Oracle Adaptive Access Manager Server application (OAAM\_SERVER).
- An Oracle Adaptive Access Manager Managed Server WLS\_OAAM\_OFFLINE1 that hosts Oracle Adaptive Access Manager Offline Server application (OAAM\_OFFLINE).
- An Oracle Adaptive Access Manager Managed Server WLS\_OAAM\_ADMIN1 that hosts Oracle Adaptive Access Manager Admin application (OAAM\_ADMIN).
- A WebLogic Server Administration Server. Under normal operations, this is the active Administration Server.

The host OAAMHOST2 contains the following:

- An Oracle Adaptive Access Manager Managed Server WLS\_OAAM\_SERVER2 that hosts Oracle Adaptive Access Manager Server application (OAAM\_SERVER).
- An Oracle Adaptive Access Manager Managed Server WLS\_OAAM\_OFFLINE2 that hosts Oracle Adaptive Access Manager Offline Server application (OAAM\_OFFLINE).
- An Oracle Adaptive Access Manager Managed Server WLS\_OAAM\_ADMIN2 that hosts Oracle Adaptive Access Manager Admin application (OAAM\_ADMIN).
- A WebLogic Server Administration Server. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on OAAMHOST1 becomes unavailable.

The Oracle Adaptive Access Manager Managed Servers WLS\_OAAM\_SERVER1 and WLS\_OAAM\_SERVER2 hosting Oracle Adaptive Access Manager Server application on OAAMHOST1 and OAAMHOST2 are configured in a cluster named OAAM\_SERVER\_CLUSTER, to work in active-active mode.

The Oracle Adaptive Access Manager Managed Servers WLS\_OAAM\_OFFLINE1 and WLS\_OAAM\_OFFLINE2 hosting Oracle Adaptive Access Manager Offline Server application on OAAMHOST1 and OAAMHOST2 are configured in a cluster named OAAM\_OFFLINE\_CLUSTER, to work in active-active mode.

The Oracle Adaptive Access Manager Managed Servers WLS\_OAAM\_ADMIN1 and WLS\_OAAM\_ADMIN2 hosting Oracle Adaptive Access Manager Admin application on OAAMHOST1 and OAAMHOST2 are configured in a cluster named OAAM\_ADMIN\_CLUSTER, to work in active-active mode.

## 19.2 Upgrade Roadmap

Table 19–1 lists the steps to upgrade Oracle Adaptive Access Manager high availability environment illustrated in Figure 19–1 to 11.1.2.3.0.

**Table 19–1 Oracle Adaptive Access Manager High Availability Upgrade Roadmap**

Task No	Task	For More Information
1	Review the Oracle Adaptive Access Manager high availability upgrade topology, and identify OAAMHOST1 and OAAMHOST2 on your setup.	See, <a href="#">Understanding Oracle Adaptive Access Manager High Availability Upgrade Topology</a>
2	Shut down the Administration Server and all the Managed Servers on OAAMHOST1 and OAAMHOST2.	See, <a href="#">Shutting Down Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2</a>
3	Back up the existing environment.	See, <a href="#">Backing Up the Existing Environment</a>
4	Update the binaries of Oracle WebLogic Server and Oracle Adaptive Access Manager on OAAMHOST2.	See, <a href="#">Updating Binaries of WebLogic Server and Oracle Adaptive Access Manager on OAAMHOST2</a>
5	Upgrade OAAMHOST1 to 11.1.2.3.0. This is the host with active Administration Server running on it.	See, <a href="#">Upgrading OAAMHOST1 to 11.1.2.3.0</a>
6	If your starting point is Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0), you must upgrade the OAAM packages to 11.1.2.3.0 on OAAMHOST1.	See, <a href="#">Updating Component Versions on OAAMHOST1</a>
8	If your starting point is Oracle Adaptive Access Manager 11.1.1.5.0, after you upgrade OAAMHOST1, you must replicate the configurations on OAAMHOST2 by packing the domain on OAAMHOST1 and unpacking it on OAAMHOST2.	See, <a href="#">Replicating Domain Configuration on OAAMHOST2</a>
6	Start the WebLogic Administration Server and the Managed Servers on OAAMHOST1 and OAAMHOST2.	See, <a href="#">Starting Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2</a>

## 19.3 Shutting Down Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2

Before you begin the upgrade process, you must stop the WebLogic Administration Server and all of the Oracle Adaptive Access Manager Managed Servers on OAAMHOST1 and OAAMHOST2 in the following order:

1. Stop the Oracle Adaptive Access Manager Managed Servers on both OAMHOST1 and OAMHOST2.
2. Stop the WebLogic Administration Server on OAMHOST1.

For information about stopping the Managed Server, see [Section 24.1.9.1, "Stopping the Managed Server\(s\)"](#).

For information about stopping the Administration Server, see [Section 24.1.9.2, "Stopping the WebLogic Administration Server"](#).

## 19.4 Backing Up the Existing Environment

After stopping all the servers, you must back up the following before proceeding with the upgrade process:

- `MW_HOME` directory (Middleware home directory), including the Oracle Home directories inside Middleware home on both OAMHOST1 and OAMHOST2.
- Oracle Adaptive Access Manager Domain Home directory on both OAMHOST1 and OAMHOST2.
- Following Database schemas:
  - Oracle Adaptive Access Manager schema
  - IAU schema, if it is part of any of your Oracle Adaptive Access Manager schemas
  - MDS schema

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

## 19.5 Updating Binaries of WebLogic Server and Oracle Adaptive Access Manager on OAMHOST2

Before you upgrade OAMHOST1 that hosts Administration Server, you must do the following on OAMHOST2:

and Oracle Adaptive Access Manager to 10.3.6 and 11.1.2.3.0 versions respectively on OAMHOST2. To do this, complete the following steps on OAMHOST2:

1. Upgrade Oracle WebLogic Server to 10.3.6 on OAMHOST2, if you are using a previous version.

For information about upgrading Oracle WebLogic Server to 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#)
2. Update the binaries of Oracle Adaptive Access Manager to 11.1.2.3.0 on OAMHOST2 using the Oracle Identity and Access Management 11.1.2.3.0 installer.

For information about upgrading Oracle Adaptive Access Manager binaries to 11.1.2.3.0, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#)

## 19.6 Upgrading OAMHOST1 to 11.1.2.3.0

After you upgrade the binaries of Oracle WebLogic Server and Oracle Adaptive Access Manager on OAMHOST2, you must upgrade OAMHOST1 which has the active

Administration Server. Upgrading OAAMHOST2 to 11.1.2.3.0 includes the following important tasks:

- Upgrading Oracle WebLogic Server to 10.3.6.
- Upgrading the Oracle Adaptive Access Manager binaries to 11.1.2.3.0.
- Upgrading the database schemas.
- Upgrading Oracle Platform Security Services.
- Redeploying applications.

The procedure to upgrade OAAMHOST1 depends on your starting point.

- If your starting point is Oracle Adaptive Access Manager 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0), follow the instructions described in [Chapter 9, "Upgrading Oracle Adaptive Access Manager 11g Release 2 \(11.1.2.x.x\) Environments"](#) to upgrade OAAMHOST1 to 11.1.2.3.0.
- If your starting point is Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0), follow the instructions described in [Chapter 13, "Upgrading Oracle Adaptive Access Manager 11g Release 1 \(11.1.1.x.x\) Environments"](#) to upgrade OAAMHOST1 to 11.1.2.3.0.

## 19.7 Updating Component Versions on OAAMHOST1

If your starting point is Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0), you must upgrade the following packages from 11g Release 1 (11.1.1.5.0) to 11g Release 2 (11.1.2.3.0):

- oracle.dogwood.top
- oracle.idm.oinav
- oracle.oaam.suite
- oracle.oaam.oaam\_admin
- oracle.oaam.oaam\_server
- oracle.oaam.oaam\_offline

---

**Note:** If your starting point is Oracle Adaptive Access Manager 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0) or 11g Release 2 (11.1.2), skip this task.

---

To upgrade the packages, you must run the domain updater utility (com.oracle.cie.domain-update\_1.0.0.0.jar) on OAAMHOST1 which updates the domain-info.xml. OAAMHOST1 is the host on which Administration Server is running.

To upgrade the necessary Oracle Adaptive Access Manager packages to 11.1.2.3.0, complete the following steps on OAAMHOST1:

1. Go to the directory `$ORACLE_HOME/oaam/upgrade`. The domain updater utility `com.oracle.cie.domain-update_1.0.0.0.jar` file is located in this directory.
2. Upgrade the packages using the following command:

```
java -cp MW_
HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
_1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
<package_name>:11.1.1.5.0, :11.1.2.3.0
```

In this command, *<DOMAIN\_HOME>* refers to the absolute path to the Oracle Adaptive Access Manager domain, and *<package\_name>* refers to the package that you are upgrading.

Run this command for all of the following packages:

- oracle.dogwood.top
- oracle.idm.oinav
- oracle.oaam.suite
- oracle.oaam.oaam\_admin
- oracle.oaam.oaam\_server
- oracle.oaam.oaam\_offline

## 19.8 Replicating Domain Configuration on OAAMHOST2

This step is applicable if you are upgrading Oracle Adaptive Access Manager 11g Release 1 (11.1.1.5.0) to 11.1.2.3.0.

After you upgrade Oracle Adaptive Access Manager 11.1.1.5.0 to 11.1.2.3.0 on OAAMHOST1, you must replicate the configurations on OAAMHOST2. This task involves packing the upgraded domain on OAAMHOST1 and unpacking it on OAAMHOST2.

---

---

**Note:** Make sure that the Managed Servers are stopped before you perform this step. Do not start the Managed Servers until you complete this task.

---

---

To do this, complete the following steps:

1. On OAAMHOST1, run the following command from the location *\$MW\_HOME/oracle\_common/common/bin* to pack the upgraded domain:

**On UNIX:**

```
sh pack.sh -domain=<Location_of_OAAM_domain> -template=<Location_where_domain_configuration_jar_to_be_created> -template_name="OAAM Domain" -managed=true
```

**On Windows:**

```
pack.cmd -domain=<Location_of_OAAM_domain> -template=<Location_where_domain_configuration_jar_needs_to_be_created> -template_name="OAAM Domain" -managed=true
```

2. Copy the domain configuration jar file created by the pack command on OAAMHOST1 to any accessible location on OAAMHOST2.
3. On OAAMHOST2, run the following command from the location *\$MW\_HOME/oracle\_common/common/bin* to unpack the domain:

**On UNIX:**

```
sh unpack.sh -domain=<Location_of_OAAM_domain> -template=<Location_on_OAAMHOST2_where_you_copied_jar_file_created_by_pack_command> -overwrite_domain=true
```

**On Windows:**

```
unpack.cmd -domain=<Location_of_OAAM_domain> -template=<Location_on_
OAAMHOST2_where_you_copied_jar_file_created_by_pack_command>
-overwrite_domain=true
```

## 19.9 Starting Administration Server and Managed Servers on OAAMHOST1 and OAAMHOST2

Start the WebLogic Administration Server and the Oracle Adaptive Access Manager Managed Servers on OAAMHOST1 and OAAMHOST2 in the following order:

1. Start the WebLogic Administration Server on OAAMHOST1.
2. Start the Oracle Adaptive Access Manager Managed Servers on OAAMHOST1 and OAAMHOST2.

For more information about starting the WebLogic Administration Server, see [Section 24.1.8.2, "Starting the WebLogic Administration Server"](#).

For more information about starting the Managed Servers, see [Section 24.1.8.3, "Starting the Managed Server\(s\)"](#).



---

---

## Upgrading Oracle Identity Manager Highly Available Environments

This chapter describes how to upgrade Oracle Identity Manager highly available environments to 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

---

---

**Note:** Before you proceed, check if your existing Oracle Access Management version is supported for high availability upgrade. For more information on supported starting points for high availability upgrade, see [Section 3.3, "Supported Starting Points for Oracle Identity and Access Management Manual Upgrade"](#).

---

---

This chapter includes the following sections:

- [Section 20.1, "Upgrade Roadmap"](#)
- [Section 20.2, "Understanding Oracle Identity Manager High Availability Upgrade Topology"](#)
- [Section 20.3, "Performing the Pre-Upgrade Tasks"](#)
- [Section 20.4, "Upgrading Oracle Home on OIMHOST1 and OIMHOST2"](#)
- [Section 20.5, "Upgrading Database Schemas on OIMHOST1"](#)
- [Section 20.6, "Performing OIM Middle Tier Upgrade Offline on OIMHOST1"](#)
- [Section 20.7, "Replicating Domain Configuration on OIMHOST2"](#)
- [Section 20.8, "Performing OIM Middle Tier Upgrade Online on OIMHOST1"](#)
- [Section 20.9, "Scaling out Oracle BI Publisher"](#)
- [Section 20.10, "Upgrading Other OIM Installed Components on OIMHOST1"](#)
- [Section 20.11, "Performing Post-Upgrade Tasks"](#)

- [Section 20.12, "Verifying the Upgrade"](#)
- [Section 20.13, "Troubleshooting"](#)

## 20.1 Upgrade Roadmap

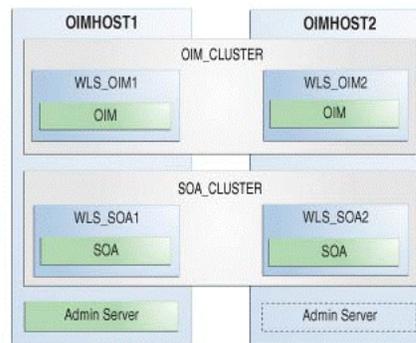
[Table 20–1](#) lists the steps to upgrade Oracle Identity Manager high availability environment illustrated in [Figure 20–1](#) to 11.1.2.3.0.

**Table 20–1 Oracle Identity Manager High Availability Upgrade Roadmap**

Task No	Task	For More Information
1	Review the Oracle Identity Manager high availability upgrade topology, and identify OIMHOST1 and OIMHOST2 on your setup.	See, <a href="#">Understanding Oracle Identity Manager High Availability Upgrade Topology</a>
2	Perform the necessary pre-upgrade tasks.	See, <a href="#">Performing the Pre-Upgrade Tasks</a>
3	Upgrade the binaries of Oracle WebLogic Server, Oracle SOA Suite, and Oracle Identity Manager on both OIMHOST1 and OIMHOST2.	See, <a href="#">Upgrading Oracle Home on OIMHOST1 and OIMHOST2</a>
4	Upgrade the Database schemas and create necessary schemas.	See, <a href="#">Upgrading Database Schemas on OIMHOST1</a>
5	Perform the Oracle Identity Manager middle tier upgrade offline on OIMHOST1 by running the middle tier upgrade utility offline.	See, <a href="#">Performing OIM Middle Tier Upgrade Offline on OIMHOST1</a>
6	Replicate the domain configuration on OIMHOST2 by pack the domain on OIMHOST1 and unpacking it on OIMHOST2.	See, <a href="#">Replicating Domain Configuration on OIMHOST2</a>
7	Perform the Oracle Identity Manager middle tier upgrade online on OIMHOST1 by running the middle tier upgrade utility online.	See, <a href="#">Performing OIM Middle Tier Upgrade Online on OIMHOST1</a>
8	Scale out the BI Publisher for high availability setup.	See, <a href="#">Scaling out Oracle BI Publisher</a>
9	Upgrade the Oracle Identity Manager Design Console and the Oracle Identity Manager Remote Manager to 11.1.2.3.0 on OIMHOST1.	See, <a href="#">Upgrading Other OIM Installed Components on OIMHOST1</a>
10	Perform the necessary post-upgrade tasks.	See, <a href="#">Performing Post-Upgrade Tasks</a>
11	Verify the upgrade.	See, <a href="#">Verifying the Upgrade</a>

## 20.2 Understanding Oracle Identity Manager High Availability Upgrade Topology

[Figure 20–1](#) shows the Oracle Identity Manager cluster set up that can be upgraded to 11.1.2.3.0 by following the procedure described in this chapter.

**Figure 20–1 Oracle Identity Manager High Availability Upgrade Topology**

On OIMHOST1, the following installations have been performed:

- An Oracle Identity Manager instance has been installed in the WLS\_OIM1 Managed Server and a SOA instance has been installed in the WLS\_SOA1 Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the active Administration Server.

On OIMHOST2, the following installations have been performed:

- An Oracle Identity Manager instance has been installed in the WLS\_OIM2 Managed Server and a SOA instance has been installed in the WLS\_SOA2 Managed Server.
- A WebLogic Server Administration Server has been installed. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on OIMHOST1 becomes unavailable.

The instances in the WLS\_OIM1 and WLS\_OIM2 Managed Servers on OIMHOST1 and OIMHOST2 are configured as the OIM\_CLUSTER cluster.

The instances in the WLS\_SOA1 and WLS\_SOA2 Managed Servers on OIMHOST1 and OIMHOST2 are configured as the SOA\_CLUSTER cluster.

## 20.3 Performing the Pre-Upgrade Tasks

Before you begin with the upgrade process, you must perform necessary pre-upgrade tasks on OIMHOST1. It includes reviewing the features of 11.1.2.3.0, reviewing system requirements and certifications, generating and analyzing the pre-upgrade report, backing up the existing environment, and other specific tasks required for your starting point.

If your starting point is Oracle Identity Manager 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0), or 11g Release 2 (11.1.2), perform the pre-upgrade tasks described in [Section 10.2, "Performing the Required Pre-Upgrade Tasks"](#).

If your starting point is Oracle Identity Manager 11g Release 1 (11.1.1.5.0), perform the pre-upgrade tasks described in [Section 14.2, "Performing the Required Pre-Upgrade Tasks"](#).

## 20.4 Upgrading Oracle Home on OIMHOST1 and OIMHOST2

You must upgrade the Oracle Home on both OIMHOST1 and OIMHOST2 by upgrading the binaries of Oracle WebLogic Server, Oracle SOA Suite, and Oracle Identity Manager to 10.3.6, 11.1.1.9.0, and 11.1.2.3.0 versions respectively.

---

---

**Note:** If you are using a shared file system, binary upgrade is not required on OIMHOST2.

---

---

If your starting point is Oracle Identity Manager 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0), or 11g Release 2 (11.1.2), follow the instructions described in [Section 10.3, "Upgrading Oracle Home"](#) to upgrade Oracle Home.

If your starting point is Oracle Identity Manager 11g Release 1 (11.1.1.5.0), follow the instructions described in [Section 14.3, "Upgrading Oracle Home"](#) to upgrade Oracle Home.

## 20.5 Upgrading Database Schemas on OIMHOST1

After you upgrade the Oracle Home, you must upgrade the Database schemas on OIMHOST1. Also, you must create Oracle BI Publisher (BIP) schemas.

If your starting point is Oracle Identity Manager 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0), or 11g Release 2 (11.1.2), follow the instructions described in [Section 10.4, "Creating Necessary Schemas and Upgrading Existing Schemas"](#) to upgrade Database schemas.

If your starting point is Oracle Identity Manager 11g Release 1 (11.1.1.5.0), follow the instructions described in [Section 14.4, "Creating Necessary Schemas and Upgrading the Existing Schemas"](#) to upgrade Database schemas.

## 20.6 Performing OIM Middle Tier Upgrade Offline on OIMHOST1

After you upgrade Oracle Home and Database schemas, you must perform Oracle Identity Manager middle tier upgrade offline. This is done by running the middle tier offline script.

To perform the Oracle Identity Manager middle tier upgrade offline, complete the following tasks described in [Section 24.2.4, "Upgrading Oracle Identity Manager Middle Tier"](#):

1. [Additional Task for Windows 64-Bit Users Before Upgrading Middle Tier](#)
2. [Creating a Truststore for Upgrading SSL Enabled Middleware](#)
3. [Updating the Properties File](#)
4. [Performing Oracle Identity Manager Middle Tier Upgrade Offline](#)

## 20.7 Replicating Domain Configuration on OIMHOST2

You must replicate the domain configuration on OIMHOST2. This task involves packing the upgraded domain on OIMHOST1 and unpacking it on OIMHOST2.

---



---

**Note:** Make sure that the Managed Servers are stopped before you perform this step. Do not start the Managed Servers until you complete this task.

---



---

To do this, complete the following steps:

1. On OIMHOST1, run the following command from the location `$MW_HOME/oracle_common/common/bin` to pack the upgraded domain:

**On UNIX:**

```
sh pack.sh -domain=<Location_of_OIM_domain> -template=<Location_where_domain_configuration_jar_to_be_created> -template_name="OIM Domain" -managed=true
```

**On Windows:**

```
pack.cmd -domain=<Location_of_OIM_domain> -template=<Location_where_domain_configuration_jar_needs_to_be_created> -template_name="OIM Domain" -managed=true
```

2. Copy the domain configuration jar file created by the pack command on OIMHOST1 to any accessible location on OIMHOST2.
3. On OIMHOST2, run the following command from the location `$MW_HOME/oracle_common/common/bin` to unpack the domain:

**On UNIX:**

```
sh unpack.sh -domain=<Location_of_OIM_domain> -template=<Location_on_OIMHOST2_where_you_copied_jar_file_created_by_pack_command> -overwrite_domain=true
```

**On Windows:**

```
unpack.cmd -domain=<Location_of_OIM_domain> -template=<Location_on_OIMHOST2_where_you_copied_jar_file_created_by_pack_command> -overwrite_domain=true
```

4. After you unpack the domain, copy the content of the following directory on OIMHOST1 to the same directory on OIMHOST2:

```
DOMAIN_HOME/soa/autodeploy
```

## 20.8 Performing OIM Middle Tier Upgrade Online on OIMHOST1

After you replicate the domain configuration on OIMHOST2, you must perform the Oracle Identity Manager middle tier upgrade online on OIMHOST1. This is done by running the middle tier online upgrade script.

To perform the Oracle Identity Manager middle tier upgrade online, complete the following tasks described in [Section 24.2.4, "Upgrading Oracle Identity Manager Middle Tier"](#):

1. [Starting Administration Server and SOA Managed Server\(s\)](#) - Start the WebLogic Administration Server and SOA Managed Server(s) on OIMHOST1.
2. [Performing Oracle Identity Manager Middle Tier Upgrade Online](#)
3. [Starting the Oracle Identity Manager Managed Server\(s\) and the BIP Server](#) - Start the Oracle Identity Manager Managed Server(s) on both OIMHOST1 and OIMHOST2, BIP Managed Server(s) on OIMHOST1, and the SOA Managed Server on OIMHOST2.

4. [Changing the Deployment Order of Oracle Identity Manager EAR](#) - Perform this step only if you are upgrading Oracle Identity Manager 11g Release 1 (11.1.1.5.0) environments.

## 20.9 Scaling out Oracle BI Publisher

This is an optional step.

After you upgrade the Oracle Identity Manager middle tier, if you wish to scale out the Oracle BI Publisher (BIP), complete the following steps:

1. [Creating a new BIP Server on OIMHOST2](#)
2. [Setting the Location of the Shared BI Publisher Configuration Folder](#)
3. [Setting Scheduler Configuration Options](#)
4. [Configuring JMS for BI Publisher](#)
5. [Verifying the BIP Server Scale Out](#)

### 20.9.1 Creating a new BIP Server on OIMHOST2

To create a new BIP server on OIMHOST2 and add it to the existing BIP cluster, do the following:

1. Log in to the WebLogic Administration Server using the following URL:  
`http://host:port/console`
2. Create a new BIP Server on OIMHOST2 and add it to the existing BIP cluster by completing the following steps:
  - a. Click **Lock & Edit** next to **Change Center** on the upper left of the WebLogic Administration Console screen.
  - b. Expand **Environment** under **Domain Structure**.
  - c. Click **Servers**. The **Summary of Servers** page is displayed.
  - d. Click **New**.
  - e. Specify the server name. For example, `bi_server2`.
  - f. Specify the **Server Listen Address** and **Server Listen Port**.
  - g. Select **Yes** for **Make this server a member of an existing cluster**, and select the BIP cluster.
  - h. Click **Next**, and then click **Finish**.
  - i. Click **Activate Changes**.
3. If you wish to start the BIP server on OIMHOST2 using the Node Manager, you must assign a machine to the BIP server. To do this, complete the following steps:
  - a. Click **Lock & Edit** next to **Change Center** on the upper left of the WebLogic Administration Console screen.
  - b. Expand **Environment** under **Domain Structure**.
  - c. Click **Servers**. The **Summary of Servers** page is displayed.
  - d. Select the BIP Server that you created on OIMHOST2.
  - e. Go to the **General** tab under **Configuration**.

- f. Select the Machine name from the Machine drop-down list.
- g. Click **Save**.
- h. Click **Activate Changes**.

## 20.9.2 Setting the Location of the Shared BI Publisher Configuration Folder

After creating a new BIP server on OIMHOST2, you must set the server configuration options for Oracle BI Publisher.

---

**Note:** If you are upgrading an Oracle Identity Manager, Access Manager, Oracle Adaptive Access Manager integrated environment, where the Administration Server and the Managed Servers have different domain location, follow the instructions described in [Steps for Setting Location of the Shared BI Publisher Configuration Folder in Case of an Integrated Environment](#) to set the shared BIP configuration folder location.

---

To set the server configuration options for Oracle BI Publisher, complete the following steps:

1. Copy the contents of the `DOMAIN_HOME/config/bipublisher/repository` directory to the shared configuration folder location.
2. On APPHOST1, log in to the BI Publisher using administrator's credentials.
3. Go to the **Administration** tab.
4. Select **Server Configuration** under **System Maintenance**.
5. Enter the shared location for the configuration folder in the **Path** field under **Configuration Folder**.
6. Enter the shared location for the BI Publisher Repository in the **BI Publisher Repository** field under **Catalog**.
7. Apply your changes.
8. Restart the BI Publisher application by doing the following:
  1. Log in to the WebLogic Administration Console using the following URL:  
`http://host:port/console`
  2. Expand **Deployments** under **Domain Structure**.
  3. Click **bipublisher(11.1.1.)**.
  4. Click **Stop** and then select **When work completes** or **Force Stop Now**.
  5. After the application has stopped, click **Start** and then select **servicing all requests**.

### Steps for Setting Location of the Shared BI Publisher Configuration Folder in Case of an Integrated Environment

If you are upgrading an Oracle Identity Manager, Access Manager, Oracle Adaptive Access Manager integrated environment, where the Administration Server and the Managed Servers have different domain location, complete the following steps to set the location of the shared BIP configuration folder:

1. Stop the BIP Managed Server(s) on OIMHOST1 and OIMHOST2. For information about stopping the servers, see [Section 24.1.9.1, "Stopping the Managed Server\(s\)"](#).
2. Copy the contents of the `DOMAIN_HOME/config/bipublisher/repository` directory to the shared configuration folder location.
3. Open the `xmlp-server-config.xml` file available in the Admin domain at the location at `DOMAIN_HOME/config/bipublisher/` on OIMHOST1.
4. Update the file path in the `xmlp-server-config.xml` file with the shared configuration folder location shown in the following example:
 

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<xmlpConfig xmlns="http://xmlns.example.com/oxp/xmlp">
  <resource>
    <file path="<shared configuration folder location>/repository"/>
  </resource>
  <config>
    <file path="<shared configuration folder location>/repository"/>
  </config>
</xmlpConfig>
```
5. Start the BI Managed Server(s) on OIMHOST1 and OIMHOST2.

### 20.9.3 Setting Scheduler Configuration Options

To set the scheduler configuration options, complete the following steps:

1. On APPHOST1, log in to the BI Publisher using administrator's credentials.
2. Go to the **Administration** tab.
3. Select **Scheduler Configuration** under **System Maintenance**.
4. Select **Quartz Clustering** under **Scheduler Selection**.
5. Click **Apply**.

### 20.9.4 Configuring JMS for BI Publisher

You must configure the location for all persistence stores to a directory that is accessible from both OIMHOST1 and OIMHOST2. This can be done by changing all persistent stores to use this shared base directory. To do this, complete the following steps:

1. Log in to the WebLogic Administration Console using the following URL:
 

```
http://host:port/console
```
2. Expand **Services** under **Domain Structure**.
3. Click **Persistent Stores**. The **Summary of Persistent Stores** page is displayed.
4. Click **Lock & Edit** under **Change Center**.
5. Click on an existing File Store (for example, `BipJmsStore`), and verify the target. If the target is `bi_server2`, then you must target the new File Store that you will be creating in the next step, to `bi_server1`.
6. Click **New** and then click **Create File Store**.
7. Enter a name for the new file store (for example, `BipJmsStore1`), and specify `bi_server1` as the **Target**. Specify the directory that is located in the shared storage which is accessible from both APPHOST1 and APPHOST2.

8. Click **OK**, and then click **Activate Changes**.
9. Go back to the home page of the WebLogic Administration Console, and expand **Services** under **Domain Structure**.
10. Click **Messaging**, and then select **JMS Servers**. The **Summary of JMS Servers** page is displayed.
11. Click **Lock & Edit** under **Change Center**.
12. Click **New**.
13. Enter a name for the JMS Server (for example, `BipJmsServer1`).
14. In the **Persistent Store** drop-down list, select the file store that you just created (for example, `BipJmsStore1`).
15. Click **Next**.
16. Select `bi_server1` as the **Target**.
17. Click **Finish**, and then click **Activate Changes**.
18. Go back to the home page of the WebLogic Administration console, and expand **Services** under **Domain Structure**.
19. Click **Messaging**, and select **JMS Modules**.
20. Click **Lock & Edit** under **Change Center**.
21. Click **BipJmsResource**, and go to the **Subdeployments** tab.
22. Select **BipJmsSubDeployment** under Subdeployments.
23. Add the newly created JMS Server (`BipJmsServer1`), as an additional target for the subdeployment.
24. Click **Save**, and then click **Activate Changes**.

To validate the JMS configuration for BI Publisher, complete the steps described in [Updating the BI Publisher Scheduler Configuration](#).

### Updating the BI Publisher Scheduler Configuration

This section describes how to update the JMS Shared Temp directory for the BI Publisher Scheduler. Complete the following steps on only one host, either `APPHOST1` or `APPHOST2`:

1. Log in to BI Publisher using the following URL:  

```
http://host:port/xmlpserver
```

For example:  

```
http://APPHOST1VHN1:9704/xmlpserver
```
2. Go to the **Administration** tab.
3. Click **Scheduler Configuration** under **System Maintenance**. The **Scheduler Configuration** screen is displayed.
4. Update **Shared Directory** with the directory that is located in the shared storage. This shared storage must be accessible from both `APPHOST1` and `APPHOST2`.
5. Click **Test JMS**.

---

---

**Note:** When you click Test JMS, a confirmation message is displayed indicating that the JMS was tested successfully.

If you do not see a confirmation message for a successful test, verify if the JDNI URL is set to the following:

```
cluster:t3://bi_cluster
```

---

---

6. Click **Apply**.
7. Go to the **Scheduler Diagnostics** tab, and check the Scheduler status.
8. Restart *bi\_server1* and *bi\_server2*.

---

---

**Note:** For more information about scaling out BI Publisher, see "Scaling Out the Oracle Business Intelligence System" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence* for 11g Release 1 (11.1.1.7.0).

---

---

### 20.9.5 Verifying the BIP Server Scale Out

Verify that you have successfully scaled out Oracle BI Publisher by starting the Node Manager, WebLogic Administration Server, SOA Managed Server, OIM Managed Server, and BIP Server on OIMHOST2, and checking the status of the servers in the WebLogic Administration console.

Verify that you can access BIP links on both OIMHOST1 and OIMHOST2 using the following URL:

```
http://host:port/xmlpserver
```

## 20.10 Upgrading Other OIM Installed Components on OIMHOST1

After you complete the middle tier upgrade, you must upgrade the Oracle Identity Manager Design Console and the Oracle Identity Manager Remote Manager to 11.1.2.3.0 on OIMHOST1.

For information about upgrading the Design Console and Remote Manager, see [Section 24.2.5, "Upgrading Other Oracle Identity Manager Installed Components"](#).

## 20.11 Performing Post-Upgrade Tasks

After you upgrade Oracle Identity Manager high availability environments to 11.1.2.3.0, you must perform the necessary post-upgrade tasks described in [Section 24.2.6, "Performing Oracle Identity Manager Post-Upgrade Tasks"](#).

## 20.12 Verifying the Upgrade

This section describes how to verify the upgrade.

If your starting point is Oracle Identity Manager 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0), or 11g Release 2 (11.1.2), you must complete the steps described in [Section 10.8, "Verifying the Oracle Identity Manager Upgrade"](#) to verify the upgrade.

If your starting point is Oracle Identity Manager 11g Release 1 (11.1.1.5.0), you must complete the steps described in [Section 14.8, "Verifying the Oracle Identity Manager Upgrade"](#) to verify the upgrade.

## 20.13 Troubleshooting

For the list of common issues that you might encounter during the Oracle Identity Manager upgrade process, and their workaround, see [Section 25.1, "Troubleshooting Oracle Identity Manager Upgrade Issues"](#).

For the list of known issues related to upgrade, and their workaround, see "Upgrade and Migration Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes for Identity Management*.



---

---

## Upgrading Oracle Entitlements Server Highly Available Environments

This chapter describes how to upgrade Oracle Entitlements Server highly available environments to 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

---

---

**Note:** Before you proceed, check if your existing Oracle Entitlements Server version is supported for high availability upgrade. For more information on supported starting points for high availability upgrade, see [Section 3.3, "Supported Starting Points for Oracle Identity and Access Management Manual Upgrade"](#).

---

---

This chapter includes the following sections:

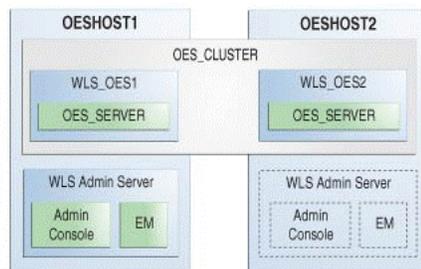
- [Section 21.1, "Understanding Oracle Entitlements Server High Availability Upgrade Topology"](#)
- [Section 21.2, "Upgrade Roadmap"](#)
- [Section 21.3, "Shutting Down Administration Server and Managed Servers on OESHOST1 and OESHOST2"](#)
- [Section 21.4, "Backing Up the Existing Environment"](#)
- [Section 21.5, "Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST1"](#)
- [Section 21.6, "Upgrading Oracle Platform Security Services Schema on OESHOST1"](#)
- [Section 21.7, "Upgrading Oracle Platform Security Services on OESHOST1 and OESHOST2"](#)

- Section 21.8, "Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST2"
- Section 21.9, "Redeploying APM Applications on OESHOST1 and OESHOST2"
- Section 21.10, "Starting Administration Server and Managed Servers on OESHOST1 and OESHOST2"

## 21.1 Understanding Oracle Entitlements Server High Availability Upgrade Topology

Figure 21–1 shows the Oracle Entitlements Server cluster set up that can be upgraded to 11.1.2.3.0 by following the procedure described in this chapter.

**Figure 21–1 Oracle Entitlements Server High Availability Upgrade Topology**



The host OESHOST1 has the following installations:

- An Oracle Entitlements Server instance in the WLS\_OES1 Managed Server.
- A WebLogic Server Administration Server. Under normal operations, this is the active Administration Server.

The host OESHOST2 has the following installations:

- An Oracle Entitlements Server instance in the WLS\_OES2 Managed Server.
- A WebLogic Server Administration Server. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on OESHOST1 becomes unavailable.

The instances in the WLS\_OES1 and WLS\_OES2 Managed Servers on OESHOST1 and OESHOST2 are configured in a cluster named OES\_CLUSTER.

## 21.2 Upgrade Roadmap

Table 21–1 lists the steps to upgrade Oracle Entitlements Server high availability environment illustrated in Figure 21–1 to 11.1.2.3.0.

**Table 21–1 Oracle Entitlements Server High Availability Upgrade Roadmap**

Task No	Task	For More Information
1	Review the Oracle Entitlements Server high availability upgrade topology, and identify OESHOST1 and OESHOST2 on your setup.	See, <a href="#">Understanding Oracle Entitlements Server High Availability Upgrade Topology</a>

**Table 21–1 (Cont.) Oracle Entitlements Server High Availability Upgrade Roadmap**

Task No	Task	For More Information
2	Shut down the Administration Server and all the Managed Servers on OESHOST1 and OESHOST2.	See, <a href="#">Shutting Down Administration Server and Managed Servers on OESHOST1 and OESHOST2</a>
3	Back up the Middleware home, Oracle home, and the Oracle Platform Security Services schema on OESHOST1 and OESHOST2.	See, <a href="#">Backing Up the Existing Environment</a>
4	Update the binaries of Oracle WebLogic Server and Oracle Entitlements Server on OESHOST1.	See, <a href="#">Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST1</a>
5	Upgrade the Oracle Platform Security Services schema on OESHOST1.	See, <a href="#">Upgrading Oracle Platform Security Services Schema on OESHOST1</a>
6	Upgrade Oracle Platform Security Services on OESHOST1 and OESHOST2.	See, <a href="#">Upgrading Oracle Platform Security Services on OESHOST1 and OESHOST2</a>
7	Update the binaries of Oracle WebLogic Server and Oracle Entitlements Server on OESHOST2.	See, <a href="#">Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST2</a>
8	Redeploy the following APM applications on OESHOST1 and OESHOST2.	See, <a href="#">Redeploying APM Applications on OESHOST1 and OESHOST2</a>
9	Start the WebLogic Administration Server and the Managed Servers on OESHOST1 and OESHOST2.	See, <a href="#">Starting Administration Server and Managed Servers on OESHOST1 and OESHOST2</a>

## 21.3 Shutting Down Administration Server and Managed Servers on OESHOST1 and OESHOST2

Before you begin the upgrade process, you must stop the WebLogic Administration Server and all the Oracle Entitlements Server Managed Servers on OESHOST1 and OESHOST2 in the following order:

1. Stop the Oracle Entitlements Server Managed Servers on both OESHOST1 and OESHOST2.
2. Stop the WebLogic Administration Server on OESHOST1.

For information about stopping the Managed Server, see [Section 24.1.9.1, "Stopping the Managed Server\(s\)"](#).

For information about stopping the Administration Server, see [Section 24.1.9.2, "Stopping the WebLogic Administration Server"](#).

## 21.4 Backing Up the Existing Environment

After stopping all the servers, you must back up the following before proceeding with the upgrade process:

- *MW\_HOME* directory (Middleware home directory), including the Oracle Home directories inside Middleware home on both OESHOST1 and OESHOST2.
- Oracle Entitlements Server Domain Home directory on both OESHOST1 and OESHOST2.
- Oracle Platform Security Services schema

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

## 21.5 Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST1

Oracle Identity and Access Management is certified with Oracle WebLogic Server 10.3.6. Therefore, if you are not using Oracle WebLogic Server 10.3.6, you must upgrade Oracle WebLogic Server to 10.3.6 on OESHOST1. For information about upgrading Oracle WebLogic Server to 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

After you upgrade Oracle WebLogic Server to 10.3.6, update the binaries of Oracle Entitlements Server to 11.1.2.3.0 on OESHOST1 using the Oracle Identity and Access Management 11.1.2.3.0 installer. For information about upgrading Oracle Entitlements Server binaries, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 21.6 Upgrading Oracle Platform Security Services Schema on OESHOST1

After updating the Oracle WebLogic Server and Oracle Entitlements Server binaries on OESHOST1, you must upgrade the Oracle Platform Security Services schema using Patch Set Assistant.

For information about upgrading schemas using Patch Set Assistant, see [Section 24.1.4, "Upgrading Schemas Using Patch Set Assistant"](#).

## 21.7 Upgrading Oracle Platform Security Services on OESHOST1 and OESHOST2

After you upgrade Oracle Platform Security Services schema on OESHOST1, you must upgrade Oracle Platform Security Services (OPSS) on OESHOST1 and OESHOST2. This task is optional; however, it is recommended that you perform this task.

---

---

**Note:** If you are upgrading Oracle Entitlements Server 11.1.2.1.0 environments to 11.1.2.3.0, you must upgrade Oracle Platform Security Services if Audit schema is installed. This step is required to upgrade the policy store to include the new 11.1.2.3.0 audit policies.

---

---

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores of Oracle Entitlements Server to 11.1.2.3.0. It upgrades the `jps-config.xml` file and policy stores.

For information about upgrading Oracle Platform Security Services, see [Section 24.1.7, "Upgrading Oracle Platform Security Services"](#).

## 21.8 Updating Binaries of WebLogic Server and Oracle Entitlements Server on OESHOST2

After upgrading Oracle Platform Security Services on OESHOST1, you must update the binaries of Oracle WebLogic Server to 10.3.6 on OESHOST2 (if you are not using Oracle WebLogic Server 10.3.6 already). Also, you must update the binaries of Oracle

Entitlements Server to 11.1.2.3.0 on OESHOST2 using the Oracle Identity and Access Management 11.1.2.3.0 installer.

For information about upgrading Oracle WebLogic Server to 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

For information about upgrading Oracle Entitlements Server binaries, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 21.9 Redeploying APM Applications on OESHOST1 and OESHOST2

After you update Oracle Entitlements Server binaries on OESHOST2, you must redeploy the following APM applications on OESHOST1 and OESHOST2:

- oracle.security.apm.ear
- oracle.security.apm.core.model.ear
- oracle.security.apm.core.view.war

To redeploy the APM applications, do the following:

1. Start the WebLogic Administration Server. For more information, see [Section 24.1.8.2, "Starting the WebLogic Administration Server"](#).
2. Launch the WebLogic Scripting Tool (WLST) by running the command from the location `$MWHOME/wlserver_10.3/common/bin`:

On UNIX: `./wlst.sh`

On Windows: `wlst.cmd`

3. Connect to the Administration Server by running the following command:  
`connect('weblogic-username','weblogic-password','weblogic-url')`
4. Run the following commands to redeploy the APM applications:

On UNIX:

- `redeploy(appName='oracle.security.apm')`
- `redeploy(appName='oracle.security.apm.core.model')`
- `redeploy(appName='oracle.security.apm.core.view')`

On Windows:

- `$DOMAIN_HOME\serverConfig\redeploy(appName='oracle.security.apm')`
- `$DOMAIN_HOME\serverConfig\redeploy(appName='oracle.security.apm.core.model')`
- `$DOMAIN_HOME\serverConfig\redeploy(appName='oracle.security.apm.core.view')`

In these commands, `$DOMAIN_HOME` refers to the absolute path to the Oracle Entitlements Server 11.1.2.3.0 domain.

The following is an example of redeploying an APM application on Windows:

```
C:\Oracle\Middleware\user_projects\domains\OES_Domain\serverConfig\
redeploy(appName='oracle.security.apm')
```

5. Stop the WebLogic Administration Server. For more information, see [Section 24.1.8.2, "Starting the WebLogic Administration Server"](#).

## 21.10 Starting Administration Server and Managed Servers on OESHOST1 and OESHOST2

Start the WebLogic Administration Server and the Oracle Entitlements Server Managed Servers on OESHOST1 and OESHOST2 in the following order:

1. Start the WebLogic Administration Server on OESHOST1.
2. Start the Oracle Entitlements Server Managed Servers on OESHOST1 and OESHOST2.

For more information about starting the WebLogic Administration Server, see [Section 24.1.8.2, "Starting the WebLogic Administration Server"](#).

For more information about starting the Managed Servers, see [Section 24.1.8.3, "Starting the Managed Server\(s\)"](#).

---

---

## Upgrading Oracle Privileged Account Manager Highly Available Environments

This chapter describes how to upgrade Oracle Privileged Account Manager highly available environments to 11g Release 2 (11.1.2.3.0) on Oracle WebLogic Server, using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

---

---

**Note:** Before proceeding, check if your existing Oracle Privileged Account Manager version is supported for high availability upgrade. For more information on supported starting points for high availability upgrade, see [Section 3.3, "Supported Starting Points for Oracle Identity and Access Management Manual Upgrade"](#).

---

---

This chapter includes the following sections:

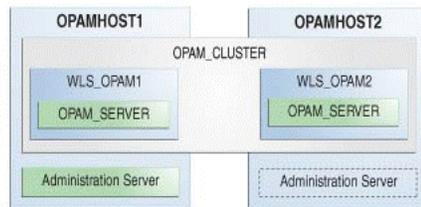
- [Section 22.1, "Understanding Oracle Privileged Account Manager High Availability Upgrade Topology"](#)
- [Section 22.2, "Upgrade Roadmap"](#)
- [Section 22.3, "Shutting Down all Servers on OPAMHOST1 and OPAMHOST2"](#)
- [Section 22.4, "Backing Up the Existing Environment"](#)
- [Section 22.5, "Updating Binaries of WebLogic Server and Oracle Privileged Account Manager on OPAMHOST1 and OPAMHOST2"](#)
- [Section 22.6, "Upgrading Database Schemas on OPAMHOST1"](#)
- [Section 22.7, "Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2"](#)
- [Section 22.8, "Redeploying Applications on OPAMHOST1"](#)
- [Section 22.9, "Verifying the Domain Upgrade"](#)

- [Section 22.10, "Optional: Configuring Oracle Privileged Account Manager Session Manager"](#)
- [Section 22.11, "Optional: Configuring Oracle Privileged Account Manager Console Application on WLS\\_OPAM1 and WLS\\_OPAM2"](#)

## 22.1 Understanding Oracle Privileged Account Manager High Availability Upgrade Topology

Figure 22–1 shows the Oracle Privileged Account Manager cluster set up that can be upgraded to 11.1.2.3.0 by following the procedure described in this chapter.

**Figure 22–1 Oracle Privileged Account Manager High Availability Upgrade Topology**



The host OPAMHOST1 has the following installations:

- An Oracle Privileged Account Manager instance in the WLS\_OPAM1 Managed Server.
- A WebLogic Server Administration Server. Under normal operations, this is the active Administration Server.

The host OPAMHOST2 has the following installations:

- An Oracle Privileged Account Manager instance in the WLS\_OPAM2 Managed Server.
- A WebLogic Server Administration Server. Under normal operations, this is the passive Administration Server. You make this Administration Server active if the Administration Server on OPAMHOST1 becomes unavailable.

The instances in the WLS\_OPAM1 and WLS\_OPAM2 Managed Servers on OPAMHOST1 and OPAMHOST2 are configured as the cluster named OPAM\_CLUSTER.

## 22.2 Upgrade Roadmap

Table 22–1 lists the steps to upgrade Oracle Privileged Account Manager high availability environment illustrated in Figure 22–1 to 11.1.2.3.0.

**Table 22–1 Oracle Privileged Account Manager High Availability Upgrade Roadmap**

Task No	Task	For More Information
1	Review the Oracle Privileged Account Manager high availability upgrade topology, and identify OPAMHOST1 and OPAMHOST2 on your setup.	See, <a href="#">Understanding Oracle Privileged Account Manager High Availability Upgrade Topology</a>

**Table 22–1 (Cont.) Oracle Privileged Account Manager High Availability Upgrade**

<b>Task No</b>	<b>Task</b>	<b>For More Information</b>
2	Shut down the Administration Server, Oracle Privileged Account Manager Managed Servers, and the Node Manager on OPAMHOST1 and OPAMHOST2.	See, <a href="#">Shutting Down all Servers on OPAMHOST1 and OPAMHOST2</a>
3	Back up the Middleware Home, the Oracle Home, and the Database schemas on OPAMHOST1 and OPAMHOST2.	See, <a href="#">Backing Up the Existing Environment</a>
4	Update the binaries of WebLogic Server and Oracle Privileged Account Manager on OPAMHOST1 and OPAMHOST2.	See, <a href="#">Updating Binaries of WebLogic Server and Oracle Privileged Account Manager on OPAMHOST1 and OPAMHOST2</a>
5	Upgrade the OPAM and OPSS schema on OPAMHOST1 by running the Patch Set Assistant.	See, <a href="#">Upgrading Database Schemas on OPAMHOST1</a>
6	Start the WebLogic Administration Server and all the Managed Servers on OPAMHOST1 and OPAMHOST2.	See, <a href="#">Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2</a>
7	Redeploy the Oracle Privileged Account Manager Console application, Oracle Privileged Account Manager applications, and Oracle Privileged Account Manager Session Manager application on OPAMHOST1.	See, <a href="#">Redeploying Applications on OPAMHOST1</a>
8	Verify the domain upgrade.	See, <a href="#">Verifying the Domain Upgrade</a>
9	If you are upgrading Oracle Privileged Account Manager 11g Release 2 (11.1.2.1.0) or 11g Release 2 (11.1.2), and if you wish to configure Oracle Privileged Account Manager session manager, you can do so by running the WLST command <code>configureSessionManager.py</code> , and targeting it to the <code>OPAM_CLUSTER</code> .  This step is optional.	See, <a href="#">Optional: Configuring Oracle Privileged Account Manager Session Manager</a>
10	If you wish to configure Oracle Privileged Account Manager Console application on the Oracle Privileged Account Manager Managed Servers <code>WLS_OPAM1</code> and <code>WLS_OPAM2</code> , you can do so by running WLST script <code>configureOPAMConsole.py</code> on OPAMHOST1.  This step is optional.	See, <a href="#">Optional: Configuring Oracle Privileged Account Manager Console Application on WLS_OPAM1 and WLS_OPAM2</a>

## 22.3 Shutting Down all Servers on OPAMHOST1 and OPAMHOST2

Before you begin the upgrade process, you must stop the WebLogic Administration Server, Oracle Privileged Account Manager Managed Servers, and Node Manager on OPAMHOST1 and OPAMHOST2 in the following order:

1. Stop the Oracle Privileged Account Manager Managed Servers on both OPAMHOST1 and OPAMHOST2.
2. Stop the WebLogic Administration Server on OPAMHOST1.

3. Stop the Node Manager on OPAMHOST1 and OPAMHOST2.

For information about stopping the Managed Server, see [Section 24.1.9.1, "Stopping the Managed Server\(s\)"](#).

For information about stopping the Administration Server, see [Section 24.1.9.2, "Stopping the WebLogic Administration Server"](#).

For information about stopping the Node Manager, see [Section 24.1.9.3, "Stopping the Node Manager"](#).

## 22.4 Backing Up the Existing Environment

After stopping all the servers, you must back up the following before proceeding with the upgrade process:

- *MW\_HOME* directory (Middleware home directory), including the Oracle Home directories inside Middleware home on both OPAMHOST1 and OPAMHOST2.
- Oracle Privileged Account Manager Domain Home directory on both OPAMHOST1 and OPAMHOST2.
- Following Database schemas:
  - Oracle Privileged Account Manager schema
  - Oracle Platform Security Services schema

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

## 22.5 Updating Binaries of WebLogic Server and Oracle Privileged Account Manager on OPAMHOST1 and OPAMHOST2

Oracle Identity and Access Management is certified with Oracle WebLogic Server 10.3.6. Therefore, if you are not using Oracle WebLogic Server 10.3.6, you must upgrade Oracle WebLogic Server to 10.3.6 on OPAMHOST1 and OPAMHOST2. For information about upgrading Oracle WebLogic Server to 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

After you upgrade Oracle WebLogic Server to 10.3.6, update the binaries of Oracle Privileged Account Manager to 11.1.2.3.0 on both OPAMHOST1 and OPAMHOST2 using the Oracle Identity and Access Management 11.1.2.3.0 installer. For information about upgrading Oracle Privileged Account Manager binaries, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 22.6 Upgrading Database Schemas on OPAMHOST1

On OPAMHOST1, you must upgrade the following schemas by running the Patch Set Assistant:

- OPAM schema
- OPSS schema - OPSS schema is selected as a dependency when you select OPAM.

For information about upgrading schemas using Patch Set Assistant, see [Section 24.1.4, "Upgrading Schemas Using Patch Set Assistant"](#).

After you upgrade the OPAM and OPSS schemas, the version of the OPAM schema will be 11.1.2.3.0.

## 22.7 Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2

After upgrading the database schemas on OPAMHOST1, you must start the WebLogic Administration Server, Node Manager, and the Oracle Privileged Account Manager Managed Servers on OPAMHOST1 and OPAMHOST2 in the following order:

1. On OPAMHOST1, start the WebLogic Administration Server, Node Manager, and Oracle Privileged Account Manager Managed Server.
2. On OPAMHOST2, start the Node Manager, and the Oracle Privileged Account Manager Managed Server.

For more information about starting the WebLogic Administration Server, see [Section 24.1.8.2, "Starting the WebLogic Administration Server"](#).

For more information about starting the Node Manager, see [Section 24.1.8.1, "Starting the Node Manager"](#).

For more information about starting the Managed Servers, see [Section 24.1.8.3, "Starting the Managed Server\(s\)"](#).

## 22.8 Redeploying Applications on OPAMHOST1

After you start the servers, you must redeploy Oracle Identity Navigator and Oracle Privileged Account Manager applications on OPAMHOST1 namely `oinav.ear` and `opam.ear`. You can do this using either the WebLogic Administration console or the WebLogic Scripting Tool (WLST).

For more information about redeploying Oracle Identity Navigator and Oracle Privileged Account Manager applications, see [Section 7.9, "Redeploying the Applications"](#).

## 22.9 Verifying the Domain Upgrade

Verify that the Oracle Privileged Account Manager domain was upgraded successfully by doing the following:

1. Log in to the Oracle Privileged Account Manager 11.1.2.3.0 console using the following URL:

```
http://adminserver_host:adminserver_port/oinav/opam
```

2. Verify that the pre-upgrade data, targets, accounts, grants are present, and working as expected.

## 22.10 Optional: Configuring Oracle Privileged Account Manager Session Manager

The Oracle Privileged Account Manager session manager application named `opamsessionmgr` was introduced in 11.1.2.2.0. If you are upgrading Oracle Privileged Account Manager 11g Release 2 (11.1.2.1.0) or 11g Release 2 (11.1.2), and if you want to configure the Oracle Privileged Account Manager session manager application, you must run the WebLogic Scripting Tool (WLST) command `configureSessionManager.py` on OPAMHOST1, and target it to the `OPAM_CLUSTER`.

For more information about configuring Oracle Privileged Account Manager session manager, see [Section 7.13, "Optional: Configuring the Oracle Privileged Account Manager 11.1.2.3.0 Session Manager"](#).

After you configure Oracle Privileged Account Manager session manager, start all the servers on OPAMHOST1 and OPAMHOST2. For more information about starting all the servers, see [Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2](#).

## 22.11 Optional: Configuring Oracle Privileged Account Manager Console Application on WLS\_OPAM1 and WLS\_OPAM2

If you wish to configure Oracle Privileged Account Manager console application on the Oracle Privileged Account Manager Managed Servers WLS\_OPAM1 and WLS\_OPAM2 in order to achieve high availability use cases for the Oracle Privileged Account Manager console, complete the steps described in [Section 7.14, "Optional: Configuring Oracle Privileged Account Manager Console Application on OPAM Managed Server"](#).

After you complete the upgrade, start all the servers on OPAMHOST1 and OPAMHOST2. For more information about starting all the servers, see [Starting Administration Server, Node Manager, and Managed Servers on OPAMHOST1 and OPAMHOST2](#).

To verify the upgrade, follow the instructions described in [Section 7.15, "Verifying the Oracle Privileged Account Manager Upgrade"](#).

---

---

## Upgrading OIM-OAM Integrated Highly Available Environments

This chapter describes how to upgrade Oracle Identity Manager (OIM), Oracle Access Management Access Manager (Access Manager), and Oracle Adaptive Access Manager (OAAM) integrated split domain highly available environments to 11g Release 2 (11.1.2.3.0) using the manual upgrade procedure.

---

---

**Note:** If your existing Oracle Identity and Access Management environment was deployed using the Life Cycle Management (LCM) Tools, you must use the automated upgrade procedure to upgrade to Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0).

For information about automated upgrade procedure, supported starting points and topologies, see [Chapter 2, "Understanding the Oracle Identity and Access Management Automated Upgrade"](#).

---

---

This chapter includes the following sections:

- [Section 23.1, "Understanding the Integrated HA Upgrade Topology"](#)
- [Section 23.2, "Upgrade Overview"](#)
- [Section 23.3, "Supported Starting Points for an Integrated, HA Upgrade"](#)
- [Section 23.4, "Roadmap for Upgrading OIM/OAM/OAAM Integrated Highly Available Environments"](#)
- [Section 23.5, "Performing the Required Pre-Upgrade Tasks"](#)
- [Section 23.6, "Upgrading Oracle Home"](#)
- [Section 23.7, "Creating Necessary Schemas and Upgrading the Existing Schemas"](#)
- [Section 23.8, "Upgrading Oracle Identity Manager Domain"](#)
- [Section 23.9, "Upgrading Oracle Access Management Domain Which Also Contains Oracle Adaptive Access Manager"](#)
- [Section 23.10, "Seeding the Oracle Identity Manager 11.1.2.3.0 Resources in Oracle Access Management"](#)
- [Section 23.11, "Verifying the Upgraded Environment"](#)
- [Section 23.12, "Troubleshooting"](#)

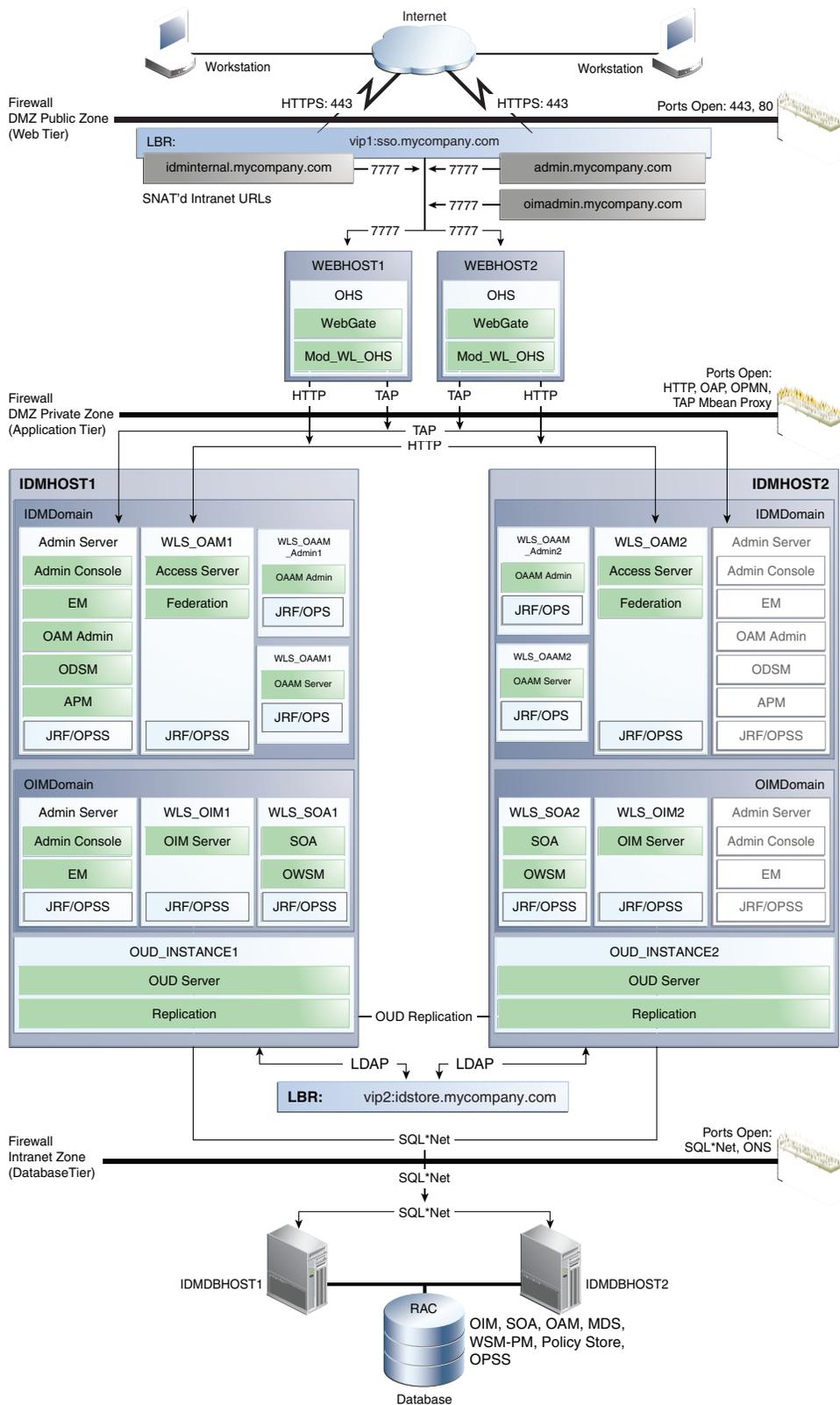
## 23.1 Understanding the Integrated HA Upgrade Topology

This chapter describes how to upgrade the topology shown in [Figure 23–1](#). This topology is based on the split domain topology described in the *Enterprise Deployment Guide for Oracle Identity and Access Management 11g Release 2 (11.1.2.1)*. It has been modified to include Oracle Adaptive Access Manager (OAAM).

This topology and the accompanying procedures in this chapter are provided to serve as an example for upgrading a highly available, integrated Oracle Identity and Access Management environment. Your specific Oracle Identity and Access Management installation will vary, but this topology and upgrade procedure demonstrates the key elements of the upgrade process, which can be applied to your specific environment.

For a complete description of the topology diagram, refer to the *Enterprise Deployment Guide* in the Oracle Identity and Access Management 11g Release 2 (11.1.2.1) Documentation Library.

Figure 23-1 Starting Point for the OIM/OAM/OAAM Integrated HA Upgrade



## 23.2 Upgrade Overview

The procedure for upgrading the OIM-OAM-OAAM integrated highly available environments involves the following high level tasks:

- 1. Pre-Upgrade Tasks:** This step includes reviewing system requirements, reviewing the customizations that are lost as part of the upgrade, generating the pre-upgrade reports and completing the necessary tasks specified in the pre-upgrade report, backing up the existing environment, and stopping the servers.
- 2. Upgrading Oracle Home:** This step includes upgrading the binaries of Oracle WebLogic Server (if necessary), Oracle SOA Suite, Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager using the Oracle Universal Installer.
- 3. Creating Necessary Schemas and Upgrading the Existing Schemas:** This step includes creating new schemas like Oracle Mobile Security Manager (OMSM) schema, Oracle BI Publisher (BIP) schema and upgrading the existing schemas like Oracle Identity Manager schema, Oracle Access Manager schema, Oracle Platform Security Services schema and so on.
- 4. Upgrading Oracle Identity Manager Domain:** This step includes tasks like upgrading the Oracle Identity Manager middle tier, scaling out Oracle Business Publisher, upgrading Oracle Remote Manager and Oracle Design Console and so on.
- 5. Upgrading Oracle Access Management Domain Which Also Contains Oracle Adaptive Access Manager:** This step includes tasks like upgrading Oracle Access Management system configurations, extending the Oracle Access Management domain to include Oracle Mobile Security Suite and Policy Manager and so on. The Oracle Access Management domain also contains Oracle Adaptive Access Manager (OAAM). Therefore, you must redeploy OAAM applications as part of the Access Manager domain upgrade.
- 6. Seeding the Oracle Identity Manager 11.1.2.3.0 Resources in Oracle Access Management:** If you upgraded Oracle Identity Manager domain prior to upgrading Oracle Access Management domain, you must run the `-configOIM` command to seed the Oracle Identity Manager 11.1.2.3.0 resources in Oracle Access Management.  
  
This step is not required if you upgraded Oracle Access Management domain first.
- 7. Verifying the Upgraded Environment:** This step includes tasks for verifying if the upgrade was successful.

---

**Note:** It is assumed that you are running Oracle HTTP Server (OHS) 11g Release 1 (11.1.1.6.0), WebGate 11g Release 2 (11.1.2.1.0), and Oracle Unified Directory (OUD) 11g Release 2 (11.1.2.1.0) installed with Oracle Identity and Access Management 11g Release 2 (11.1.2.1.0).

Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) is compatible with Oracle HTTP Server 11g Release 1 (11.1.1.6.0), WebGate 11g Release 2 (11.1.2.1.0), and Oracle Unified Directory (OUD) 11g Release 2 (11.1.2.1.0). Therefore, it is not mandatory to upgrade these components. However, if you wish to upgrade them, refer to the following document:

For information about upgrading Oracle HTTP Server to 11g Release 1 (11.1.1.9.0), see "Task 4: Upgrading the Oracle HTTP Server Oracle Home Using the Oracle Web Tier Patch Set Installer" in the Oracle Fusion Middleware Patching Guide for 11g Release 1 (11.1.1.9.0). When you run the Patch Set Installer for upgrading Oracle HTTP Server, select **Install Software and Do Not configure** option on the **Select Installation Type** screen.

For information about upgrading WebGate to 11g Release 2 (11.1.2.3.0), use the instructions described in the *Oracle Fusion Middleware Installing WebGates for Oracle Access Manager*. During the process, ensure that you point to the existing 11g Release 2 (11.1.2.1.0) WebGates, when prompted.

For information about upgrading Oracle Unified Directory (OUD) to 11g Release 2 (11.1.2.3.0), see "Updating the Oracle Unified Directory Software" in the *Oracle Fusion Middleware Installing Oracle Unified Directory*.

---

## 23.3 Supported Starting Points for an Integrated, HA Upgrade

Table 23–1 lists the starting points that are supported for upgrade of an integrated highly available environments.

**Table 23–1 Supported Starting Points for Upgrade of an Integrated Environment**

Component	Supported Starting Point
Oracle Identity Manager	11g Release 2 (11.1.2.1.0)
Oracle Access Management	11g Release 2 (11.1.2.1.0)
Oracle Adaptive Access Manager	11g Release 2 (11.1.2.1.0)
Oracle SOA Suite	11g Release 1 (11.1.1.6.0)
Oracle WebLogic Server	10.3.6  Oracle Identity and Access Management 11.1.2.3.0 is compatible with Oracle WebLogic Server 10.3.6. Therefore, you do not have to upgrade Oracle WebLogic Server if you are already using 10.3.6 version.

## 23.4 Roadmap for Upgrading OIM/OAM/OAAM Integrated Highly Available Environments

Table 23–2 lists the tasks that you must complete to upgrade an integrated high availability environment.

**Table 23–2 Upgrade Roadmap**

	Task	For more information,
1	Review the topology that can be upgraded using the procedure described in this chapter.	See, <a href="#">Understanding the Integrated HA Upgrade Topology</a>
2	Review the supported starting points for upgrading integrated environments.	See, <a href="#">Supported Starting Points for an Integrated, HA Upgrade</a>
3	Complete the necessary pre-upgrade tasks before you start the upgrade process.	See, <a href="#">Performing the Required Pre-Upgrade Tasks</a>
4	Upgrade Oracle Home by upgrading the binaries of Oracle Identity and Access Management, Oracle WebLogic Server, and Oracle SOA Suite.	See, <a href="#">Upgrading Oracle Home</a>
5	Create necessary database schemas using the Repository Creation Utility (RCU), and upgrade the existing schemas using the Patch Set Assistant (PSA).	See, <a href="#">Creating Necessary Schemas and Upgrading the Existing Schemas</a>
6	Upgrade the Oracle Identity Manager domain.	See, <a href="#">Upgrading Oracle Identity Manager Domain</a>
7	Upgrade the Oracle Access Management domain. This domain also includes Oracle Adaptive Access Manager.	See, <a href="#">Upgrading Oracle Access Management Domain Which Also Contains Oracle Adaptive Access Manager</a>
8	If you upgraded Oracle Identity Manager domain prior to upgrading Oracle Access Management domain, you must run the <code>-configOIM</code> command to seed the Oracle Identity Manager 11.1.2.3.0 resources in Oracle Access Management.	See, <a href="#">Seeding the Oracle Identity Manager 11.1.2.3.0 Resources in Oracle Access Management</a>
9	Verify the OIM-OAM-OAAM integrated upgrade.	See, <a href="#">Verifying the Upgraded Environment</a>

## 23.5 Performing the Required Pre-Upgrade Tasks

Before you start with the upgrade, you must complete the following pre-upgrade tasks:

1. Review the *Oracle Fusion Middleware System Requirements and Specifications* and *Oracle Fusion Middleware Supported System Configurations* documents to ensure that your system meets the minimum requirements for the products you are installing or upgrading to. For more information see [Section 24.1.1, "Verifying Certification, System Requirements, and Interoperability"](#).
2. Ensure that you are using a Java Development Kit (JDK) version that is supported and certified with Oracle Identity and Access Management 11.1.2.3.0.

You can verify the required JDK version by reviewing the certification information on the *Oracle Fusion Middleware Supported System Configurations* page.

The JDK can be downloaded from the Java SE Development Kit 7 Downloads page on Oracle Technology Network (OTN).

---

---

**Note:** For more information about JDK version requirements, see the "Oracle WebLogic Server and JDK Considerations" topic in the *Oracle Fusion Middleware System Requirements and Specifications for Oracle Identity and Access Management 11g Release 2 (11.1.2)* document.

---

---

3. Review the Oracle Identity Manager customizations that are lost or overwritten as part of the upgrade process.

For more information, see [Section 10.2.4, "Reviewing the Customizations that are Lost or Overwritten as Part of Upgrade"](#).

4. Generate the pre-upgrade report for Oracle Identity Manager by running the pre-upgrade utility, and analyze all the reports generated. The pre-upgrade report utility analyzes your existing Oracle Identity Manager environment, and provides information about the mandatory prerequisites that you must complete before you upgrade the existing Oracle Identity Manager environment.

For information about generating and analyzing the pre-upgrade report for Oracle Identity Manager, see [Section 24.2.2, "Generating and Analyzing Pre-Upgrade Report for Oracle Identity Manager"](#).

5. Stop all the servers on `IDMHOST1` and `IDMHOST2` in the following order:
  - a. Stop the Oracle Adaptive Access Manager Managed Server(s) on `IDMHOST1` and `IDMHOST2`.
  - b. Stop the Access Manager Managed Server(s) on `IDMHOST1` and `IDMHOST2`.
  - c. Stop the Oracle Identity Manager Managed Server(s) on `IDMHOST1` and `IDMHOST2`.
  - d. Stop the Oracle SOA Suite Managed Server(s) on `IDMHOST1` and `IDMHOST2`.
  - e. Stop the WebLogic Administration Server on `IDMHOST1`.
6. Back up your existing environment after stopping the servers. To do this, complete the following steps:
  - a. Back up the `MW_HOME` directory including the Oracle Home directories inside Middleware home on both `IDMHOST1` and `IDMHOST2`.
  - b. Back up the Access Manager Domain Home directory which also contains Oracle Adaptive Access Manager, on both `IDMHOST1` and `IDMHOST2`.
  - c. Back up the Oracle Identity Manager Domain Home directory on both `IDMHOST1` and `IDMHOST2`.
  - d. Back up the following database schemas:
    - Oracle Access Manager schema
    - Oracle Identity Manager schema
    - Oracle Adaptive Access Manager schema
    - Oracle Platform Security Services schema
    - MDS schema
    - ORASDPM schema
    - SOAINFRA schema
    - Audit schema

- IAU schema

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

## 23.6 Upgrading Oracle Home

You must upgrade Oracle SOA Suite to 11g Release 1 (11.1.1.9.0) on both `IDMHOST1` and `IDMHOST2`, as Oracle Identity Manager 11.1.2.3.0 is certified with Oracle SOA Suite 11.1.1.9.0. Also, you must update the binaries of Oracle Identity Manager, Oracle Access Management Access Manager, and Oracle Adaptive Access Manager to 11g Release 2 (11.1.2.3.0) on both `IDMHOST1` and `IDMHOST2`. To do this, complete the following steps:

1. Upgrade Oracle WebLogic Server to 10.3.6 on both `IDMHOST1` and `IDMHOST2`, if you are using an earlier version. This involves running the Oracle WebLogic Server 10.3.6 upgrade installer to upgrade the existing Oracle WebLogic Server.

---

---

**Note:** If you are already using Oracle WebLogic Server 10.3.6, ensure that you apply the mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server 10.3.6, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

---

---

For more information about upgrading Oracle WebLogic Server to 10.3.6, see [Section 24.1.5, "Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)"](#).

2. Upgrade Oracle SOA Suite to 11g Release 1 (11.1.1.9.0). This involves running the Oracle SOA Suite 11.1.1.9.0 installer to update the binaries on `IDMHOST1` and `IDMHOST2`, and performing required post-patching tasks for Oracle SOA Suite.

For more information about upgrading Oracle SOA Suite, see [Section 24.2.3, "Upgrading Oracle SOA Suite to 11g Release 1 \(11.1.1.9.0\)"](#).

3. Update the binaries of Oracle Identity Manager, Oracle Access Management Access Manager, and Oracle Adaptive Access Manager to 11g Release 2 (11.1.2.3.0) by running the Oracle Identity and Access Management 11.1.2.3.0 Oracle Universal Installer.

For more information about upgrading the Oracle Identity and Access Management binaries, see [Section 24.1.6, "Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)"](#).

## 23.7 Creating Necessary Schemas and Upgrading the Existing Schemas

In order to upgrade to Oracle Identity and Access Management 11.1.2.3.0, you must upgrade the existing database schemas before you upgrade the domain. Also, it is recommended that you create the new Oracle Mobile Security Manager (OMSM) schema to enable the new feature of Oracle Access Management - Oracle Mobile Security Services. You must also create Oracle BI Publisher schema to enable the embedded BIP feature available in Oracle Identity Manager 11.1.2.3.0.

To create new schemas, you must run the Repository Creation Utility (RCU) 11.1.1.9.0, and to upgrade the existing schemas, you must run the Patch Set Assistant (PSA). To do this, complete the following steps on `IDMHOST1`:

1. Create the following schemas by running the Repository Creation Utility 11.1.1.9.0:
  - Oracle BI Publisher (BIP) schema
  - Oracle Mobile Security Manager (OMSM) Schema

For information about running the RCU to create new schemas, see [Section 24.1.3, "Creating Database Schemas Using Repository Creation Utility"](#).

2. Upgrade the following database schemas by running the Patch Set Assistant:
  - Oracle Access Manager schema
  - Oracle Identity Manager schema
  - Oracle Adaptive Access Manager schema
  - Oracle Platform Security Services schema
  - MDS schema
  - ORASDPM schema
  - SOAINFRA schema
  - Audit schema
  - IAU schema

For more information about upgrading schemas, see [Section 24.1.4, "Upgrading Schemas Using Patch Set Assistant"](#).

## 23.8 Upgrading Oracle Identity Manager Domain

To upgrade the Oracle Identity Manager domain, complete the following steps:

1. If you are using Windows 64-bit machine, perform the additional tasks described in [Section 24.2.4.1, "Additional Task for Windows 64-Bit Users Before Upgrading Middle Tier"](#) on `IDMHOST1` before proceeding with the middle tier upgrade.
2. If you are upgrading an SSL enabled middleware, that is, if you would be specifying SSL ports for WebLogic Administration Server and SOA Managed Servers during middle tier upgrade, you must create a truststore that contains the public certificates for all SSL enabled servers (which can be WebLogic Administration Server, SOA Managed Servers, OIM Managed Servers) irrespective of the node on which the server is running. This truststore will be used a client side store by the upgrade script to communicate with various servers during upgrade.

For information about creating a truststore, see [Section 24.2.4.2, "Creating a Truststore for Upgrading SSL Enabled Middleware"](#).

3. Update the `oim_upgrade_input.properties` file located at `OIM_HOME/server/bin/` on `IDMHOST1`, with the values for the properties required for Oracle Identity Manager middle tier upgrade.

For information about the properties that you must update in the `oim_upgrade_input.properties` file, see [Section 24.2.4.3, "Updating the Properties File"](#).

4. Performing the Oracle Identity Manager middle tier upgrade offline on `IDMHOST1`. This is done by running `OIMUpgrade` offline utility.

For more information about performing Oracle Identity Manager middle tier upgrade offline, see [Section 24.2.4.4, "Performing Oracle Identity Manager Middle Tier Upgrade Offline"](#).

5. Replicate the domain configuration on `IDMHOST2` by packing the Oracle Identity Manager domain on `IDMHOST1` and unpacking it on `IDMHOST2`.

For more information about replicating the domain configuration using `pack` and `unpack` commands, see [Section 20.7, "Replicating Domain Configuration on OIMHOST2"](#).

6. Start the WebLogic Administration Server and SOA Managed Server(s) on both `IDMHOST1` and `IDMHOST2`. Make sure that you do not start the Oracle Identity Manager Managed Server(s).

For information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

7. Performing the Oracle Identity Manager middle tier upgrade online on `IDMHOST1`. This is done by running `OIMUpgrade` online utility. When you perform this step, ensure that the Administration Server for Oracle Access Manager is up and running.

For more information about performing Oracle Identity Manager middle tier upgrade online, see [Section 24.2.4.6, "Performing Oracle Identity Manager Middle Tier Upgrade Online"](#).

8. Start the Oracle Identity Manager Managed Server(s) and Oracle BI Publisher Server on `IDMHOST1` and `IDMHOST2`.

For more information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

9. If you wish to scale out Oracle BI Publisher, you can do so by creating a new BIP Server on `IDMHOST2`, setting the location of the shared BI Publisher configuration folder, setting the scheduler configuration options, and configuring JMS for BI Publisher. This step is optional.

For more information about scaling out Oracle BI Publisher, see [Section 20.9, "Scaling out Oracle BI Publisher"](#).

10. Upgrade Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager to 11.1.2.3.0 on `IDMHOST1`.

For more information, see [Section 24.2.5, "Upgrading Other Oracle Identity Manager Installed Components"](#).

11. Complete the necessary Oracle Identity Manager post-upgrade steps described in [Section 24.2.6, "Performing Oracle Identity Manager Post-Upgrade Tasks"](#).

---

**Note:** The section [Section 24.2.6, "Performing Oracle Identity Manager Post-Upgrade Tasks"](#) contains the post-upgrade tasks for various Oracle Identity Manager starting points. You must perform only those tasks that are applicable to your starting point and your environment.

---

12. If you do not plan to upgrade Oracle Access Management domain to 11.1.2.3.0, then you must manually create the resources `/soa/**` and `/xmlpserver/**` with protection level `EXCLUDED` under the IAM Suite Application domain.

---



---

**Note:** If you plan to upgrade Oracle Access Management domain to 11.1.2.3.0, post-OIM upgrade, skip this step.

---



---

To manually create the resources `/soa/**` and `/xmlpserver/**` with protection level `EXCLUDED`, complete the following steps:

- a. Log in to the Oracle Access Management console using the following URL:

`http://WLS_Admin_Host:WLS_Admin_Port/oamconsole`

- b. Click **Application Domains**.
- c. Search for **IAM Suite** and open IAM Suite Application Domain.
- d. Click **Resources**, and then click **New Resource**.
- e. Specify the following details for creating `/soa/**` resource:

**Select Type:** HTTP

**Host Identifier:** IAMSUiteAgent

**Resource URL:** `/soa/**`

**Protection Level:** Excluded

Click **Apply** to apply the changes.

- f. Specify the following details for creating `/xmlpserver/**` resource:

**Select Type:** HTTP

**Host Identifier:** IAMSUiteAgent

**Resource URL:** `/xmlpserver/**`

**Protection Level:** Excluded

Click **Apply** to apply the changes.

- g. Specify the following details for creating `/soa-infra/**` resource:

**Select Type:** HTTP

**Host Identifier:** IAMSUiteAgent

**Resource URL:** `/soa-infra/**`

**Protection Level:** Excluded

Click **Apply** to apply the changes.

## 23.9 Upgrading Oracle Access Management Domain Which Also Contains Oracle Adaptive Access Manager

To upgrade the Oracle Access Management domain, complete the following steps:

1. Stop the Oracle Access Management Access Manager Managed Servers on both `IDMHOST1` and `IDMHOST2`. Also, stop the WebLogic Administration Server on `IDMHOST1`.

For more information, see [Section 24.1.9, "Stopping the Servers"](#).

2. Upgrade Oracle Platform Security Services (OPSS) by running the WLST command `upgradeOpss()` on `IDMHOST1`. This is required to upgrade the

configuration and policy stores of Oracle Access Manager and Oracle Adaptive Access Manager to 11.1.2.3.0.

For more information, see [Section 24.1.7, "Upgrading Oracle Platform Security Services"](#).

3. Undeploy the coherence#3.7.1.1 library, as it is not shipped with Access Manager 11.1.2.3.0.

For information about undeploying coherence#3.7.1.1 library, see [Section 8.8, "Undeploying coherence#3.7.1.1 Library"](#).

4. Restart the WebLogic Administration Server and the Access Manager Managed Servers on `IDMHOST1` and `IDMHOST2`.
5. Upgrade the Oracle Access Management system configuration by running the `upgradeConfig()` command on `IDMHOST1`.

For more information, see [Section 8.10, "Upgrading System Configuration"](#).

6. Extend the Oracle Access Management domain to include Oracle Mobile Security Suite and Policy Manager. Using the functionality of Oracle Mobile Security Suite is optional. However, you must perform this step to enable the Policy Manager.

For more information, see [Section 24.3.1, "Extending the 11.1.2.3.0 Access Manager Domain to Include Mobile Security Suite and Policy Manager"](#).

---

---

**Note:** To start using the features of Oracle Mobile Security Suite, you must enable Oracle Mobile Security Suite as described in [Section 24.3.2, "Enabling Oracle Mobile Security Suite"](#).

---

---

7. Start the WebLogic Administration Server on `IDMHOST1`, and the Oracle Access Manager Managed Servers on both `IDMHOST1` and `IDMHOST2`. If you have configured Oracle Adaptive Access Manager, you must start the Oracle Adaptive Access Manager Managed Servers on both `IDMHOST1` and `IDMHOST2`.

For more information, see [Section 24.1.8, "Starting the Servers"](#).

8. Perform the required post-upgrade tasks for Oracle Access Management as described in [Performing the Required Post-Upgrade Tasks](#).
9. Redeploy the Oracle Adaptive Access Manager applications on Oracle Adaptive Access Manager 11.1.2.3.0 Server.

For more information, see [Section 9.10, "Redeploying Oracle Adaptive Access Manager Applications"](#).

## 23.10 Seeding the Oracle Identity Manager 11.1.2.3.0 Resources in Oracle Access Management

This step is required only if you upgraded Oracle Identity Manager domain before upgrading Oracle Access Management domain.

---

---

**Note:** If you upgraded Oracle Access Management domain prior to upgrading Oracle Identity Manager domain, skip this task.

---

---

If Oracle Identity Manager domain is upgraded first, then you must seed the Oracle Identity Manager 11.1.2.3.0 resources in Oracle Access Management, after upgrading

Oracle Access Management domain. To do this, you must run the `idmConfigTool -configOIM` command.

For information about running the `-configOIM` command, see "configOIM Command" in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

---

**Note:** ■ In the 11.1.2.3.0 property file for `-configOIM`, ensure that the value specified for the attribute `IDSTORE_WLSADMINUSER` is the user who has access to the Oracle Access Management console (`oamconsole`).

For example:

```
IDSTORE_WLSADMINUSER:oamAdminUser
```

- Ensure that the values specified for various attributes in the 11.1.2.3.0 property file for `-configOIM` is same as the values provided when you ran `-configOIM` in the base environment (11g Release 2 (11.1.2.1.0)).
- The following are the newly added properties for `-configOIM` property file in 11.1.2.3.0:

```
IDSTORE_WLSADMINUSER
```

```
OIM_MSM_REST_SERVER_URL
```

---

After you successfully run the `-configOIM` command, restart all the servers in `IDMDomain` and `OIMDomain` on both `IDMHOST1` and `IDMHOST2`.

## 23.11 Verifying the Upgraded Environment

Verify the upgraded environment by completing the following steps:

1. Verify the Oracle Identity Manager upgrade by completing the steps described in [Section 10.8, "Verifying the Oracle Identity Manager Upgrade"](#).
2. Verify the Oracle Access Management upgrade by completing the steps described in [Section 8.14, "Verifying the Oracle Access Management Upgrade"](#).
3. Verify the Oracle Adaptive Access Manager upgrade by completing the steps described in [Section 9.12, "Verifying the Oracle Adaptive Access Manager Upgrade"](#).

## 23.12 Troubleshooting

If you encounter any issue during upgrade, refer to the following sections:

- For issues and workaround specific to Oracle Identity Manager upgrade, see [Section 25.1, "Troubleshooting Oracle Identity Manager Upgrade Issues"](#).
- For issues and workaround specific to Oracle Access Management upgrade, see [Section 25.2, "Troubleshooting Oracle Access Management Upgrade Issues"](#).
- For the list of known issues related to upgrade, and their workaround, see "Upgrade and Migration Issues for Oracle Identity and Access Management" in the *Oracle Fusion Middleware Release Notes for Identity Management*.



# Part VI

---

## Common Upgrade Tasks and Troubleshooting

This part contains the following chapters:

- [Chapter 24, "Tasks Common to Various Manual Upgrade Scenarios"](#)
- [Chapter 25, "Troubleshooting Upgrade Issues"](#)



---

---

## Tasks Common to Various Manual Upgrade Scenarios

This chapter lists the tasks that are common to different upgrade scenarios.

---

---

**Note:** You do not have to perform all the tasks described in this chapter. Refer to the [Section 3.4, "Documentation Roadmap"](#) for the upgrade roadmap.

---

---

---

---

**Note:** In this chapter,

- 11.1.2.x.x refers to the versions 11g Release 2 (11.1.2.2.0), 11g Release 2 (11.1.2.1.0), and 11g Release 2 (11.1.2).
  - 11.1.1.x.x refers to the versions 11g Release 1 (11.1.1.7.0) and 11g Release 1 (11.1.1.5.0).
- 
- 

This chapter includes the following topics:

- [Section 24.1, "Generic Topics"](#)
- [Section 24.2, "Oracle Identity Manager Specific Topics"](#)
- [Section 24.3, "Oracle Access Management Specific Topics"](#)

### 24.1 Generic Topics

This section contains the generic tasks common to some of the Oracle Identity and Access Management components upgrade. This section includes the following topics:

- [Verifying Certification, System Requirements, and Interoperability](#)
- [Backing up the Existing Environment](#)
- [Creating Database Schemas Using Repository Creation Utility](#)
- [Upgrading Schemas Using Patch Set Assistant](#)
- [Upgrading Oracle WebLogic Server to 11g Release 1 \(10.3.6\)](#)
- [Updating Oracle Identity and Access Management Binaries to 11g Release 2 \(11.1.2.3.0\)](#)
- [Upgrading Oracle Platform Security Services](#)
- [Starting the Servers](#)

- [Stopping the Servers](#)

### 24.1.1 Verifying Certification, System Requirements, and Interoperability

The certification matrix and system requirements documents should be used in conjunction with each other to verify that your environment meets the necessary requirements for installation or upgrade.

#### Step 1 Verifying Your Environment Meets Certification Requirements

Make sure that you are installing your product on a supported hardware and software configuration. For more information, see the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page.

Oracle has tested and verified the performance of your product on all certified systems and environments; whenever new certifications occur, they are added to the proper certification document right away. New certifications can occur at any time, and for this reason the certification documents are kept outside of the documentation libraries and are available on Oracle Technology Network.

#### Step 2 Using the System Requirements Document to Verify Certification

The *Oracle Fusion Middleware System Requirements and Specifications* document should be used to verify that the requirements of the certification are met. For example, if the certification document indicates that your product is certified for installation on 64-Bit Oracle Linux 5, this document should be used to verify that your Oracle Linux 5 system has met the required minimum specifications, like disk space, available memory, specific platform packages and patches, and other operating system-specific items. System requirements can be updated at any time, and for this reason the system requirement documents are kept outside of the documentation libraries and are available on Oracle Technology Network.

#### Step 3 Verifying Interoperability Among Multiple Products

The *Oracle Fusion Middleware Interoperability and Compatibility Guide* for Oracle Identity and Access Management document defines interoperability, defines compatibility, and describes how multiple Fusion Middleware products from the same release or mixed releases may be used with each other. You should read this document if you are planning to install multiple Fusion Middleware products on your system.

### 24.1.2 Backing up the Existing Environment

To back up the existing environment, you must stop all the servers, and back up the following:

- *MW\_HOME* directory, including the Oracle Home directories inside Middleware Home
- Domain Home directory
- Database schemas

For more information about backing up schemas, see *Oracle Database Backup and Recovery User's Guide*.

### 24.1.3 Creating Database Schemas Using Repository Creation Utility

To create 11.1.2.3.0 Database schemas, you must use Repository Creation Utility (RCU) 11.1.1.9.0. When you create new schemas, do not delete your existing schemas, and do

not use the old schema name, as you will need the old schema credentials while exporting the Access Data.

To create the database schemas, perform the following tasks:

1. [Obtaining Repository Creation Utility](#)
2. [Starting Repository Creation Utility](#)
3. [Creating Schemas](#)

#### 24.1.3.1 Obtaining Repository Creation Utility

Download the Repository Creation Utility. For information about obtaining Repository Creation Utility, see "Obtaining RCU" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

#### 24.1.3.2 Starting Repository Creation Utility

Start the Repository Creation Utility from the location where you downloaded it. For information about starting Repository Creation Utility, see "Starting RCU" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

#### 24.1.3.3 Creating Schemas

Create the necessary schemas using Repository Creation Utility. For information about creating schemas, see "Creating Schemas" in the *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

### 24.1.4 Upgrading Schemas Using Patch Set Assistant

To upgrade the existing schemas to 11.1.2.3.0, you must use the Patch Set Assistant. To upgrade the database schemas, perform the following tasks:

- [Checking Your Database and Schemas](#)
- [Starting Patch Set Assistant](#)
- [Using the Patch Set Assistant Graphical Interface to Upgrade Schemas](#)
- [Verifying Schema Upgrade](#)

#### 24.1.4.1 Checking Your Database and Schemas

Before running Patch Set Assistant, you should make sure that your database is running and that the schemas are supported for upgrade. To check this, run the following SQL command:

```
SELECT OWNER, VERSION, STATUS, UPGRADED FROM SCHEMA_VERSION_REGISTRY;
```

[Table 24–1](#) lists the schemas and their versions supported for upgrade:

**Table 24–1 Schemas and Their Versions Supported for Upgrade**

Schema Name	Schema Version(s) Supported for Upgrade
Oracle Access Manager (OAM)	11.1.1.3.0
	11.1.2.1.0
	11.1.2.2.0
Oracle Adaptive Access Manager (OAAM)	11.1.1.3.0
	11.1.2.0.0

**Table 24–1 (Cont.) Schemas and Their Versions Supported for Upgrade**

Schema Name	Schema Version(s) Supported for Upgrade
Oracle Identity Manager (OIM)	11.1.1.5.0
	11.1.1.7.0
	11.1.2.0.0
	11.1.2.1.0
	11.1.2.2.0
Oracle Privileged Account Manager (OPAM)	11.1.2.0.0
	11.1.2.1.0
Oracle Platform Security Services (OPSS)	11.1.1.6.0
	11.1.1.7.2
Oracle Audit Services (IAU)	11.1.1.6.0
	11.1.1.7.0

#### 24.1.4.2 Starting Patch Set Assistant

To start Patch Set Assistant, do the following:

##### On UNIX:

1. Move from your present working directory to the <MW\_HOME>/oracle\_common/bin directory by running the following command on the command line:

```
cd <MW_HOME>/oracle_common/bin
```

2. Run the following command:

```
./psa
```

##### On Windows:

1. Move from your present working directory to the <MW\_HOME>\oracle\_common\bin directory by running the following command on the command line:

```
cd <MW_HOME>\oracle_common\bin
```

2. Execute the following command:

```
psa.bat
```

#### 24.1.4.3 Using the Patch Set Assistant Graphical Interface to Upgrade Schemas

After starting the Patch Set Assistant Installer, follow the instructions on the screen to update your schemas.

Follow the instructions in [Table 24–2](#) to update your schemas:

**Table 24–2 Patch Set Assistant Screens**

Screen	Description
Welcome	This page introduces you to the Patch Set Assistant.
Select Component	Select the component you wish to upgrade.
Prerequisite	Verify that you have satisfied the database prerequisites.

**Table 24–2 (Cont.) Patch Set Assistant Screens**

Screen	Description
Schema	Specify your database credentials to connect to your database, then select the schema you want to update.  Note that this screen appears once for each schema that must be updated as a result of the component you selected on the Select Component screen.
Examine	This page displays the status of the Patch Set Assistant as it examines each component schema. Verify that your schemas have a "successful" indicator in the Status column.
Upgrade Summary	Verify that the schemas are the ones you want to upgrade.
Upgrade Progress	This screen shows the progress of the schema upgrade.
Upgrade Success	Once the upgrade is successful, you get this screen.

#### 24.1.4.4 Verifying Schema Upgrade

You can verify the schema upgrade by checking out the log files. The Patch Set Assistant writes log files in the following locations:

##### On UNIX:

```
<MW_HOME>/oracle_common/upgrade/logs/psa/psatimestamp.log
```

##### On Windows:

```
<MW_HOME>\oracle_common\upgrade\logs\psa\psatimestamp.log
```

Some components create a second log file named `psatimestamp.out` in the same location.

The `timestamp` reflects the actual date and time when Patch Set Assistant was run.

If any failures occur when running Patch Set Assistant, you can use these log files to help diagnose and correct the problem. Do not delete them. You can alter the contents of the log files by specifying a different `-logLevel` from the command line.

Some of the operations performed by Patch Set Assistant may take longer to complete than others. If you want to see the progress of these long operations, you can see this information in the log file, or you can use the following query:

```
SELECT VERSION, STATUS, UPGRADED FROM SCHEMA_VERSION_REGISTRY WHERE  
OWNER = 'schema_name';
```

In the query results, the `STATUS` field is either `UPGRADING` or `UPGRADED` during the schema patching operation, and becomes `VALID` when the operation is completed.

### 24.1.5 Upgrading Oracle WebLogic Server to 11g Release 1 (10.3.6)

To upgrade Oracle WebLogic Server to 11g Release 1 (10.3.6), complete the following steps:

1. Download the WebLogic 10.3.6 Upgrade Installer from Oracle Technology Network.

For more information, see "Downloading an Upgrade Installer From My Oracle Support" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

2. Run the Upgrade Installer in graphical mode to upgrade your WebLogic Server.

For more information, see "Running the Upgrade Installer in Graphical Mode" in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*.

---

---

**Note:** After you upgrade Oracle WebLogic Server to 10.3.6, you must apply some mandatory patches to fix specific issues with Oracle WebLogic Server 10.3.6.

To identify the required patches that you must apply for Oracle WebLogic Server, see "Downloading and Applying Required Patches" in the *Oracle Fusion Middleware Infrastructure Release Notes*.

The patches listed in the release notes are available from My Oracle Support. The patching instructions are mentioned in the `README.txt` file that is provided with each patch.

---

---

## 24.1.6 Updating Oracle Identity and Access Management Binaries to 11g Release 2 (11.1.2.3.0)

To update the existing Oracle Identity and Access Management binaries to 11.1.2.3.0, you must use the Oracle Identity and Access Management 11.1.2.3.0 installer. To do this, perform the following tasks:

- [Obtaining the Software](#)
- [Starting the Oracle Identity and Access Management 11g Release 2 \(11.1.2.3.0\) Installer](#)
- [Installing Oracle Identity and Access Management 11g Release 2 \(11.1.2.3.0\)](#)

### 24.1.6.1 Obtaining the Software

For more information on obtaining Oracle Fusion Middleware 11g software, see *Oracle Fusion Middleware Download, Installation, and Configuration ReadMe*.

### 24.1.6.2 Starting the Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0) Installer

This topic explains how to start the Oracle Identity and Access Management Installer.

---

---

**Notes:**

- If you are installing on an IBM AIX operating system, you must run the `rootpre.sh` script from the `Disk1` directory before you start the Installer.
  - Starting the Installer as the `root` user is not supported.
- 
- 

Start the Installer by doing the following:

**On UNIX:**

1. Move from your present working directory to the directory where you extracted the contents of the Installer to.
2. Move to the following location:  

```
cd Disk1
```
3. Run the following command:

```
./runInstaller -jreLoc <full path to the JRE directory>
```

For example:

```
./runInstaller -jreLoc <MW_HOME>/jdk160_29/jre
```

#### On Windows:

1. Move from your present working directory to the directory where you extracted the contents of the Installer to.
2. Move to the following location:

```
cd Disk1
```

3. Run the following command:

```
setup.exe -jreLoc <full path to the JRE directory>
```

For Example:

```
setup.exe -jreLoc <MW_HOME>\jdk160_29\jre
```

---

**Note:** If you do not specify the `-jreLoc` option on the command line when using the Oracle JRockit JDK, the following warning message is displayed:

```
-XX:MaxPermSize=512m is not a valid VM option. Ignoring
```

This warning message does not affect the installation. You can continue with the installation.

On 64-bit platforms, when you install Oracle WebLogic Server using the generic jar file, the `jrockit_1.6.0_29` directory is not created in your Middleware Home. You must enter the absolute path to the JRE folder from where your JDK is located.

---

### 24.1.6.3 Installing Oracle Identity and Access Management 11g Release 2 (11.1.2.3.0)

Use the Oracle Identity and Access Management 11.1.2.3.0 Installer to upgrade existing Oracle Identity and Access Management binaries to 11.1.2.3.0:

1. After you start the Installer, the **Welcome** screen appears.
2. Click **Next** on the **Welcome** screen. The **Install Software Updates** screen appears. Select whether or not you want to search for updates. Click **Next**.
3. The **Prerequisite Checks** screen appears. If all prerequisite checks pass inspection, click **Next**. The **Specify Installation Location** screen appears.
4. On the **Specify Installation Location** screen, point to the Middleware Home to your existing Middleware Home installed on your system.
5. In the **Oracle Home Directory** field, specify the path of the existing Oracle Identity and Access Management Home. This directory is also referred to as `<IAM_HOME>` in this book.

Click **Next**. The **Installation Summary** screen appears.

6. The **Installation Summary** screen displays a summary of the choices that you made. Review this summary and decide whether you want to proceed with the installation. If you want to modify any of the configuration settings at this stage, select a topic in the left navigation page and modify your choices. To continue

installing Oracle Identity and Access Management, click **Install**. The **Installation Progress** screen appears.

7. Monitor the progress of your installation. The location of the installation log file is listed for reference. After the installation progress reaches 100%, click **OK**. If you encounter any issue, check the log file. For information about locating the log files, see "Locating Installation Log Files" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

---

**Note:** If you cancel or abort when the installation is in progress, you must manually delete the <IAM\_HOME> directory before you can reinstall the Oracle Identity and Access Management software.

To invoke online help at any stage of the installation process, click **Help** on the installation wizard screens.

---

8. The **Installation Complete** screen appears. On the **Installation Complete** screen, click **Finish**.

This installation process copies the 11.1.2.3.0 Oracle Identity and Access Management software to your system.

For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2.3.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 24.1.7 Upgrading Oracle Platform Security Services

This section describes how to upgrade Oracle Platform Security Services (OPSS).

Upgrading Oracle Platform Security Services is required to upgrade the configuration and policy stores to 11.1.2.3.0. It upgrades the `jps-config.xml` file and policy stores.

To upgrade Oracle Platform Security Services for LDAP- or DB-based store, complete the following steps:

1. Run the following command from the location `MW_HOME/oracle_common/common/bin` to launch the WebLogic Scripting Tool (WLST):

**On UNIX:**

```
./wlst.sh
```

**On Windows:**

```
wlst.cmd
```

2. Run the following command to upgrade OPSS:

```
upgradeOpss(jpsConfig=<absolute_path_to_old_version_jps-config.xml_file>,"
  jaznData=<absolute_path_to_new_version_OOTB_JAZN_data_file>,"
  auditStore=<absolute_path_to_OOTB_audit-store.xml_file>,"
  jdbcDriver=<jdbc_driver>,"
  url=<jdbc_ldap_url>,"
  user=<jdbc_ldap_user>,"
  password=<jdbc_ldap_password>"],
  upgradeJseStoreType="true/false"])
```

[Table 24–3](#) describes the arguments of the `upgradeOpss` command:

**Table 24–3 Arguments to be Specified While Running upgradeOpss command**

Argument	When to Use?	Mandatory/Optional	Description
jpsConfig	Use this argument if you are upgrading Oracle Identity and Access Management 11g Release 1 (11.1.1.x.x) or 11g Release 2 (11.1.2.x.x) to 11g Release 2 (11.1.2.3.0).	This argument is mandatory for both DB-based and LDAP-based store.	Specify the absolute path to the <code>jps-config.xml</code> domain configuration file.  The <code>upgradeOpss</code> script backs up the <code>jps-config.xml</code> file in the same directory as a file with the suffix <code>.bak</code> appended to the its name.  The <code>jps-config.xml</code> file is typically located in the directory <code>\$DOMAIN_HOME/config/fmwconfig</code> . The file <code>jps-config-jse.xml</code> is assumed to be located in the same directory.
jaznData	Use this argument if you are upgrading Oracle Identity and Access Management 11g Release 1 (11.1.1.x.x) or 11g Release 2 (11.1.2.x.x) to 11g Release 2 (11.1.2.3.0).	This argument is mandatory for both DB-based and LDAP-based store.	Specify the absolute path to the location of out-of-the-box <code>system-jazn-data.xml</code> file.  The <code>system-jazn-data.xml</code> file is typically located in the directory <code>\$oracle_common/modules/oracle.jps_11.1.1/domain_config</code> .
auditStore	Use this argument if you are upgrading Oracle Identity and Access Management 11g Release 2 (11.1.2.x.x) to 11g Release 2 (11.1.2.3.0).	This argument is optional for both DB-based and LDAP-based store.	Specify the absolute path to the location of 11.1.2.x.x out-of-the-box <code>audit-store.xml</code> file.  If unspecified, it defaults to the file <code>audit-store.xml</code> located in the directory specified for the argument <code>jaznData</code> .
jdbcDriver	Use this argument if you are upgrading Oracle Identity and Access Management 11g Release 2 (11.1.2.x.x) to 11g Release 2 (11.1.2.3.0).	This argument is required only in case of DB-based store.	Specify the JDBC driver to the store.  For example: <code>oracle.jdbc.OracleDriver</code>

**Table 24–3 (Cont.) Arguments to be Specified While Running upgradeOpss command**

Argument	When to Use?	Mandatory/Optional	Description
url	Use this argument if you are upgrading Oracle Identity and Access Management 11g Release 2 (11.1.2.x.x) to 11g Release 2 (11.1.2.3.0).	This argument is mandatory for both DB-based and LDAP-based store.	Specify the JDBC URL or the LDAP URL for this parameter. The following are the formats of the JDBC URL: <ul style="list-style-type: none"> <li>■ <code>driverType:@host:port/serviceName</code></li> <li>■ <code>driverType:@host:port:SID</code></li> </ul> The following is the format of the LDAP URL: <code>ldap://host:port</code> The LDAP URL must be used only if LDAP-based Policy Store is configured in your environment. If this property is unspecified, the JDBC URL or LDAP URL is read from the configuration file.
user	Use this argument if you are upgrading Oracle Identity and Access Management 11g Release 2 (11.1.2.x.x) to 11g Release 2 (11.1.2.3.0).	This argument is mandatory in case of DB-based store, whereas it is optional for LDAP-based store.	Specify the name of the Oracle Platform Security Services (OPSS) schema. For example: <code>DEV_OPSS</code>
password	Use this argument if you are upgrading Oracle Identity and Access Management 11g Release 2 (11.1.2.x.x) to 11g Release 2 (11.1.2.3.0).	This argument is mandatory in case of DB-based store, whereas it is optional for LDAP-based store.	Specify the password of the Oracle Platform Security Services (OPSS) schema.
upgradeJseStoreType	Use this argument if you are upgrading Oracle Identity and Access Management 11g Release 2 (11.1.2.x.x) to 11g Release 2 (11.1.2.3.0).	This argument is optional for both LDAP-based and DB-based store.	Specify true if you wish to upgrade JSE Store Type, which will in turn update the <code>jps-config-jse.xml</code> . The default value is false.

For example:

On UNIX:

```
upgradeOpss (jpsConfig="/Oracle/Middleware/user_projects/domains/oes_
domain/config/fmwconfig/jps-config.xml",
jaznData="/oracle/middleware/oracle_common/modules/oracle.jps_11.1.1/domain_
config/system-jazn-data.xml",
```

```
jdbcDriver="oracle.jdbc.OracleDriver",
url="jdbc:oracle:thin:@host:1234:db123",
user="R2_OPSS",
password="password123",
upgradeJseStoreType="true")
```

On Windows:

```
upgradeOpss(jpsConfig="C:\\Oracle\\Middleware\\user_projects\\domains\\oes_
domain\\config\\fmwconfig\\jps-config.xml",
jaznData="C:\\oracle\\middleware\\oracle_common\\modules\\oracle.jps_
11.1.1\\domain_config\\system-jazn-data.xml",
jdbcDriver="oracle.jdbc.OracleDriver",
url="jdbc:oracle:thin:@host:1234/db123",
user="R2_OPSS",
password="password123",
upgradeJseStoreType="true")
```

## 24.1.8 Starting the Servers

To start the WebLogic Administration Server and the Managed Server(s), refer to the following sections:

- [Starting the Node Manager](#)
- [Starting the WebLogic Administration Server](#)
- [Starting the Managed Server\(s\)](#)

---

**Note:** You must start the Node Manager, the WebLogic Administration Server, and the Managed Servers with Java Secure Socket Extension (JSSE) enabled, if you have applied the following Oracle WebLogic Server patches to your Middleware home:

- 13964737 (YVDZ)
- 14174803 (IMWL)

These patches are available from My Oracle Support.

For information on how to start the Node Manager with JSSE enabled, see the "Set the Node Manager Environment Variables" topic in the *Oracle Fusion Middleware Administering the Node Manager for Oracle WebLogic Server*.

After starting Node Manager with JSSE enabled, you must start the Administration Server and Managed Servers with JSSE enabled. For more information, see the "Using the JSSE-Enabled SSL Implementation" topic in *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.

---

### 24.1.8.1 Starting the Node Manager

To start the Node Manager, you must run the command `startNodeManager.sh` (on UNIX) or `startNodeManager.cmd` (on Windows) from the location `$WL_HOME/server/bin`.

For more information, see "startNodeManager" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

### 24.1.8.2 Starting the WebLogic Administration Server

To start the WebLogic Administration Server, do the following:

#### On UNIX:

Run the following commands:

```
cd MW_HOME/user_projects/domains/domain_name/bin
./startWebLogic.sh
```

#### On Windows:

Run the following commands:

```
cd MW_HOME\user_projects\domains\domain_name\bin
startWebLogic.cmd
```

### 24.1.8.3 Starting the Managed Server(s)

To start the Managed Server(s), do the following:

#### On UNIX:

1. Move from your present working directory to the *MW\_HOME*/user\_projects/domains/*domain\_name*/bin directory by running the following command on the command line:

```
cd MW_HOME/user_projects/domains/domain_name/bin
```

2. Run the following command to start the Managed Servers:

```
./startManagedWebLogic.sh managed_server_name admin_url admin_username password
```

where

*managed\_server\_name* is the name of the Managed Server

*admin\_url* is URL of the administration console. Specify it in the format `http://host:port/console`. Specify only if the WebLogic Administration Server is on a different computer.

*admin\_username* is the username of the WebLogic Administration Server.

*password* is the password of the WebLogic Administration Server.

For example:

```
./startManagedWebLogic.sh oim_server1 http://host.example.com:7001/console
weblogic password123
```

#### On Windows:

1. Move from your present working directory to the *MW\_HOME*\user\_projects\domains\*domain\_name*\bin directory by running the following command on the command line:

```
cd MW_HOME\user_projects\domains\domain_name\bin
```

2. Run the following command to start the Managed Servers:

```
startManagedWebLogic.cmd managed_server_name admin_url admin_username password
```

where

*managed\_server\_name* is the name of the Managed Server.

*admin\_url* is URL of the administration console. Specify it in the format `http://host:port/console`. Specify only if the WebLogic Administration Server is on a different computer.

*admin\_username* is the username of the WebLogic Administration Server.

*password* is the password of the WebLogic Administration Server.

For example:

```
startManagedWebLogic.cmd oim_server1 http://host.example.com:7001/console
weblogic password123
```

For more information, see "Starting the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

## 24.1.9 Stopping the Servers

To stop the WebLogic Administration Server and the Managed Server(s), refer to the following sections:

- [Stopping the Managed Server\(s\)](#)
- [Stopping the WebLogic Administration Server](#)
- [Stopping the Node Manager](#)

You must stop the Managed Server(s) first, and then the WebLogic Administration Server.

### 24.1.9.1 Stopping the Managed Server(s)

To stop the Managed Server(s), do the following:

**On UNIX:**

1. Move from your present working directory to the `MW_HOME/user_projects/domains/domain_name/bin` directory by running the following command on the command line:

```
cd MW_HOME/user_projects/domains/domain_name/bin
```

2. Run the following command to stop the servers:

```
./stopManagedWebLogic.sh managed_server_name admin_url admin_username
password
```

where

*managed\_server\_name* is the name of the Managed Server.

*admin\_url* is URL of the WebLogic administration console. Specify it in the format `http://host:port/console`. Specify only if the WebLogic Administration Server is on a different computer.

*admin\_username* is the username of the WebLogic Administration Server.

*password* is the password of the WebLogic Administration Server.

For example:

```
./stopManagedWebLogic.sh oim_server1 http://host.example.com:7001/console
weblogic password123
```

**On Windows:**

1. Move from your present working directory to the `MW_HOME\user_projects\domains\domain_name\bin` directory by running the following command on the command line:

```
cd MW_HOME\user_projects\domains\domain_name\bin
```

2. Run the following command to stop the Managed Servers:

```
stopManagedWebLogic.cmd managed_server_name admin_url admin_username  
password
```

where

`managed_server_name` is the name of the Managed Server.

`admin_url` is URL of the WebLogic administration console. Specify it in the format `http://host:port/console`. specify only if the WebLogic Administration Server is on a different computer.

`admin_username` is the username of the WebLogic Administration Server.

`password` is the password of the WebLogic Administration Server.

For example:

```
stopManagedWebLogic.cmd oim_server1 http://host.example.com:7001/console  
weblogic password123
```

For more information, see "Stopping the Stack" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

### 24.1.9.2 Stopping the WebLogic Administration Server

To stop the WebLogic Administration Server, do the following:

**On UNIX:**

Run the following commands:

```
cd MW_HOME/user_projects/domains/domain_name/bin  
./stopWebLogic.sh
```

**On Windows:**

Run the following commands:

```
cd MW_HOME\user_projects\domains\domain_name\bin  
stopWebLogic.cmd
```

### 24.1.9.3 Stopping the Node Manager

To stop the Node Manager, close the command shell in which it is running.

Alternatively, after having set the attribute `QuitEnabled` to `true` (the default is `false`) in `nodemanager.properties` file, you can use `WLST` command to connect to the Node Manager and shut it down. For more information, see "stopNodeManager" in the *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

## 24.2 Oracle Identity Manager Specific Topics

This section includes the topics common to various Oracle Identity Manager upgrade starting points. This section contains the following topics:

- [Protected Metadata Files for Which Customization will be Retained After Upgrade](#)

- [Generating and Analyzing Pre-Upgrade Report for Oracle Identity Manager](#)
- [Upgrading Oracle SOA Suite to 11g Release 1 \(11.1.1.9.0\)](#)
- [Upgrading Oracle Identity Manager Middle Tier](#)
- [Upgrading Other Oracle Identity Manager Installed Components](#)
- [Performing Oracle Identity Manager Post-Upgrade Tasks](#)

### 24.2.1 Protected Metadata Files for Which Customization will be Retained After Upgrade

If you had done any customization to the unprotected metadata files pre-upgrade, the customization will be lost after you upgrade to Oracle Identity Manager 11.1.2.3.0.

Customization done to the following protected metadata files are retained after upgrade:

- /file/User.xml
- /db/identity/entity-definition/RoleUserMembership.xml
- /db/identity/entity-definition/RoleCategory.xml
- /db/identity/entity-definition/OIMRoleGrantRelationProvider.xml
- /db/identity/entity-definition/Role.xml
- /db/identity/entity-definition/OIMRoleDataProvider.xml
- /db/identity/entity-definition/RoleRoleRelationship.xml
- /db/identity/entity-definition/OIMRoleCategoryDataProvider.xml
- /db/identity/entity-definition/OIMRoleRelationshipRelationProvider.xml
- /db/identity/entity-definition/OIMOrgDataProvider.xml
- /db/identity/entity-definition/UserDataProvider.xml
- /db/identity/entity-definition/Organization.xml
- /file/RECON\_USER\_OLDSTATE.xml
- /db/task.xml
- /metadata/iam-features-requestactions/model-data/SelfCreateUserDataset.xml
- /metadata/iam-features-requestactions/model-data/CreateRoleDataSet.xml
- /metadata/iam-features-requestactions/model-data/ModifyUserDataset.xml
- /metadata/iam-features-requestactions/model-data/CreateUserDataSet.xml
- /metadata/iam-features-requestactions/model-data/DisableUserDataset.xml
- /metadata/iam-features-requestactions/model-data/ModifyRoleDataSet.xml
- /metadata/iam-features-requestactions/model-data/DeleteUserDataset.xml
- /metadata/iam-features-requestactions/model-data/AssignRolesDataset.xml
- /metadata/iam-features-requestactions/model-data/RemoveRolesDataset.xml
- /metadata/iam-features-requestactions/model-data/EnableUserDataset.xml
- /metadata/iam-features-requestactions/model-data/DeleteRoleDataSet.xml

- /metadata/iam-features-requestactions/model-data/ResourceCommonDataset.xml  
1
- /metadata/iam-features-sil/db/Registration.xml
- /metadata/iam-features-sil/db/SILConfig.xml
- /metadata/iam-features-callbacks/event\_configuration/EventHandlers.xml
- /metadata/iam-features-tasklist/EventHandlers.xml
- /metadata/iam-features-transUI/EventHandlers.xml
- /metadata/iam-features-reconciliation/event-definition/EventHandlers.xml
- /metadata/iam-features-asyncwsclient/EventHandlers.xml
- /metadata/iam-features-OIMMigration/EventHandlers.xml
- /metadata/iam-features-accesspolicy/event-definition/EventHandlers.xml
- /metadata/iam-features-request/event-definition/EventHandlers.xml
- /metadata/iam-features-system-configuration/EventHandlers.xml
- /metadata/iam-features-templatefeature/EventHandlers.xml
- /metadata/iam-features-passwordmgmt/event-definition/EventHandlers.xml
- /metadata/iam-features-sod/EventHandlers.xml
- /metadata/iam-features-notification/EventHandlers.xml
- /metadata/iam-features-Scheduler/EventHandlers.xml
- /metadata/iam-features-autoroles/event-definition/EventHandlers.xml
- /metadata/iam-features-identity/event-definition/EventHandlers.xml
- /metadata/iam-features-selfservice/event-definition/EventHandlers.xml
- /metadata/iam-features-selfservice/event-definition/EventHandlers.xml
- /metadata/iam-features-requestactions/event-definition/EventHandlers.xml
- /metadata/iam-features-configservice/event-definition/EventHandlers.xml
- /db/GTC/ProviderDefinitions/IsValidDateValidatorProvider.xml
- /db/GTC/ProviderDefinitions/IsIntValidatorProvider.xml
- /db/GTC/ProviderDefinitions/IsShortValidatorProvider.xml
- /db/GTC/ProviderDefinitions/IsFloatValidatorProvider.xml
- /db/GTC/ProviderDefinitions/OnetoOne.xml
- /db/GTC/ProviderDefinitions/WSProvisioningTransport.xml
- /db/GTC/ProviderDefinitions/CSVReconFormat.xml
- /db/GTC/ProviderDefinitions/SharedDriveReconTransport.xml
- /db/GTC/ProviderDefinitions/MaxLengthValidatorProvider.xml
- /db/GTC/ProviderDefinitions/SPMLProvisioningFormat.xml
- /db/GTC/ProviderDefinitions/IsLongValidatorProvider.xml
- /db/GTC/ProviderDefinitions/Concatenation.xml
- /db/GTC/ProviderDefinitions/IsDoubleValidatorProvider.xml

- /db/GTC/ProviderDefinitions/IsByteValidatorProvider.xml
- /db/GTC/ProviderDefinitions/ValidateDateFormat.xml
- /db/GTC/ProviderDefinitions/MatchRegexpValidatorProvider.xml
- /db/GTC/ProviderDefinitions/MinLengthValidatorProvider.xml
- /db/GTC/ProviderDefinitions/IsInRangeValidatorProvider.xml
- /db/GTC/ProviderDefinitions/IsBlankOrNullValidatorProvider.xml
- /db/GTC/ProviderDefinitions/Translation.xml
- /metadata/iam-features-ldap-sync/LDAPRoleMembership.xml
- /metadata/iam-features-ldap-sync/LDAPUserMembership.xml
- /metadata/iam-features-ldap-sync/LDAPUser.xml
- /metadata/iam-features-ldap-sync/LDAPRole.xml
- /metadata/iam-features-ldap-sync/LDAPDataProvider.xml
- /metadata/iam-features-ldap-sync/LDAPRelationshipProvider.xml
- /metadata/iam-features-oimupgrade/UpgradeVersionInfo.xml
- /metadata/iam-features-notification/NotificationProviders.xmltion/EventHandlers.xml
- /metadata/iam-features-identity/event-definition/EventHandlers.xml
- /metadata/iam-features-selfservice/event-definition/EventHandlers.xml
- /metadata/iam-features-requestactions/event-definition/EventHandlers.xml
- /metadata/iam-features-configservice/event-definition/EventHandlers.xml
- /db/GTC/ProviderDefinitions/IsValidDateValidatorProvider.xml
- /db/GTC/ProviderDefinitions/IsIntValidatorProvider.xml
- /db/GTC/ProviderDefinitions/IsShortValidatorProvider.xml
- /db/GTC/ProviderDefinitions/IsFloatValidatorProvider.xml
- /db/GTC/ProviderDefinitions/OnetoOne.xml
- /db/GTC/ProviderDefinitions/WSProvisioningTransport.xml
- /db/GTC/ProviderDefinitions/CSVReconFormat.xml
- /db/GTC/ProviderDefinitions/SharedDriveReconTransport.xml
- /db/GTC/ProviderDefinitions/MaxLengthValidatorProvider.xml
- /db/GTC/ProviderDefinitions/SPMLProvisioningFormat.xml
- /db/GTC/ProviderDefinitions/IsLongValidatorProvider.xml
- /db/GTC/ProviderDefinitions/Concatenation.xml
- /db/GTC/ProviderDefinitions/IsDoubleValidatorProvider.xml
- /db/GTC/ProviderDefinitions/IsByteValidatorProvider.xml
- /db/GTC/ProviderDefinitions/ValidateDateFormat.xml
- /db/GTC/ProviderDefinitions/MatchRegexpValidatorProvider.xml
- /db/GTC/ProviderDefinitions/MinLengthValidatorProvider.xml

- /db/GTC/ProviderDefinitions/IsInRangeValidatorProvider.xml
- /db/GTC/ProviderDefinitions/IsBlankOrNullValidatorProvider.xml
- /db/GTC/ProviderDefinitions/Translation.xml
- /metadata/iam-features-ldap-sync/LDAPRoleMembership.xml
- /metadata/iam-features-ldap-sync/LDAPUserMembership.xml
- /metadata/iam-features-ldap-sync/LDAPUser.xml
- /metadata/iam-features-ldap-sync/LDAPRole.xml
- /metadata/iam-features-ldap-sync/LDAPDataProvider.xml
- /metadata/iam-features-ldap-sync/LDAPRelationshipProvider.xml
- /metadata/iam-features-oimupgrade/UpgradeVersionInfo.xml
- /metadata/iam-features-notification/NotificationProviders.xml

## 24.2.2 Generating and Analyzing Pre-Upgrade Report for Oracle Identity Manager

To generate and analyze the pre-upgrade report for Oracle Identity Manager, complete the tasks described in the following sections:

- [Obtaining Pre-Upgrade Report Utility](#)
- [Generating the Pre-Upgrade Report](#)
- [Analyzing the Pre-Upgrade Report](#)

### 24.2.2.1 Obtaining Pre-Upgrade Report Utility

You must download the pre-upgrade utility from Oracle Technology Network (OTN). The utility is available in two zip files named `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002`, along with `ReadMe.doc` at the following location on My Oracle Support:

My Oracle Support document ID 1599043.1

The `ReadMe.doc` contains information about how to generate and analyze the pre-upgrade reports.

### 24.2.2.2 Generating the Pre-Upgrade Report

To generate the pre-upgrade report for Oracle Identity Manager 11.1.2.x.x upgrade, do the following:

1. Create a directory at any location and extract the contents of `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002` in the newly created directory.
2. Create a directory where pre-upgrade reports need to be generated. For example, name the directory `OIM_preupgrade_reports`.
3. Go to the directory where you extracted `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002`, and open the `preupgrade_report_input.properties` file in a text editor. Update the properties file by specifying the appropriate values for the parameters listed in [Table 24-4](#):

**Table 24–4 Parameters to be Specified in the `preupgrade_report_input.properties` File**

Parameter	Description
<code>oim.targetVersion</code>	Specify 11.1.2.3.0 for this parameter, as 11.1.2.3.0 is the target version for which pre-upgrade utility needs to be run.
<code>oim.jdbcurl</code>	Specify the JDBC URL for Oracle Identity Manager in the following format: <code>&lt;host&gt;:&lt;port&gt;/&lt;service_name&gt;</code>
<code>oim.oimschemaowner</code>	Specify the name of the OIM schema owner.
<code>oim.mdsjdbcurl</code>	Specify the MDS JDBC URL in the following format: <code>&lt;host&gt;:&lt;port&gt;/&lt;service_name&gt;</code>
<code>oim.mdsschemaowner</code>	Specify the name of the MDS schema owner.
<code>oim.databaseadminname</code>	Specify the user with DBA privilege. For example, <code>sys</code> as <code>sysdba</code> .
<code>oim.outputreportfolder</code>	Specify the absolute path to the directory that you created in step-2 (directory with name <code>OIM_preupgrade_reports</code> ), where the pre-upgrade reports need to be generated.  Make sure that the output report folder has read and write permissions.
<code>oim.oimhome</code>	Specify the absolute path to the OIM home.
<code>oim.domain</code>	Specify the absolute path to the Oracle Identity Manager domain home.  For example: <code>/Middleware/user_projects/domains/base_domain</code>
<code>oim.wlshome</code>	Specify the absolute path to the WebLogic Server home.  For example: <code>/Middleware/wlserver_10.3</code>
<code>oim.mwhome</code>	Specify the absolute path to the Middleware home.  For example: <code>/Oracle/Middleware</code>  This property is not required if you are upgrading Oracle Identity Manager 9.1.x.x environments.
<code>oim.javahome</code>	Specify the absolute path to the Java home.

- Run the following command from the location where you extracted the contents of `PreUpgradeReport.zip.001` and `PreUpgradeReport.zip.002`.

- **On UNIX:**

```
sh generatePreUpgradeReport.sh
```

- **On Windows:**

```
generatePreUpgradeReport.bat
```

- Provide the details when the following is prompted:

- **OIM Schema Password**

Enter the password of the Oracle Identity Manager (OIM) schema.

- MDS Schema Password  
Enter the password of the Metadata Services (MDS) schema.
  - DBA Password  
Enter the password of the Database Administrator.
6. The reports are generated as HTML pages at the location you specified for the parameter `oim.outputreportfolder` in the `preupgrade_report_input.properties` file. The logs are stored in the log file `preUpgradeReport<time>.log` in the folder `logs` at the same location.
- For the list of pre-upgrade reports generated for various starting points, and for information about analyzing the pre-upgrade reports, see [Section 24.2.2.3, "Analyzing the Pre-Upgrade Report"](#).

### 24.2.2.3 Analyzing the Pre-Upgrade Report

After you generate the pre-upgrade report, you must review each of the reports, and perform all the tasks described in them. If you do not perform the mandatory tasks described in the report before you upgrade, the upgrade might fail.

[Table 24–5](#) provides the description for all of the pre-upgrade reports generated for Oracle Identity Manager. The column `Generated for the Starting Points` in [Table 24–5](#) specifies the starting point(s) for which the pre-upgrade report is generated.

**Table 24–5 Pre-Upgrade Reports Generated for Oracle Identity Manager**

SI No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
1	<code>index.html</code>	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	<p>This report provides links to all the other reports generated by the pre-upgrade report utility.</p> <p>It also states that you must run the pre-upgrade report utility till no pending issues are listed in this report.</p>	See, <a href="#">Description of index.html Report</a>
2	<code>APPROVALPOLICYPreUpgradeReport.html</code>	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	<p>This report lists the request approval policies that has a rule defined on the non existing template.</p>	See, <a href="#">Description of APPROVALPOLICYPreUpgradeReport.html Report</a>
3	<code>AUTHORIZATION_R2PS3PreUpgradeReport.html</code>	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> </ul>	<p>This report provides a list of the home-org policies, self-service policies, and the rule condition for <code>OrclOIMUserManagementChainApprovalPolicy</code> that will be replaced with the out-of-the-box secure rule.</p>	See, <a href="#">Description of AUTHORIZATION_R2PS3PreUpgradeReport.html Report</a>

**Table 24–5 (Cont.) Pre-Upgrade Reports Generated for Oracle Identity Manager**

SI No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
3	CertificationUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.1.0</li> </ul>	<p>This report lists the certification records processed during the upgrade of snapshot data.</p> <p>You must review the information provided in this report.</p>	See, <a href="#">Description of CertificationUpgradeReport.html Report</a>
4	ChallengeQuestionsPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> </ul>	<p>This report provides information about upgrading localized challenge questions data. This report is generated for Oracle Identity Manager upgrade on WebLogic Server only.</p> <p>When you upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.3.0, the existing localization data for challenge questions is lost. Therefore, before proceeding with the upgrade process, you must backup the existing localized challenge questions data.</p> <p>After you upgrade to Oracle Identity Manager 11.1.2.3.0, you must perform the tasks described in this report.</p> <p>If you have already migrated the localized challenge questions data per new localization model provided in Oracle Identity Manager 11g Release 2 (11.1.2.0.11) or (11.1.2.1.3), then skip the tasks described in this report.</p>	See, <a href="#">Description of ChallengeQuestionsPreUpgradeReport.html Report</a>

**Table 24–5 (Cont.) Pre-Upgrade Reports Generated for Oracle Identity Manager**

SI No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
5	CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	<p>This report detects and displays the list of cyclic groups in LDAP.</p> <p>Cyclic groups in LDAP directory are not supported in 11.1.2.2.0. Therefore, you must remove the cyclic dependency from existing Oracle Identity Manager setup and reconcile data from LDAP to Oracle Identity Manager Database. The procedure for doing this is described in the report.</p>	See, <a href="#">Description of CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html Report</a>
6	DOMAIN_CONFIG_CHECKPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	<p>This report lists the applications in Stage mode.</p> <p>This is only applicable for Out of the Box applications; not for the custom applications.</p>	See, <a href="#">Description of DOMAIN_CONFIG_CHECKPreUpgradeReport.html Report</a>
7	DomainReassocAuthorization.html	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> </ul>	<p>This report lists the checks executed for authorization feature data upgrade. It checks if the Oracle Identity Manager is reassociated with the DB-based policy store.</p> <p>Review the table that lists the checks executed and the status of the checks.</p>	See, <a href="#">Description of DomainReassocAuthorization.html Report</a>
8	EVENT_HANDLERPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	<p>This report lists the event handlers that are affected by the upgrade.</p> <p>Review the details in the report, and perform any necessary resolution tasks specified in the report.</p>	See, <a href="#">Description of EVENT_HANDLERPreUpgradeReport.html Report</a>
9	MANDATORY_DATABASE_PRIVILEGE_CHECKPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	<p>This report lists the Database privileges that should be given to the schema owner before you perform schema upgrade.</p>	See, <a href="#">Description of MANDATORY_DATABASE_PRIVILEGE_CHECKPreUpgradeReport.html Report</a>

**Table 24–5 (Cont.) Pre-Upgrade Reports Generated for Oracle Identity Manager**

SI No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
10	ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	This report provides the status of the mandatory database components or settings for Oracle Identity Manager upgrade. Verify the installation or setup status for each of the mandatory component or setting. If any of the component or setting is not setup correctly, follow the recommendations provided in the report to fix them.	See, <a href="#">Description of ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html Report</a>
11	ORACLE_ONLINE_PURGEPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	<p>This report lists the pre-requisites for Online Purge that needs to be addressed before you proceed with the upgrade.</p> <p>This report will not be generated if there is no action item related to purge.</p>	See, <a href="#">Description of ORACLE_ONLINE_PURGEPreUpgradeReport.html Report</a>
12	PasswordPolicyPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 9.1.x.x</li> </ul>	<p>This report lists the potential upgrade issues for password policies.</p> <p>If you are relying on 9.1.x.x password policy model, you must update to new password policies, as 9.1.x.x password policy model is not supported in 11.1.2.3.0. Review the report and assign the password policies listed in the report to appropriate organization(s).</p>	See, <a href="#">Description of PasswordPolicyPreUpgradeReport.html Report</a>
13	PROVISIONINGBYREQUESTPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	This report lists the requests that are not viewable in Track Requests page.	See, <a href="#">Description of PROVISIONINGBYREQUESTPreUpgradeReport.html Report</a>

**Table 24–5 (Cont.) Pre-Upgrade Reports Generated for Oracle Identity Manager**

SI No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
14	PROVISIONINGPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	<p>This report lists the potential application instance creation issues. It provides information about the following:</p> <ul style="list-style-type: none"> <li>■ Provisioning Configuration</li> <li>■ Entitlement Configuration</li> <li>■ Access Policy Configuration</li> <li>■ List of Resource Objects without Process Form</li> <li>■ List of Resource Objects without ITResource field Type in Process Form</li> <li>■ List of Resource Objects with multiple ITResource Lookup fields in Process Form</li> <li>■ List of Access Policies without ITResource value set in default policy data</li> <li>■ List of Access Policies with Revoke If No Longer Applies flag unchecked</li> <li>■ List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value</li> </ul> <p>Review all the sections in the report and perform necessary tasks.</p>	See, <a href="#">Description of PROVISIONINGPreUpgradeReport.html Report</a>
15	REQUESTPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	<p>This report lists any invalid requests and the actions to be taken.</p>	See, <a href="#">Description of REQUESTPreUpgradeReport.html Report</a>
16	UDFPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	<p>This report lists the tasks that you must perform prior to upgrade to ensure that the User Defined Fields (UDFs) are upgraded seamlessly.</p> <p>Perform all the necessary tasks described in this report.</p>	See, <a href="#">Description of UDFPreUpgradeReport.html Report</a>

**Table 24–5 (Cont.) Pre-Upgrade Reports Generated for Oracle Identity Manager**

SI No	HTML Report Name	Generated for the Starting Points	Description	For Detailed Description
17	UISimplificationUpgradeImpactReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> </ul>	This report lists the customizations that are impacted by the upgrade. It also provides the workaround for the known issues related to customizations.	See, <a href="#">Description of UISimplificationUpgradeImpactReport.html Report</a>
18	WLSMBEANPreUpgradeReport.html	<ul style="list-style-type: none"> <li>■ 11.1.2.2.0</li> <li>■ 11.1.2.1.0</li> <li>■ 11.1.2</li> <li>■ 11.1.1.7.0</li> <li>■ 11.1.1.5.0</li> <li>■ 9.1.x.x</li> </ul>	This report lists the .jar files present in the WebLogic.mbean paths that need to be deleted before performing middle tier upgrade. Review the information provided in this report, and perform necessary action.	See, <a href="#">Description of WLSMBEANPreUpgradeReport.html Report</a>

**24.2.2.3.1 Description of index.html Report** The `index.html` report is an index page that contains the names of pre-upgrade reports generated for your starting point, and provides links to their corresponding HTML report. You can navigate to various reports from the index page.

**24.2.2.3.2 Description of APPROVALPOLICYPreUpgradeReport.html Report** The report `APPROVALPOLICYPreUpgradeReport.html` lists the invalid approval policies. This report contains the following sections:

- [Approval Policy rule defined on template](#)
- [List of Approval Polices which needs to be updated with custom approval process](#)
- [Approval policy based on unsupported request type](#)

This report also contains an additional note on approval policy based on deprecated request type. You must review the report completely, before you start upgrading the Oracle Identity Manager 11.1.1.x.x environment.

#### **Approval Policy rule defined on template**

This section lists the Oracle Identity Manager approval policies whose rules are defined based on the request template.

The Request templates feature is not supported in Oracle Identity Manager 11.1.2.3.0. Therefore, if your existing Oracle Identity Manager contains approval policies having rules based on request template, you must reconfigure the request approval policies by following the steps described in the report.

#### **List of Approval Polices which needs to be updated with custom approval process**

This section lists the existing approval policies that need to be associated with different approval process before you start the upgrade process.

The approval process `default/ResourceAdministratorApproval`, `default/ResourceAuthorizerApproval` are not supported in 11.1.2.3.0. Therefore, if

your existing Oracle Identity Manager contains approval policies having these approval process, you must associate them with different approval process.

### Approval policy based on unsupported request type

This section provides information about the request types that are not supported in 11.1.2.3.0.

The following request types are not supported in 11.1.2.3.0, and they are changed to non-self request type in 11.1.2.3.0:

- Self Assign Roles
- Modify Self Profile
- Self Remove Roles
- Self De-Provision Resource
- Self Modify Provisioned Resource
- Self-Request Resource

Self-request type mapping to Non-Self request type is shown [Table 24–6](#).

**Table 24–6 Mapping of Self request type to Non-Self request type**

Self Request Type	Non-Self Request Type
Self-Request Resource	Provision Resource
Self Modify Provisioned Resource	Modify Provisioned Resource
Self Remove Roles	Remove from Roles
Modify Self Profile	Modify User Profile
Self De-Provision Resource	De-Provision Resource
Self Assign Roles	Assign Roles

### Approval policy based on deprecated request type

This section provides information about deprecated request types in 11.1.2.3.0.

The following request types are deprecated in 11.1.2.3.0:

- Provision Resource
- De-Provision Resource
- Disable Provisioned Resource
- Enable Provisioned Resource
- Modify Provisioned Resource

Approval policies based on these deprecated request types will continue to work for any pending requests based on these request types even after upgrade. But, these policies will not work for requests created for Application Instance based request types such as - Provision Application Instance, Revoke Account, Disable Account, Enable Account, and Modify Account.

In addition, approval policies for Application Instance based request types need to be explicitly created for the request based on Application Instance.

**24.2.2.3.3 Description of AUTHORIZATION\_R2PS3PreUpgradeReport.html Report** The AUTHORIZATION\_R2PS3PreUpgradeReport.html report provides a list of the home-org

policies, self-service policies, and the rule condition for `OrclOIMUserManagementChainApprovalPolicy` that will be replaced with the out-of-the-box secure rule. Review the information provided in the report.

**24.2.2.3.4 Description of CertificationUpgradeReport.html Report** The report `CertificationUpgradeReport.html` lists the certification records processed during the upgrade of snapshot data. This report displays a table that contains the certification record ID, column name, current value, and the new value. Review the information provided in the table.

**24.2.2.3.5 Description of ChallengeQuesPreUpgradeReport.html Report** The report `ChallengeQuesPreUpgradeReport.html` is generated for both 11.1.2 and 11.1.2.1.0 starting points.

When you upgrade Oracle Identity Manager 11.1.2.x.x to 11.1.2.3.0, the existing localization data for challenge questions is lost as it is not upgrade-safe. Therefore, before you upgrade to Oracle Identity Manager 11.1.2.3.0, you must backup the existing localized challenge questions data.

After you upgrade to 11.1.2.3.0, perform the tasks described in this report to localize challenge questions. Follow the instructions in the section applicable for your starting point.

---

**Note:** If you have already migrated the localized challenge questions data per localization model provided in Oracle Identity Manager 11g Release 2 (11.1.2.0.11) or (11.1.2.1.3), ignore the tasks described in this report.

---

**24.2.2.3.6 Description of CYCLIC\_GROUP\_MEMBERSHIP\_CHKPreUpgradeReport.html Report** The report `CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html` provides information about the Cyclic groups in LDAP directory.

Oracle Identity Manager 11.1.2.3.0 does not support cyclic groups in the LDAP directory. Therefore, you must remove any cyclic dependency from your existing setup and reconcile data from LDAP to Oracle Identity Manager Database, before you proceed with the upgrade.

For more information about removing the cyclic groups dependent on LDAP, see [Removing Cyclical Groups Dependent on LDAP and Reconciling Data From LDAP to OIM Database](#). The procedure for removing cyclic groups is also described in this report.

### **Removing Cyclical Groups Dependent on LDAP and Reconciling Data From LDAP to OIM Database**

If the LDAP in your existing Oracle Identity Manager environment has cyclic groups loaded, you must remove the cyclic groups by doing the following:

1. Use JEXplorer or Softerra LDAP Administrator and navigate to the cyclic groups.
2. Look for **uniquemember** attribute.
3. Remove all values from the attribute.
4. Save the group.
5. Reconcile the data from LDAP to Oracle Identity Manager Database by running the following command:

On UNIX: `LDAPConfigPostSetup.sh`

On Windows: LDAPConfigPostSetup.bat

### Example Scenario

If you have cyclic group dependency between two groups: Group1 and Group2, do the following to remove cyclic dependency:

1. Connect to LDAP using JEXplorer or Softerra LDAP.
2. Go to the group container of Group1.
3. Go to the **uniquemember** attribute under Group1.
4. Remove the value of Group2, from unique members, and save the change made.
5. Run LDAPConfigPostSetup.sh (on UNIX) or LDAPConfigPostSetup.bat (on Windows) to reconcile data from LDAP to Oracle Identity Manager database.

**24.2.2.3.7 Description of DOMAIN\_CONFIG\_CHECKPreUpgradeReport.html Report** This report lists the applications in Stage mode.

This is only applicable for Out of the Box applications; not for the custom applications.

**24.2.2.3.8 Description of DomainReassocAuthorization.html Report** The pre-upgrade report utility checks if the Oracle Identity Manager domain is reassociated to Database based policy store and generates the DomainReassocAuthorization.html report. The result of this check is displayed in the **Result** column of this report. Review the checks executed and the result of the checks.

**24.2.2.3.9 Description of EVENT\_HANDLERPreUpgradeReport.html Report** This report lists all the event handlers that are affected during upgrade. It displays a table with information related to the event handler XML, event handler name, entity type, operation, and stage. The table also contains a **Resolution/Information** column which provides any resolution tasks that need to be completed. Review the information in the table.

**24.2.2.3.10 Description of MANDATORY\_DATABASE\_PRIVILEGE\_CHECKPreUpgradeReport.html Report** This report lists the Database privileges that should be given to the schema owner before you perform schema upgrade.

**24.2.2.3.11 Description of ORACLE\_MANDATORY\_COMPONENT\_CHKPreUpgradeReport.html Report** This report lists all the mandatory database components or settings for Oracle Identity Manager upgrade. This report contains a table which lists the component or setting, it's installation or setup status, and recommendations if any. You must review the installation or setup status for each of the mandatory component or setting listed in the table. If the component or setting is not setup correctly, follow the recommendations specified in the **Note** column of the table in the report to fix them.

**24.2.2.3.12 Description of ORACLE\_ONLINE\_PURGEPreUpgradeReport.html Report** Before you upgrade Oracle Identity Manager to 11.1.2.3.0, you must complete the pre-requisites for online purge.

The table in this report lists the database tables on which the mentioned pre-upgrade steps need to be performed before you upgrade. The table also shows the status of the database tables in **OIM schema** and **Note** section. Review the table, and perform the actions required.

**24.2.2.3.13 Description of PasswordPolicyPreUpgradeReport.html Report** The report PasswordPolicyPreUpgradeReport.html lists the potential upgrade issues for

password policies. If you are using 9.1.x.x password policy model, you must update them to new password policies. The 9.1.x.x password policy model is no longer supported for Users, and any such customizations done are not migrated to the new password policy model. A default password policy is seeded at TOP organization that needs to be revisited.

This report contains a table that lists the password policies that are attached to the Xellerate User resource object according to the 9.1.x.x password policy model. You must assign those password policies to appropriate organization(s).

**24.2.2.3.14 Description of PROVISIONINGBYREQUESTPreUpgradeReport.html Report** The following table provides information about the requests that are not viewable in Track Requests page:

**Table 24-7 Password Policies**

Request Key	Beneficiary Key	Entity Type	Entity Name	Entity Key	Request Model Name	Issue
81	83	Resource	AD User	7	Access Policy Based Provisioning	No process form entry found for process instance. Cannot update rbe_entity_key in request_beneficiary_entities table since application instance for the entry is not created.
82	85	Resource	AD User	7	Access Policy Based Provisioning	No process form entry found for process instance. Cannot update rbe_entity_key in request_beneficiary_entities table since application instance for the entry is not created.
86	99	Resource	AD User	7	Provision Resource	No process form entry found for process instance. Cannot update rbe_entity_key in request_beneficiary_entities table since application instance for the entry is not created.

**24.2.2.3.15 Description of PROVISIONINGPreUpgradeReport.html Report** This report lists the potential application instances creation issues. The report contains the following sections:

- [Provisioning, Entitlement, and Access Policy Configuration Details](#)
- [List of Resource Objects without Process Form](#)
- [List of Resource Objects without ITResource field Type in Process Form](#)
- [List of Resource Objects with multiple ITResource Lookup fields in Process Form](#)
- [List of Access Policies without ITResource value set in default policy data](#)
- [List of Access Policies with Revoke If No Longer Applies flag unchecked](#)
- [List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value](#)

#### **Provisioning, Entitlement, and Access Policy Configuration Details**

This section describes the steps you must complete before you upgrade Oracle Identity Manager 11.1.2.3.0. These steps are related to provisioning, entitlement, and access policy configuration. Complete all the steps described in this section of the report.

**List of Resource Objects without Process Form**

This section provides information about the resource objects in your existing Oracle Identity Manager that do not have process form. Each resource object must have a process form associated with it. Therefore, if a resource object is not associated with a process form, you must associate the resource object with a process form before you start the upgrade process. Review the table in this section of the report, that lists the details of the resource objects without process form.

**List of Resource Objects without ITResource field Type in Process Form**

This section provides information about the resource objects without ITResource field type in their respective process forms. Review the table in this section of the report, which contains more details. If your existing Oracle Identity Manager has resource objects without ITResource field in their process forms, do the following:

1. Create appropriate IT resource definition.
2. Create IT resource instance for the same corresponding to the target that is being provisioned.
3. Edit the process form and add a field of type "ITResource" to the process form. Set the following properties:

```
Type=IT Resource definition created in step-1
```

```
ITResource=true
```

4. Activate the form.
5. Update the IT resource field on existing provisioned accounts using FVC Utility.
6. Once the above steps are completed, you can create application instances corresponding to the Resource Object+ITResource combination.

**List of Resource Objects with multiple ITResource Lookup fields in Process Form**

This section provides information about the resource objects that have multiple lookup fields in their process form. In your existing Oracle Identity Manager environment, if you have resource objects with multiple ITResource set in the process form, you must set the value of the property `ITResource Type` to `true` for at least one of the attributes.

**List of Access Policies without ITResource value set in default policy data**

This section lists the access policies for which the ITResource values of the resource objects should be set in the default policy data. The table in this section lists the access policies in your existing Oracle Identity Manager for which ITResource field is missing. You must set the values of ITResource field for each of the access policy listed in the table.

**List of Access Policies with Revoke If No Longer Applies flag unchecked**

This section lists the access policies that have Revoke If No Longer Applies flag unchecked. The table in this section contains the list of access policies that will be updated to Disable If No Longer Applies, during upgrade. The table also indicates if tasks for enable, disable, revoke actions are not defined for these policies. You must add the missing tasks before you proceed with the upgrade. Also, if you want the behavior of the policy to change to RNLA checked, you must check the RNLA flag for the respective policy.

### List of Entitlements stored in Lookup definitions that do not have IT Resource Key in the lookup encode value

This section lists entitlements stored in lookup definitions that do not have IT Resource Key pretended to their encoding values using "~". Entitlements stored in lookup definitions need IT Resource Key prepended to the encoded values using "~". Review the table in this section of the pre-upgrade report, which contains more details.

**24.2.2.3.16 Description of REQUESTPreUpgradeReport.html Report** The report `REQUESTPreUpgradeReport.html` lists requests that are affected because of the upgrade. This report contains the following sections:

- [Requests with unsupported request stages](#)
- [Requests which will be automatically changed to corresponding non-self request type](#)

#### Requests with unsupported request stages

This section lists the requests that are in one of the following unsupported request stages:

- Obtaining Template Approval
- Template Approval Approved
- Template Approval Rejected
- Template Approval Auto Approved

Manual intervention is required to move these requests to the next stage by approving, withdrawing, or closing such requests. Otherwise, requests are moved to request closed stage as part of the upgrade.

Review the list of requests that are in the unsupported request stage.

#### Requests which will be automatically changed to corresponding non-self request type

This section lists the requests that are based on one of the following request types will be changed to the corresponding non-self request type after the upgrade:

- Self Assign Roles
- Modify Self Profile
- Self Remove Roles
- Self De-Provision Resource
- Self Modify Provisioned Resource
- Self-Request Resource

Request types for these requests are automatically changed to the corresponding non-self request type as part of the upgrade.

Self-request type mapping to non-self request type is shown in [Table 24–8](#):

**Table 24–8 Mapping of Self-Request Type to Non-Self Request Type**

Self request type	Non-Self request type
Self-Request Resource	Provision Resource

**Table 24–8 (Cont.) Mapping of Self-Request Type to Non-Self Request Type**

Self request type	Non-Self request type
Self Modify Provisioned Resource	Modify Provisioned Resource
Self Remove Roles	Remove from Roles
Modify Self Profile	Modify User Profile
Self De-Provision Resource	De-Provision Resource
Self Assign Roles	Assign Roles

**24.2.2.3.17 Description of UDFPreUpgradeReport.html Report** The report `UDFPreUpgradeReport.html` lists the steps that you must complete before you proceed with the upgrade process, to ensure that the User Defined Fields/Attributes (UDFs) are upgraded seamlessly.

Note that you may have to edit the entity xml file manually. To edit a file in MetaData Services (MDS), you must export the file from MDS repository. After making the required changes, you must import the file back to MDS.

This report contains the following tables:

- Table that lists the path to the entity XML file in MDS corresponding to a particular entity type
- Table that lists the UDFs with inconsistent max-size. You must edit the entity xml file per the list provided in the table, to change the max-size of the attributes to expected values, and re-import the file back into MDS.
- Table that lists the UDFs with inconsistent default values. You must edit the corresponding entity xml file manually to change the default value to one of the allowed values.

**24.2.2.3.18 Description of UISimplificationUpgradeImpactReport.html Report** Oracle Identity Manager 11.1.2.3.0 comes with improved and simplified Self-Service UI. Some of the changes include simplified workspace based navigation model, new OIM-alta skin enforcing uniform look and feel across the UI, flow based UI rendering, usage of pagination instead of scroll bars, and improved search pattern on Self-Service search pages. Therefore some of the UI customizations must be reimplemented post upgrade. Review the information provided in this report, and redo the UI customizations as required after upgrade.

**24.2.2.3.19 Description of WLSMBEANPreUpgradeReport.html Report** The report `WLSMBEANPreUpgradeReport.html` lists the `.jar` files in WebLogic mbeans path that need to be deleted prior to middle tier upgrade. The report contains a table that lists the `.jar` files, their status whether they are present in the WebLogic mbean path, and the action required. Review the information provided in the table, and perform necessary action.

## 24.2.3 Upgrading Oracle SOA Suite to 11g Release 1 (11.1.1.9.0)

Oracle Identity Manager 11.1.2.3.0 is certified with Oracle SOA Suite 11g Release 1 (11.1.1.9.0). If you are not using Oracle SOA Suite 11.1.1.9.0, you must upgrade your existing Oracle SOA Suite to 11.1.1.9.0 by completing the following steps:

1. Review the Oracle Fusion Middleware System Requirements and Specifications for 11g Release 1 (11.1.1) at the following link:

<http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-requirements-100147.html>

2. Complete the steps described in the section "Special Instructions for Patching Oracle SOA Suite" in the *Oracle Fusion Middleware Patching Guide* for 11g Release 1 (11.1.1.9.0), before you upgrade Oracle SOA Suite to 11.1.1.9.0.
3. Download the Oracle SOA Suite 11.1.1.9.0 installer. This installer can also function as upgrade installers. For more information about downloading Oracle SOA Suite 11.1.1.9.0 installer, see "Downloading Oracle Fusion Middleware Patches for an Existing 11g Release 1 Installation" in the *Oracle Fusion Middleware Download, Installation, and Configuration Readme for 11g Release 1 (11.1.1.9.0)*.
4. Start the installer and apply the patch. For more information, see "Patching Oracle Fusion Middleware" in the *Oracle Fusion Middleware Patching Guide* for 11g Release 1 (11.1.1.9.0).
5. Upgrade the SOAINFRA schema by running the Patch Set Assistant (PSA). For more information, see "Upgrading Your Schemas with Patch Set Assistant" in the *Oracle Fusion Middleware Patching Guide* for 11g Release 1 (11.1.1.9.0).
6. After you upgrade Oracle SOA Suite to 11.1.1.9.0, you must perform the necessary post-patching tasks depending on your SOA starting point.

[Table 24–9](#) lists the post-patching tasks for Oracle SOA Suite, and the SOA starting point they are applicable for.

**Table 24–9 Post-Patching Tasks for Oracle SOA Suite**

SI No	Post-Patching Task	Perform if Your SOA Starting Point is
1	Removing the tmp Folder for SOA Composer, BPM Workspace and B2B	<ul style="list-style-type: none"> <li>■ 11.1.1.6.0</li> <li>■ 11.1.1.5.0</li> </ul>
2	Upgrading the "BPEL Message Recovery Required" Warning Message Duration	<ul style="list-style-type: none"> <li>■ 11.1.1.6.0</li> </ul>
3	Upgrading MAXRECOVERATTEMPT Attribute to 2	<ul style="list-style-type: none"> <li>■ 11.1.1.6.0</li> <li>■ 11.1.1.5.0</li> </ul>
4	Extending the SOA Domain with UMS Adapter Features	<ul style="list-style-type: none"> <li>■ 11.1.1.6.0</li> <li>■ 11.1.1.5.0</li> </ul>
5	Extending the SOA Domain with Business Process Management Features	<ul style="list-style-type: none"> <li>■ 11.1.1.6.0</li> <li>■ 11.1.1.5.0</li> </ul>
6	Upgrading the Oracle Data Integrator Clients if BAM-ODI Integration is Enabled	<ul style="list-style-type: none"> <li>■ 11.1.1.5.0</li> </ul>
7	Saving and Restoring XEngine Customizations for Oracle B2B	<ul style="list-style-type: none"> <li>■ 11.1.1.5.0</li> </ul>

7. Start the WebLogic Administration Server and the SOA Managed Server(s). For information about starting the servers, [Section 24.1.8, "Starting the Servers"](#).
8. Verify the Patch Set installation by following the instructions described in the section "Verifying Your Patch Set Installation" in the *Oracle Fusion Middleware Patching Guide* for 11g Release 1 (11.1.1.9.0).

## 24.2.4 Upgrading Oracle Identity Manager Middle Tier

Middle tier upgrade is performed using the `OIMUpgrade.sh` utility. Oracle Identity Manager middle tier upgrade is carried out in two stages:

### 1. Middle tier upgrade offline

This is the first stage where `OIMUpgrade.sh` is run in `offline` mode, that is, with the Administration Server and the Managed Server(s) in shutdown state.

### 2. Middle tier upgrade online

This is the second stage where `OIMUpgrade.sh` is run in `online` mode, that is with the Administration Server and the SOA Managed Server(s) in running state.

To upgrade the Oracle Identity Manager middle tier, complete the following tasks:

- [Additional Task for Windows 64-Bit Users Before Upgrading Middle Tier](#)
- [Creating a Truststore for Upgrading SSL Enabled Middleware](#)
- [Updating the Properties File](#)
- [Performing Oracle Identity Manager Middle Tier Upgrade Offline](#)
- [Starting Administration Server and SOA Managed Server\(s\)](#)
- [Performing Oracle Identity Manager Middle Tier Upgrade Online](#)
- [Starting the Oracle Identity Manager Managed Server\(s\) and the BIP Server](#)
- [Changing the Deployment Order of Oracle Identity Manager EAR](#)

#### 24.2.4.1 Additional Task for Windows 64-Bit Users Before Upgrading Middle Tier

If you are upgrading Oracle Identity Manager on a 64-bit Windows platform and if you have installed JAVA in a directory where there is a space in the installed classpath (for example, `C:\Program File\Java`), then you must complete the following steps:

1. Add a `JAVA_HOME` entry to the environment variable pointing to a JDK installation, not to a JRE installation.

---

---

**Note:** This path should be without spaces or like  
`C:\Progra~1\Java\jdk1.6.0_29`.

---

---

2. Hard code the value of `JAVA_HOME` in `<WL_HOME>\server\bin\setWLSEnv.cmd` file to avoid any Middle Tier upgrade failures.

#### 24.2.4.2 Creating a Truststore for Upgrading SSL Enabled Middleware

If you are upgrading an SSL enabled middleware, that is, if you would be specifying SSL ports for WebLogic Administration Server and SOA Managed Servers during middle tier upgrade, you must create a truststore that contains the public certificates for all SSL enabled servers (which can be WebLogic Administration Server, SOA Managed Servers, OIM Managed Servers) irrespective of the node on which the server is running. This truststore will be used a client side store by the upgrade script to communicate with various servers during upgrade.

To create a truststore, complete the following steps:

1. Export the public certificate from the identity store for each server, and place all of them in a single directory.
2. Import all of the public certificates to a single truststore.

3. Copy the truststore to a location accessible by upgrade script.
4. Specify the truststore location and type for the properties `wls.trustStore.loc` and `wls.trustStore.type` respectively, when updating the properties file as described in [Section 24.2.4.3, "Updating the Properties File"](#).

### 24.2.4.3 Updating the Properties File

You must update the `oim_upgrade_input.properties` file with the values for the properties required for middle tier upgrade. To do this, complete the following steps:

1. Open the `oim_upgrade_input.properties` file located at `ORACLE_OIM_HOME/server/bin/` in a text editor.
2. Specify the values for all of the properties required for the middle tier upgrade.

[Table 24–10](#) lists the properties and their descriptions:

**Table 24–10 Parameters to be specified in the Properties File**

Parameter	Used for SSL or Non-SSL Environment?	Description
<code>java.home</code>	Both SSL and Non-SSL	Specify the JAVA HOME location.
<code>server.type</code>	Both SSL and Non-SSL	Specify the Application Server that you are using.  For example, if you are using Oracle WebLogic Server, specify <code>wls</code> for this parameter; or if you are using IBM WebSphere, specify <code>was</code> .  As this document describes the procedure to upgrade Oracle Identity Manager on WebLogic, you must specify <code>wls</code> for this parameter.
<code>oim.jdbcurl</code>	Both SSL and Non-SSL	Specify the Oracle Identity Manager JDBC URL in the format:  <code>host:port/db servicename</code>
<code>oim.oimschemaowner</code>	Both SSL and Non-SSL	Specify the Oracle Identity Manager schema owner.
<code>oim.oimmdsjdbcurl</code>	Both SSL and Non-SSL	Specify the MDS JDBC URL.
<code>oim.opssschemowner</code>	Both SSL and Non-SSL	Specify the Oracle Platform Security Services (OPSS) schema owner.  This property is required only if you are upgrading Oracle Identity Manager 11.1.1.x.x environments.
<code>oim.opssjdbcurl</code>	Both SSL and Non-SSL	Specify the JDBC URL of the Oracle Platform Security Services.  This property is required only if you are upgrading Oracle Identity Manager 11.1.1.x.x environments.
<code>oim.mdsschemaowner</code>	Both SSL and Non-SSL	Specify the MDS schema owner name.
<code>oim.adminhostname</code>	Both SSL and Non-SSL	Specify the Oracle WebLogic Server Administration host name.

**Table 24–10 (Cont.) Parameters to be specified in the Properties File**

<b>Parameter</b>	<b>Used for SSL or Non-SSL Environment?</b>	<b>Description</b>
<code>oim.adminport</code>	Both SSL and Non-SSL	Specify the Oracle WebLogic Server Administration port.
<code>oim.adminUserName</code>	Both SSL and Non-SSL	Specify the username that is used to log in to the Oracle WebLogic Server Administration Console.
<code>oim.soahostmachine</code>	Both SSL and Non-SSL	Specify the SOA host name where SOA Server is running.
<code>oim.soaportnumber</code>	Both SSL and Non-SSL	Specify the SOA Server port.
<code>oim.soasusername</code>	Both SSL and Non-SSL	Specify the SOA Managed Server username.
<code>oim.domain</code>	Both SSL and Non-SSL	Specify the Oracle Identity Manager domain location.
<code>oim.home</code>	Both SSL and Non-SSL	Specify the Oracle OIM Home location.
<code>oim.mw.home</code>	Both SSL and Non-SSL	Specify the Oracle Middleware Home location.
<code>soa.home</code>	Both SSL and Non-SSL	Specify the Oracle SOA Home location.
<code>wl.home</code>	Both SSL and Non-SSL	Specify the WebLogic Home location.
<code>wls.trustStore.loc</code>	SSL only	<p>Specify the client-side trust store location which contains the public certificate of the WebLogic Administration Server, SOA Managed Server(s), and the OIM Managed server(s).</p> <p>For example:</p> <pre>wls.trustStore.loc=/u01/client_store.jks</pre> <p>In case of SSL enabled environment with DEMO keystore, specify DemoTrust.</p> <p>For example:</p> <pre>wls.trustStore.loc=DemoTrust</pre> <p>This property is required only in case of SSL enabled environment with custom keystore.</p> <p>In case of non-SSL environment, do not specify any value for this property.</p>
<code>wls.trustStore.type</code>	SSL only	<p>Specify the type of the truststore, that you specified for the property <code>wls.trustStore.loc</code>. The type of truststore is the extension of the truststore file like JKS, PKCS12, JCEK, JCERACFKS and so on.</p> <p>For example:</p> <pre>wls.trustStore.type=JKS</pre>
<code>bip.server.name</code>	Both SSL and Non-SSL	The value for this property will be existing already. Verify if the BIP server name is correct. Modify the value if required.

**Table 24–10 (Cont.) Parameters to be specified in the Properties File**

<b>Parameter</b>	<b>Used for SSL or Non-SSL Environment?</b>	<b>Description</b>
bip.cluster.name	Both SSL and Non-SSL	Specify the name of the BIP cluster.
bip.server.host.name	Both SSL and Non-SSL	Specify the fully qualified hostname of the Oracle BI Publisher server.
bip.server.port	Both SSL and Non-SSL	The value for this property will be existing already. Verify if the BIP server port is correct. Modify the value if required.
bip.server.ssl.port	SSL only	Specify the SSL port of the Oracle BI Publisher server.
bip.server.ssl.enabled	Both SSL and Non-SSL	Set the value of this property to true if BIP server is SSL enabled; else, set it to false.
bip.jdbc.url	Both SSL and Non-SSL	Specify the BIP server JDBC URL.
bip.schema	Both SSL and Non-SSL	Specify the name of the BIP schema.
oam.version	Both SSL and Non-SSL	This property is required if you are upgrading Oracle Identity Manager - Oracle Access Manager integrated environments. Specify the Oracle Access Manager version for this property. For example, if the Oracle Access Manager version that you are using is 11g Release 2 (11.1.2.3.0), specify 11.1.2.3.0.
oam.wls.admin.host	Both SSL and Non-SSL	This property is required if you are upgrading Oracle Identity Manager - Oracle Access Manager integrated environments. Specify the WebLogic Administration Server host name for Oracle Access Manager.
oam.wls.admin.port	Both SSL and Non-SSL	This property is required if you are upgrading Oracle Identity Manager - Oracle Access Manager integrated environments. Specify the WebLogic Administration Server port for Oracle Access Manager.
oam.admin.username	Both SSL and Non-SSL	This property is required if you are upgrading Oracle Identity Manager - Oracle Access Manager integrated environments. Specify the username of the Oracle Access Manager administrator. This is the user who has admin access to the Oracle Access Manager console.

**Table 24–10 (Cont.) Parameters to be specified in the Properties File**

Parameter	Used for SSL or Non-SSL Environment?	Description
<code>oam.admin.trust.store.loc</code>	SSL only	<p>This property is required if you are upgrading Oracle Identity Manager - Oracle Access Manager integrated environments.</p> <p>If SSL is enabled in Oracle Access Manager Administration Server and SSL port is specified for the property <code>oam.wls.admin.port</code>, then you specify the location of the trust store file for this property.</p> <p>If you have specified a value for the property <code>wls.trustStore.loc</code>, then the value specified for the property <code>oam.admin.trust.store.loc</code> will be ignored. The upgrade utility will consider the value specified for <code>wls.trustStore.loc</code>.</p> <p>If SSL is enabled and SSL port is specified for both Oracle Identity Manager and Oracle Access Manager, you must import Oracle Access Manager certificate to Oracle Identity Manager trust store, or import both Oracle Access Manager and Oracle Identity Manager certificates to a common trust store and specify the location of the trust store for the property <code>wls.trustStore.loc</code>.</p> <p>If <code>wls.trustStore.loc</code> is <code>DemoTrust</code>, specify the full path to the <code>DemoTrust.jks</code> file, which is usually located at <code>WL_HOME/server/lib</code>.</p>
<code>oam.admin.trust.store.type</code>	SSL only	<p>This property is required if you are upgrading Oracle Identity Manager - Oracle Access Manager integrated environments.</p> <p>Specify the trust store type. The trust store can be <code>JKS</code> OR <code>PKCS12</code>. The default trust store is <code>JKS</code>.</p>

The following is a sample of the `oim_upgrade_input.properties` file:

```
#The user inputs are taken from this property file
#Please enter the appropriate values.

#1. JAVA HOME
#java.home=/scratch/wars2install/was/java/
java.home=/scratch/jdk1.7.0_11/

#2. Server type Weblogic/Websphere
#server.type=wls/was
server.type=wls

#OIM SCHEMA DETAILS

#3. Oim Connection String
#GIVE ONLY NON-SSL DB PORT
#host:port/serviceName (SID Not Supported)
#oim.jdbcurl=localhost:1521/oim123.example.com
oim.jdbcurl=myhost.example.com:1522/oimdb.example.com
```

```
#4. Oim Schema owner
#oim.oimschemaowner=hhs_oim
oim.oimschemaowner=OES_11.1.1.5.0_oim

#-----
-----
#MDS SCHEMA DETAILS
#5. MDS Connection String
#GIVE ONLY NON-SSL DB PORT
#host:port/serviceName (SID Not Supported)
#oim.oimmdsjdbcurl=localhost:1521/oim123.example.com
oim.oimmdsjdbcurl=myhost.example.com:1522/oimdb.example.com

#6. MDS Schema Owner
#oim.mdsschemaowner=hhs_mds
oim.mdsschemaowner=OES_11.1.1.5.0_mds

#-----
-----
#ADMIN SERVER DETAILS
#7. Admin Host name
#oim.adminhostname=localhost
oim.adminhostname=myhost.example.com

#8. Admin Port
#oim.adminport=7001
oim.adminport=7002

#9. Admin User name
#oim.adminUserName=weblogic
oim.adminUserName=weblogic
#-----
-----

#SOA DETAILS
#10. SOA Host name
#oim.soahostmachine=localhost
oim.soahostmachine=myhost.example.com

#11. SOA Port
#oim.soaportnumber=8001
oim.soaportnumber=8002

#12. SOA User name
#oim.soausername=weblogic
oim.soausername=weblogic

#-----
-----

#DOMAIN LOCATION
#13. Domain Location
#oim.domain=/u01/oim/user_projects/domains/base_domain
oim.domain=/u01/oim/user_projects/domains/base_domain

#14. Oracle OIM Home
#oim.home=/u01/oim/Oracle_IDM1
oim.home=/u01/oim/Oracle_IDM1
```

```

#15. Middleware Home
#oim.mw.home=/u01/oim
oim.mw.home=/u01/oim

#16. SOA Home
#soa.home=/u01/oim/Oracle_SOA1
soa.home=/u01/oim/Oracle_SOA1
### Weblogic specific Properties

#17 Weblogic Home
#wl.home=
wl.home=/u01/oim/wlserver_10.3/
### Websphere specific properties

#19 CSFSeed=true/false to make MT run in two modes i.e PRE_OIM_CONFIG and POST_
OIMCONFIG respectively
#Choose CSFSeed=true to run in PRE_OIM_Config and CSFSeed=false to run in POST_
OIMCONFIG mode.
CSFSeed=<true/false>

#20 OIM 91 Home Location
oim91Home=<oim 91 home directory>

#21 Management bootstrap port
#oim.bootstrapport=9813
oim.bootstrapport=<Management bootstrap port>

#22 SOA Bootstrap port
#soa.bootstrapport=2801
soa.bootstrapport=<SOA bootstrap port>

#23 Websphere Home
#ws.home=/scratch/wars2install/was
ws.home=<websphere home directory>

#24 Websphere Custom profile path
#ws.custom.path=/scratch/wars2install/was/profiles/Custom05
ws.custom.path=<websphere custom path>

##### ssl env only properties
#####

#25. Client-side trust store location which contains the public certificate of
WLS, SOA, OIM servers
#Fill in trust store location and type only in case of ssl enabled env with
custom keystore
#wls.trustStore.loc=/u01/client_store.jks
#In Case of ssl enabled env with DEMO keystore, give "DemoTrust"
#wls.trustStore.loc=DemoTrust
#In case of non-ssl env, leave blank
#wls.trustStore.loc=

#wls.trustStore.loc=/u01/oim/user_projects/domains/base_
domain/config/fmwconfig/client_store.jks
wls.trustStore.loc=/u01/oim/user_projects/domains/base_
domain/config/fmwconfig/client_store.jks

#26 Type of above trust store
#wls.trustStore.type=JKS
wls.trustStore.type=JKS

```

```

##### BIP Properties #####
#27 BIP Server Name
#bip.server.name=bi_server1
bip.server.name=bi_server1

#28 BIP Cluster Name
#bip.cluster.name=bi_cluster
bip.cluster.name=bi_cluster

#29 BIP Server Port
#bip.server.port=9704
bip.server.port=9704

#30 BIP Server SSL Port
#bip.server.ssl.port=9804
bip.server.ssl.port=9804

#31 BIP Server SSL Enabled
#bip.server.ssl.enabled=false
bip.server.ssl.enabled=false

#32 BIP JDBC URL
#host:port/serviceName (SID Not Supported)
#bip.jdbc.url=localhost:1521/oim123.example.com
bip.jdbc.url=myhost.example.com:1522/oimdb.example.com

#34 BIP Schema Name
#bip.schema=BIP_BIPLATFORM
bip.schema=BIP_BIPLATFORM

##### R1
track#####

# Fill in these values only If you havent extended the domain with OPSS
template
# applicable for source 11.1.1.5.0 and 11.1.1.7.0
# If OPSS datasource (name : opss-DBDS) is already created, these values will
be autodiscovered
and not required to be filled.

#36.oim.opssschemaowner=OES_11.1.1.5.0_opss
oim.opssschemaowner=DEV2_OPSS

#37. oim.opssjdbcurl=localhost:1521:oim123
oim.oimopssjdbcurl=myhost.example.com:1522/oimdb.example.com

##### OAM Integrated
#####
# Fill in these values only if you have OIM-OAM integrated environment
# Make sure OAM admin server (OracleAdminServer in case of Websphere in OAM
Node)
# is running before executing OIMUpgrade.sh/OIMUpgrade.bat command

#37 Specify target OAM version
#If target OAM is 11gR2PS2 then, version is 11.1.2.2.0
#If target OAM is 11gR2PS3 then, version is 11.1.2.3.0
#oam.version=11.1.2.3.0
oam.version=<oam version>

```

```

#38 Specify OAM WLS Admin Server Host Name
#oam.wls.admin.host=localhost
oam.wls.admin.host=<oam wls admin host>

#39 OAM WLS Admin Server port
#oam.wls.admin.port=7001
oam.wls.admin.port=<oam wls admin port>

#40 user who is has administrator access in OAM (The user who has admin access
to oamconsole.)
#oam.admin.username=oamAdminUser
oam.admin.username=<user who is has administrator access in OAM>

#41 If SSL is enabled in OAM admin server and SSL port is specified in the
property
# 'oam.wls.admin.port' then, specify the trust store file location else ignore
this.
#
# NOTE:- If OIM property - 'wls.trustStore.loc' is specified then, any value
for 'oam.admin.trust.store.loc'
# property would be IGNORED and 'wls.trustStore.loc' value would be taken. In
such case where both for
# OIM and OAM, SSL is enabled and SSL port is specified then, import OAM
certificate to OIM truststore
# or both OIM and OAM certificates to a common trust store and specify the same
'wls.trustStore.loc' value here.
#
# If 'wls.trustStore.loc' is DemoTrust then, specify full path of DemoTrust.jks
file, which is usually
# present in '$WL_HOME/server/lib' location.
#
#oam.admin.trust.store.loc=/net/oam_machine/u01/idm/trust/oamtrust.jks

```

#### 24.2.4.4 Performing Oracle Identity Manager Middle Tier Upgrade Offline

Perform the middle tier upgrade offline by doing the following:

1. Make sure that you have stopped the WebLogic Administration Server, the Oracle Identity Manager Managed Server(s), and the SOA Managed Server(s).
2. Run the following command from the location `OIM_ORACLE_HOME/server/bin`:

On UNIX: `./OIMUpgrade.sh offline`

On Windows: `OIMUpgrade.bat offline`

3. Enter the passwords of the following schemas, when prompted:
  - [input]OIM Schema Password: Enter the password of the Oracle Identity Manager (OIM) schema.
  - [input]MDS Password: Enter the password of the Metadata Services (MDS) schema.
  - [input]OPSS Schema Password: Enter the password of the Oracle Platform Security Services (OPSS) schema. You will be prompted for OPSS schema password only if you are upgrading Oracle Identity Manager 11.1.1.x.x environments.
  - [input]SOA Schema Password: Enter the password of the SOA Infrastructure (SOAINFRA) schema.

- [input]BIP Schema Password: Enter the password of the Oracle BI Publisher (BIP) schema.
4. Verify the middle tier offline upgrade by doing the following:
- Check the HTML reports generated at `ORACLE_HOME/server/upgrade/logs/MT/oidUpgradeReportDir_offline`.
  - Check the logs files generated at `ORACLE_HOME/server/upgrade/logs/MT/` to verify if the middle tier offline upgrade was successful.
- [Table 24–11](#) lists the log files generated for Oracle Identity Manager middle tier offline upgrade at the location `ORACLE_HOME/server/upgrade/logs/MT/`.

**Table 24–11 Logs Generated for OIM Middle Tier Offline Upgrade**

Log File Name	Generated for
<code>ant_ApplicationDB.log</code>	■ 11.1.1.x.x
<code>ant_applyBip.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_configureSecurityStore.log</code>	■ 11.1.1.x.x
<code>ant_createBIPDatasources_BPEL.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_createBIPDatasources_OIM.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_createBipServer.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_deploySCIMWebapp.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_extendOPSSDomain.log</code>	■ 11.1.1.x.x
<code>ant_isClusterOIM.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_JMSModuleTargetScript.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_JRF_WsAsync.log</code>	■ 11.1.1.x.x
<code>ant_JVMParams.log</code>	■ 11.1.2.x.x
<code>ant_MigrateJazn_bi-policystore-systemrole-jazn.xml.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_MigrateJazn_jazn-data-oid.xml.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_MigrateJazn_jazn-data-self.xml.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_MigrateJazn_oid-bi-policystore-appPoliciesMigrate.xml.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_MiscUpgrade.log</code>	■ 11.1.2.x.x ■ 11.1.1.x.x
<code>ant_oidUpgradeDomainPackages.log</code>	■ 11.1.1.x.x

**Table 24–11 (Cont.) Logs Generated for OIM Middle Tier Offline Upgrade**

Log File Name	Generated for
ant_OPSS.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> <li>■ 11.1.1.x.x</li> </ul>
ant_oracle.idm.ids.config.ui#11.1.2@11.1.2.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> <li>■ 11.1.1.x.x</li> </ul>
ant_oracle.idm.ipf#11.1.2@11.1.2.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> <li>■ 11.1.1.x.x</li> </ul>
ant_soaOIMLookupDB.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> <li>■ 11.1.1.x.x</li> </ul>
ant_targetBIPResources.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> <li>■ 11.1.1.x.x</li> </ul>
ant_updateBIPJmsSecurity.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> </ul>
ant_Update_setDomainEnv.log	<ul style="list-style-type: none"> <li>■ 11.1.1.x.x</li> </ul>
ant_UpgardeJRF.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> <li>■ 11.1.1.x.x</li> </ul>
ant_Workmanager.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> <li>■ 11.1.1.x.x</li> </ul>
ant_enableJsseSsl.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> <li>■ 11.1.1.x.x</li> </ul>
ant_MigrateJazn_backup.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> </ul>
delta_jobs.xml	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> </ul>
SeedSchedulerData.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> <li>■ 11.1.1.x.x</li> </ul>
OIMUpgrade_offline<timestamp>.log	<ul style="list-style-type: none"> <li>■ 11.1.2.x.x</li> </ul>

#### 24.2.4.5 Starting Administration Server and SOA Managed Server(s)

After you upgrade middle tier offline, you must start the WebLogic Administration Server and the SOA Managed Server(s) in order to perform middle tier upgrade online.

---

**Note:** Before you start the servers, you must add the following property below the `JAVA_PROPERTIES` entry in the `DOMAIN_HOME/bin/setDomainEnv.sh` (on UNIX) or `DOMAIN_HOME/bin/setDomainEnv.cmd` (on Windows) file, to ignore hostname verification:

```
-Dweblogic.security.SSL.ignoreHostnameVerification=true
```

If you are starting the servers on command line, pass the above argument on command line.

This argument can be removed after you complete the upgrade.

---

For information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

---



---

**Note:** Make sure that you do not start the Oracle Identity Manager Managed Server(s).

---



---

#### 24.2.4.6 Performing Oracle Identity Manager Middle Tier Upgrade Online

Perform the middle tier upgrade online by doing the following:

1. Make sure that the WebLogic Administration Server and the SOA Managed Server(s) are up and running. Also, make sure that the Oracle Identity Manager Managed Server(s) and the BIP Managed Server(s) are not in running state.

---



---

**Note:** Ensure that the SOA Managed Server is up and running by verifying the message "SOA Platform is running and accepting requests" in the `soa_server-diagnostic.log` file located at `DOMAIN_HOME/servers/soa_server1/logs/`.

---



---

2. Make sure that the offline middle tier upgrade was run successfully.
3. Run the following command from the location `OIM_ORACLE_HOME/server/bin`:  
On UNIX: `./OIMUpgrade.sh online`  
On Windows: `OIMUpgrade.bat online`
4. Enter the passwords of the following schemas, when prompted:
  - `[input]OIM Schema Password:` Enter the password of the Oracle Identity Manager (OIM) schema.
  - `[input]MDS Password:` Enter the password of the Metadata Services (MDS) schema.
  - `[input]Weblogic Admin Password:` Enter the password of the Oracle WebLogic Server Administrator.
  - `[input]SOA Admin Password:` Enter the password of the Oracle SOA Suite Administrator.
  - `[input]SOA Schema Password:` Enter the password of the SOA Infrastructure (SOAINFRA) schema.
  - `[input]BIP Schema Password:` Enter the password of the Oracle BI Publisher (BIP) schema.

---



---

**Note:** If you are upgrading Oracle Identity Manager - Oracle Access Manager integrated environments, you will be prompted for `[input]OAM 'oamAdminUser' Password`.

---



---

5. Verify the middle tier online upgrade by doing the following:
  - Check the HTML reports generated at `ORACLE_HOME/server/upgrade/logs/MT/oimUpgradeReportDir_online`.
  - Check the following log files generated at the location `ORACLE_HOME/server/upgrade/logs/MT/`:
    - `OIMUpgrade_online<timestamp>.log`
    - `ant_createUserInSecurityRealm_BISystemUser.log`

- ant\_updateBIPJmsSecurity.log
- ant\_importOwSMPolicySCIM.log
- ant\_create\_UserInSecurityRealm\_BISystemUser.log

---

**Note:** Any customizations done to `setDomainEnv.sh`, `startManagedWeblogic.sh`, and `startWeblogic.sh` will be lost after middle tier online upgrade. These customizations include any changes done to these `.sh` and `.cmd` files manually, that is, without using the WLST templates. Examples of customizations are `tnsnames.ora`, `jvm` or performance arguments, `ssl` parameters and so on.

After middle tier upgrade, you must re-apply the customizations, if any.

---

#### 24.2.4.7 Starting the Oracle Identity Manager Managed Server(s) and the BIP Server

After you upgrade the Oracle Identity Manager middle tier online, you must start the Oracle Identity Manager Managed Server (s) and the BIP Server.

---

**Note:** ■ Before starting the servers, you must add the following property below the `JAVA_PROPERTIES` entry in the `DOMAIN_HOME/bin/setDomainEnv.sh` (on UNIX) or `DOMAIN_HOME/bin/setDomainEnv.cmd` (on Windows) file, to ignore hostname verification:

```
-Dweblogic.security.SSL.ignoreHostnameVerification=true
```

- When you start the Managed Servers for the first time after middle tier upgrade, the servers must be connected to the non-SSL Administration Server port. To do this, complete the following steps:
  1. Before you start the Managed Servers, enable the non-SSL port for the Administration Server.
  2. Ensure that the Managed Servers connect to the non-SSL admin port while starting. For example, if managed server is started using `startManagedWebLogic.sh` script, update the `ADMIN_URL` in this script to use the non SSL url.

These changes can be reverted back once the servers are up.

---

For more information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

#### 24.2.4.8 Changing the Deployment Order of Oracle Identity Manager EAR

If you are upgrading Oracle Identity Manager 11.1.1.x.x environments, change the deployment order of `oim.ear` from 47 to 48. To do this, complete the following steps:

1. Log in to the WebLogic Administration console using the following URL:

```
http://wls_admin_host:wls_admin_port/console
```

2. Click **Deployments** on the left pane.
3. Click **oim.ear**.
4. Update the deployment order from 47 to 48.
5. Click **Save**.

## 24.2.5 Upgrading Other Oracle Identity Manager Installed Components

This section describes how to upgrade other Oracle Identity Manager installed components such as Oracle Identity Manager Design Console and Oracle Identity Manager Remote Manager to 11.1.2.3.0.

This section includes the following sections:

- [Upgrading Oracle Identity Manager Design Console](#)
- [Upgrading Oracle Identity Manager Remote Manager](#)

### 24.2.5.1 Upgrading Oracle Identity Manager Design Console

The Oracle Identity Manager Design Console is used to configure system settings that control the system-wide behavior of Oracle Identity Manager and affect its users. The Design Console allows you to perform user management, resource management, process management, and other administration and development tasks.

Oracle recommends that Oracle Identity Manager and Design Console are installed in different directory paths, if the Design console is on the same system as the Oracle Identity Manager server.

To upgrade Design Console, complete the following steps:

1. Back up the following files:
  - On UNIX, `<XLDC_HOME>/xlclient.sh`
  - `<XLDC_HOME>/config/xlconfig.xml`
  - On Windows, `<XLDC_HOME>\xlclient.cmd`
  - `<XLDC_HOME>\config\xlconfig.xml`
2. Run the Oracle Identity and Access Management 11.1.2.2.0 Installer to upgrade the Design Console home `<XLDC_HOME>`.

For more information, see "Optional: Configuring Oracle Identity Manager Design Console" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

3. Restore the following backed up files in the upgraded Design Console home:

**On UNIX:**

- `xlclient.sh`
- `xlconfig.xml`

**On Windows:**

- `xlclient.cmd`
- `xlconfig.xml`

4. Build and copy the `wlfullclient.jar` file as follows:
  - a. Go to `WebLogic_Home/server/lib` directory on UNIX and `WebLogic_Home\server\lib` directory on Windows.

- b. Set the `JAVA_HOME` environment variable and add the `JAVA_HOME` variable to the `PATH` environment variable. You can set the `JAVA_HOME` to the `jdk160_21` directory inside the Middleware home.

For example:

**On UNIX:** `setenv JAVA_HOME $MW_HOME/jdk160_29`

**On Windows:** `SET JAVA_HOME="MW_HOME\jdk160_29"`

- c. Run the following command to build the `wlfullclient.jar` file:

```
java -jar <MW_HOME>/modules/com.bea.core.jarbuilder_1.7.0.0.jar
```

- d. Copy the `wlfullclient.jar` file to the `<IAM_HOME>` where you installed the Design Console. For example:

**On UNIX:**

```
cp wlfullclient.jar <Oracle_IDM2>/designconsole/ext
```

**On Windows:**

```
copy wlfullclient.jar <Oracle_IDM2>\designconsole\ext
```

5. If the Design Console is SSL enabled, do the following:

- a. Copy the `webserviceclient+ssl.jar` file from the directory `WL_HOME/server/lib/` to the directory `ORACLE_HOME/designconsole/ext/`.
- b. Copy the `cryptoj.jar` file from the directory `MW_HOME/modules/` to the directory `ORACLE_HOME/designconsole/ext/`.
- c. If `DESIGN_CONSOLE_HOME/config/xl.policy` does not contain the default grant policy for all, then add the following permission for `cryptoj.jar` at the end of the `xl.policy` file:

```
grant codeBase "file:DIRECTORY_PATH_TO_cryptoj.jar" {permission
java.security.AllPermission;};
```

6. Open the `xlclient.sh` file (located at `XLDC_HOME/xlclient.sh` on UNIX) or `xlclient.cmd` file (located at `XLDC_HOME\xlclient.cmd` on Windows) in a text editor, and add the following argument to the java command:

```
-DAPPSERVER_TYPE=wls
```

### 24.2.5.2 Upgrading Oracle Identity Manager Remote Manager

Complete the following steps to upgrade Remote Manager:

1. Back up configuration files

Before starting the Remote Manager upgrade, back up the following Remote Manager configuration files:

- On UNIX, `<XLREMOTE_HOME>/remotemanager.sh`
- `<XLREMOTE_HOME>/xlremote/config/xlconfig.xml` file.
- On Windows, `<XLREMOTE_HOME>\remotemanager.bat`
- `<XLREMOTE_HOME>\xlremote\config\xlconfig.xml` file.

2. Run the Oracle Identity and Access Management Installer to upgrade the Remote Manager home.

For more information, see "Installing and Configuring Oracle Identity and Access Management (11.1.2.3.0)" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

3. Restore the following backed up configuration files in the upgraded Remote Manager home.

**On UNIX:**

- remotemanager.sh
- xlconfig.xml

**On Windows:**

- remotemanager.bat
- xlconfig.xml

## 24.2.6 Performing Oracle Identity Manager Post-Upgrade Tasks

This section describes all the post-upgrade tasks applicable for both Oracle Identity Manager 11.1.2.x.x and 11.1.1.x.x upgrade. You must perform the necessary post-upgrade tasks that are relevant to your starting point.

Table 24–12 lists the post-upgrade tasks and the Oracle Identity Manager upgrade starting points that they are applicable for.

**Table 24–12 Post-Upgrade Tasks for Oracle Identity Manager**

Task No	Post-Upgrade Task	Applicable for
1	<a href="#">After You Upgrade</a>	■ 11.1.1.x.x
2	<a href="#">Enabling Oracle BI Publisher</a>	■ 11.1.2.x.x ■ 11.1.1.x.x
3	<a href="#">Reviewing Performance Tuning Recommendations</a>	■ 11.1.2.x.x ■ 11.1.1.x.x
4	<a href="#">Creating PeopleSoft Enterprise HRMS Reconciliation Profile</a>	■ 11.1.2.0.0 ■ 11.1.1.x.x
5	<a href="#">Reviewing OIM Data Purge Job Parameters</a>	■ 11.1.2.x.x ■ 11.1.1.x.x
6	<a href="#">Reconfiguring Lookup Based UDF Field</a>	■ 11.1.2.x.x
7	<a href="#">Reviewing Connector Certification</a>	■ 11.1.2.x.x ■ 11.1.1.x.x
8	<a href="#">Verifying the Functionality of Connectors</a>	■ 11.1.2.x.x ■ 11.1.1.x.x
9	<a href="#">Validating the Database Objects</a>	■ 11.1.1.x.x
10	<a href="#">Impact of Removing Approver-Only Attribute in Request Data Set</a>	■ 11.1.1.x.x
11	<a href="#">Changes to Request API After Upgrading to Oracle Identity Manager 11g Release 2 (11.1.2.3.0)</a>	■ 11.1.1.x.x
12	<a href="#">Verifying the Compatibility of Oracle Identity Manager Integrated with Oracle Access Manager</a>	■ 11.1.1.x.x

**Table 24–12 (Cont.) Post-Upgrade Tasks for Oracle Identity Manager**

<b>Task No</b>	<b>Post-Upgrade Task</b>	<b>Applicable for</b>
13	Running the Entitlement List Schedule	■ 11.1.1.x.x
14	Running the Evaluate User Policies Scheduled Task	■ 11.1.1.x.x
15	Running Catalog Synchronization	■ 11.1.1.x.x
16	UMS Notification Provider	■ 11.1.1.x.x
17	Upgrading User UDF	■ 11.1.1.x.x
18	Upgrading Application Instances	■ 11.1.1.x.x
19	Re XIMDD	■ 11.1.1.x.x
20	Re SPML-DSML	■ 11.1.1.x.x
21	Customizing Event Handlers	■ 11.1.1.x.x
22	Upgrading SOA Composites	■ 11.1.1.x.x
23	Authorization Policy Changes	■ 11.1.1.x.x
24	Creating Password Policies	■ 11.1.1.x.x
25	Migrating Customized Oracle Identity Manager Reports Built on BI Publisher 10g to BI Publisher 11g	■ 11.1.1.x.x
26	Updating the Provider URL For ForeignJNDIPProvider-SOA	■ 11.1.1.x.x
27	Rebuilding the Indexes of Oracle Identity Manager Table to Change to Reverse Type	■ 11.1.2.x.x ■ 11.1.1.x.x
28	Reviewing System Property	■ 11.1.2.x.x ■ 11.1.1.x.x
29	Updating Message Buffer Size for UMSJMSServer	■ 11.1.2.x.x ■ 11.1.1.x.x
30	Changing the Authentication Scheme to TAPScheme After Upgrading Oracle Identity Manager in an OIM-OAM Integrated Environment	■ 11.1.2.x.x
31	Updating the URI of the Human Task Service Component with Oracle HTTP Server Details	■ 11.1.2.x.x ■ 11.1.1.x.x
32	Migrating Approval Policies to Approval Workflow Rules	■ 11.1.2.x.x ■ 11.1.1.x.x
33	Disabling Oracle SOA Suite Server	■ 11.1.2.x.x ■ 11.1.1.x.x
34	Adjusting the Width of UDF Components	■ 11.1.2.x.x ■ 11.1.1.x.x
35	Enabling Certification Using the System Property <code>OIG.IsIdentityAuditorEnabled</code>	■ 11.1.2.x.x
36	Updating the OHS Configuration File After Upgrading OIM 11.1.1.x.x Highly Available Environments	■ 11.1.2.x.x ■ 11.1.1.x.x
37	Observing the UI Changes in the Catalog Page	■ 11.1.2.x.x

### 24.2.6.1 After You Upgrade

After upgrading from Oracle Identity Manager 11.1.1.x.x to Oracle Identity Manager 11.1.2.3.0:

- The name of the following EARs remain unchanged from Oracle Identity Manager 11.1.1.x.x to Oracle Identity Manager 11.1.2.3.0:
  - Oracle Identity Manager Metadata (11.1.1.3.0)
  - Oracle Identity Manager (11.1.1.3.0)

There is no functional loss.

- All of the resources provisioned to an organization in Oracle Identity Manager 11.1.1.x.x is available in **Provisioned Accounts**, after upgrading to Oracle Identity Manager 11.1.2.3.0. To view, go to the following path:
  1. Connect to the Oracle Identity Manager Identity console.
  2. Go to **Administration**.
  3. Select **Organizations**.
  4. Search for organizations.
  5. Select any organization.
  6. Go to **Provisioned Accounts** to see all Oracle Identity Manager 11.1.1.x.x based resources, provisioned to an organization.
- In Oracle Identity Manager 11.1.1.x.x, data object permission was shown in the Administration Console under **Roles**.

In Oracle Identity Manager 11.1.2.3.0, data object permission is not shown.

### 24.2.6.2 Enabling Oracle BI Publisher

In Oracle Identity Manager 11g Release 2 (11.1.2.x.x) and 11g Release 1 (11.1.1.x.x), you would have configured Oracle BI Publisher (BIP) as a standalone product wired to Oracle Identity Manager database. In that case, there would be a separate domain for BIP, where Administration Server and BIP Managed Server(s) are configured. After you upgrade to Oracle Identity Manager 11.1.2.3.0, embedded BIP Server will be enabled by default, and the embedded BIP will be available in the OIM domain, along with the standalone BIP setup.

Therefore, post-upgrade, you have the following two options:

#### Option 1: Using the Embedded BIP

To start using embedded BIP, complete the following steps:

1. Update the BIP URL in Oracle Identity Manager if it is pointing to the standalone BIP or if it is empty. To do this, complete the following steps:
  - a. Log in to Oracle Enterprise Manager using the following URL:
 

```
http://hostname:portnumber/em
```
  - b. Expand **Identity and Access** on the left navigation pane, and then expand **OIM**.
  - c. Right click on **oim(11.1.2.0.0)** and select **System MBean Browser**.
  - d. On the left navigation pane under **System MBean Browser**, expand the following in the same order:

**Application Defined MBeans**



`http://weblogic_host:weblogic_port/console`

- b. In the **Change Center**, click **Lock & Edit**.
- c. In the left navigation pane, expand **Diagnostics** and then click **Context**.
- d. Select the **BIP Server** for which you want to enable diagnostic context.
- e. Select **Enable**.
- f. Click **Activate Changes** to activate the changes.

### Option 2: Using the Existing Standalone BIP

You can retain the existing deployment of Oracle BI Publisher, whose domain is separate from the Oracle Identity Manager. The embedded BIP set up by the upgrade process can be ignored. You can continue to use your existing standalone BIP after upgrade.

To start using your existing standalone BIP, complete the following steps:

1. Copy the new reports available as part of 11.1.2.3.0 (if any) to your existing standalone BIP deployment repository at the following location:

`DOMAIN_HOME/config/bipublisher/repository`

2. Stop the embedded BIP Managed Server (if running).

### 24.2.6.3 Reviewing Performance Tuning Recommendations

After you upgrade to Oracle Identity Manager 11.1.2.3.0, you must review the Oracle Identity Manager specific performance tuning recommendations described in "Oracle Identity Manager Performance Tuning" in the *Oracle Fusion Middleware Performance and Tuning Guide*.

### 24.2.6.4 Creating PeopleSoft Enterprise HRMS Reconciliation Profile

If you are upgrading Oracle Identity Manager 11.1.2 with PeopleSoft connector to Oracle Identity Manager 11.1.2.3.0, you must create PeopleSoft HRMS reconciliation profile after you upgrade to 11.1.2.3.0. For information about creating reconciliation profile, see "Updating Reconciliation Profiles Manually" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

### 24.2.6.5 Reviewing OIM Data Purge Job Parameters

This post-upgrade task is optional.

In Oracle Identity Manager 11g Release 2 (11.1.2.2.0), a unified automated scheduled purge job named **OIM Data Purge Job** was introduced to handle data growth of few modules. This job archive or purges data from the following modules:

- Orchestration
- Reconciliation
- Provisioning Task
- Request

In Oracle Identity Manager 11.1.2.3.0, the modules Orchestration, Reconciliation, and Provisioning Task are enabled by default out of the box. After upgrading to Oracle Identity Manager 11.1.2.3.0, ensure that the modules are set as shown in the following table:

Module Name	Enabled (By Default)
Reconciliation	Y
Orchestration	Y
Provisioning Task	Y
Request	N

To verify that the modules are set correctly, complete the following steps:

1. Log in to the SYSADMIN console using the following URL:  

```
http://OIM_HOST:OIM_PORT/sysadmin
```
2. Select **Scheduler** under **System Configuration** on the left pane.
3. Check for **OIM Data Purge Job** schedule Job.
4. Check if the radio buttons against **Yes** for the modules **Orchestration**, **Reconciliation**, and **Provisioning Task** are selected.

If not, select the radio buttons against **Yes** for the modules **Orchestration**, **Reconciliation**, and **Provisioning Task**, and click **Apply**. Click **Refresh** to ensure that the changes are saved.

The OIM Data Purge Job archives or purges data from modules listed in [Table 24–13](#) with the mentioned purge criteria, by default.

**Table 24–13 Modules and Their Purge Criteria**

Module Name	Enabled (By Default)	Type of Operation	Retention Period	Purge Criteria
Reconciliation	Y	Purge	30 Days	Closed Recon Events
Orchestration	Y	Purge	1 Day	Completed Orchestrations
Provisioning Task	Y	Purge	90 Days	Completed Prov. Task
Request	N	Purge	N/A	N/A

If there is any custom report or logic build on older data, then based on the functional (custom) requirement, amend the Retention Period and Purge Criteria accordingly.

For more information about purge criteria, see "Using the Archival and Purge Utilities for Controlling Data Growth" in the *Oracle Fusion Middleware Administering Oracle Identity Manager*.

For information about the user-configurable attributes, see "Configuring Real-Time Purge and Archival" in the *Oracle Fusion Middleware Administering Oracle Identity Manager*.

#### 24.2.6.6 Reconfiguring Lookup Based UDF Field

If you had User Defined Fields (UDF) of type lookup or drop-down as **outputText** field in your 11.1.2.x.x environment, you will see backend value for that UDF on the **View User Details** page. Therefore, you must complete the following steps to set the right customizations:

1. Log in to the Identity console using the following URL:

`http://host:port/identity`

2. Click **Sandboxes** on the top navigation pane, and then click **Create Sandbox**.
3. Enter the **Sandbox Name** and the **Sandbox Description**. Select the check box **Activate Sandbox**, and then click **Save and Close**. Click **OK** to confirm.
4. Click **Customize** on the top navigation pane.
5. Click **Users** on the left navigation pane, and select the user to open the **User Details** page.
6. Click **Structure** on the top left corner of the console.
7. Select the existing **outputText** field. Click **Delete** to delete this field.
8. Close the customize mode, and publish the sandbox by clicking **Publish Sandbox**.
9. Export the metadata file `userDetailsPageDef.xml` to MDS. The following is the full path to the file to be exported:

```
/oracle/iam/ui/manageusers/pages/mdssys/cust/site/site/userDetailsPageDef.xml
```

The UI modifications should be done via sandbox export/import, which is available in OIM UI. For information about exporting metadata files to MDS, see My Oracle Support document ID 1594327.1 - "How To Export OIM-UI Metadata Using Enterprise Manager".

10. Open the exported file in a text editor.
11. Search for the drop-down or lookup attribute that was added as **outputText**. For example, if the attribute name is `lovattr`, search for a snippet similar to the following:

```
<mds:insert parent="..." position="...">
  <attributeValues IterBinding="..." id="lovattr__c" xmlns="...">
    <AttrNames>
      <Item Value="lovattr__c"/>
    </AttrNames>
  </attributeValues>
</mds:insert>
```

Delete the snippet, that is, delete the lines starting from the `<mds:insert ... >` tag till the `</mds:insert>` tag.

Repeat this step for all drop-down or lookup attributes.

12. Save the file.
13. Import the `userDetailsPageDef.xml` back into the MDS. For information about importing metadata file, see "Importing Metadata Files from MDS" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
14. Log in to the Identity console again.
15. Create another sandbox by clicking **Create Sandbox**. Enter the **Sandbox Name** and the **Sandbox Description**. Select the check box **Activate Sandbox**, and then click **Save and Close**. Click **OK** to confirm.
16. Click **Customize** on the top navigation pane.
17. Click **Users** on the left navigation pane, and select the user to open the **User Details** page.
18. Click **Structure** on the top left corner of the console.

19. Add the LOV drop-down field as **ADF Select one choice (if NON searchable) ' , 'Input list of values (If Searchable picklist)'** to the required section.
20. Select **readonly** on the **Component Properties dialog** box.
21. Close the customize mode, and publish the sandbox by clicking **Publish Sandbox**.

#### 24.2.6.7 Reviewing Connector Certification

Before you upgrade your existing Oracle Identity Manager environments, you must verify if the version of the existing connector is supported for Oracle Identity Manager 11.1.2.3.0. For information about the supported connector versions for Oracle Identity Manager 11.1.2.3.0, refer to the sections "Certified Components" and "Usage Recommendation" in the respective *Connector Guide* in Oracle Identity Manager Identity Connectors Documentation Library.

If you are using 9.x connector or GTC connector, do the following:

- If the 9.x connector that you are using is supported, you can continue to use the existing connector.
- If the 9.x connector is not supported, you must upgrade the existing 9.x connector to the latest 11.x connector after you upgrade the Oracle Identity Manager server to 11.1.2.3.0.
- Verify the data in the `Lookup` populated through lookup reconciliation that the IT Resource Key & IT Resource name is pre-fixed for code & decode respectively. If not, you must upgrade the existing connector to the latest available connector after you upgrade Oracle Identity Manager server.

If you are using 11g connector, the connector upgrade is not required.

#### 24.2.6.8 Verifying the Functionality of Connectors

After you upgrade Oracle Identity Manager to 11.1.2.3.0, complete the following steps to verify the functionality of connectors:

- Verify if Account and Entitlement Tagging are available on the process form. For the connectors to work with Oracle Identity Manager 11.1.2.3.0, you must complete the steps described in the section "Configuring Oracle Identity Manager 11.1.2 or Later" in the respective *Connector Guide*.
- Verify if the customizations made to the connectors are intact.
- Verify if the 11.1.2.3.0 related artifacts like UI Forms and Application Instances are generated.
- Ensure that all the operations of the connectors are working fine.
- If there are two or more IT Resource field in the process form, complete the steps described in the following My Oracle Support note:  
My Oracle Support document ID 1535369.1
- If there are any lookup query fields in the process form of the related connector, then you must customize the UI need to display the same.

#### 24.2.6.9 Validating the Database Objects

If you are using Oracle Database, you must check for the `INVALID` schema objects, and compile them if there are any. To do this, complete the following steps:

1. Identify the `INVALID` schema objects by running the following SQL query as `SYS` user:

```
SELECT owner,object_type,object_name,status FROM dba_objects WHERE
status='INVALID' AND owner in ('<OIM_Schema_Name1>') ORDER BY owner,
object_type, object_name;
```

2. If there are any INVALID schema objects, you must compile them by connecting to the database as SYS user, and running the following from SQL\*Plus:

```
@<$Oracle_Database_Home_Location>/rdbms/admin/utlrp.sql
```

After running the utlrp.sql, run the SQL query described in step-1 to ensure that there are no INVALID Database objects.

#### 24.2.6.10 Impact of Removing Approver-Only Attribute in Request Data Set

Removing approver-only attribute in the Request Data Set results in the following:

- Before upgrade: The requester cannot see attributes approver-only='true', during request submission.

After upgrade: The requester must provide the value during request submission.

- All attributes in the request data sets marked with required=true and approver-only=true should be marked as required=false in the data set.

Make the required fields mandatory in the approver screen through user interface customization.

- For information about attributes in the request data sets marked with required=true, see [Section 24.2.6.17.2, "User Interface Customization for 11.1.1.x.x Mandatory UDF and OOTB Attributes"](#).

- You must manually add LDAP Sync Validation Handler. To do so, complete the following steps:

1. Export the EventHandlers.xml file by running the following WLST offline command:

**On UNIX:**

```
exportAccessData (" /db/ldapMetadata/EventHandlers.xml ")
```

**On Windows:**

```
exportAccessData (" \\db\\ldapMetadata\\EventHandlers.xml ")
```

2. Add the following section of the EventHandlers.xml by editing the file in a text editor. Save the file:

```
<validation-handler
class="oracle.iam.ldapsync.impl.eventhandlers.user.UserCommonNameVa
lidationHandler" entity-type="User" operation="MODIFY"
name="UserCommonNameValidationHandler" order="1005" sync="TRUE">
</validation-handler>
```

```
<validation-handler
class="oracle.iam.ldapsync.impl.eventhandlers.user.UserCommonNameVa
lidationHandler" entity-type="User" operation="CREATE"
name="UserCommonNameValidationHandler" order="1005" sync="TRUE">
</validation-handler>
```

3. Import the EventHandlers.xml file by running the following WLST offline command:

**On UNIX:**

```
importAccessData (" /db/ldapMetadata/EventHandlers.xml ")
```

**On Windows:**

```
importAccessData (" \\db\\ldapMetadata\\EventHandlers.xml ")
```

- You must manually remove the RDN pre-process handler. To do so, complete the following steps:

1. Export the EventHandlers.xml file by running the following WLST offline command:

**On UNIX:**

```
exportAccessData (" /db/ldapMetadata/EventHandlers.xml ")
```

**On Windows:**

```
exportAccessData (" \\db\\ldapMetadata\\EventHandlers.xml ")
```

2. Remove the following section of the EventHandlers.xml by editing the file in a text editor. Save the file:

```
<action-handler
orch-target="oracle.iam.platform.kernel.vo.EntityOrchestration"
class="oracle.iam.ldapsync.impl.eventhandlers.user.RDNPreProcessHan
dler" entity-type="User" operation="CREATE"
name="CreateUserRDNPreProcessHandler" stage="preprocess"
sync="TRUE" order="10000">
```

```
</action-handler>
```

```
<action-handler
orch-target="oracle.iam.platform.kernel.vo.EntityOrchestration"
class="oracle.iam.ldapsync.impl.eventhandlers.user.RDNPreProcessHan
dler" entity-type="User"
operation="MODIFY" name="ModifyUserRDNPreProcessHandler"
stage="preprocess" sync="TRUE" order="10000">
```

```
</action-handler>
```

3. Import the EventHandlers.xml file by running the following WLST offline command:

**On UNIX:**

```
importAccessData (" /db/ldapMetadata/EventHandlers.xml ")
```

**On Windows:**

```
importAccessData (" \\db\\ldapMetadata\\EventHandlers.xml")
```

- If you have any custom validation handlers in your environment, ensure that the validation is re-entrant. For more information, see "Writing Custom Validation Event Handlers" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.
- If you have any custom user name policy configured in your environment, see "Writing Custom User Name Policy" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* to ensure the following:
  - Use the recommended `oracle.iam.identity.usermgmt.api.UserNameGenerationPolicy` interface to implement policy, instead of using `oracle.iam.identity.usermgmt.api.UserNamePolicy`.

- Ensure that Custom User Name policy return is the same user login when the approver updates an attribute that does not contribute in generating user login.

### 24.2.6.11 Changes to Request API After Upgrading to Oracle Identity Manager 11g Release 2 (11.1.2.3.0)

As part of Oracle Identity Manager 11g Release 2 (11.1.2.3.0) architecture, changes are introduced to `RequestService` and `UnauthenticatedRequestService` APIs in terms of usage and in terms of concepts involved. Request Template concept is no longer part of Oracle Identity Manager 11g Release 2 (11.1.2.3.0) and some methods in these APIs are deprecated. Also, `RequestTemplateService` API is completely deprecated.

This section contains the following topics:

- [API Methods Deprecated in RequestService](#)
- [API Methods Deprecated in UnauthenticatedRequestService](#)
- [SELF Request Types Deprecated](#)
- [API Methods That Have Changed in Terms of Usage](#)

**24.2.6.11.1 API Methods Deprecated in RequestService** The following is a list of API methods deprecated in `RequestService`:

- `public List<String> getTemplateName() throws RequestServiceException`
- `public RequestModel getModelForTemplate(String templateName) throws RequestServiceException`
- `public RequestDataSet getRestrictedDataSet(String templateName, String entityType) throws RequestServiceException`
- `public RequestTemplate getTemplate(String templateName) throws RequestServiceException`
- `public void updateApproverOnlyData(String reqId, List<RequestBeneficiaryEntity> benEntities, List<RequestEntity> reqEntities) throws RequestServiceException`
- `public List<String> getTemplateNameForSelf() throws RequestServiceException`
- `public List<RequestTemplate> getRequestTemplates(RequestTemplateSearchCriteria searchCriteria, Set<String> returnAttrs, Map<String, Object> configParams) throws RequestServiceException`

The following is a list of API methods deprecated due to storing comments in SOA Human Task comments feature:

- `public void addRequestComment(String reqId, RequestComment comment) throws RequestServiceException`
- `public List<RequestComment> getRequestComments(String reqId) throws RequestServiceException`
- `public List<RequestComment> getRequestComments(String reqId, RequestComment.TYPE type) throws RequestServiceException`
- `public List<RequestComment> getRequestComments(String reqId, String taskId, RequestComment.TYPE type) throws RequestServiceException`

**24.2.6.11.2 API Methods Deprecated in UnauthenticatedRequestService** The following is a list of API methods deprecated in `UnauthenticatedRequestService`:

- `public List<String> getTemplateName() throws RequestServiceException`
- `public RequestTemplate getTemplate(String templateName) throws RequestServiceException`
- `public RequestDataSet getRestrictedDataSet(String templateName, String entitySubType) throws RequestServiceException`

**24.2.6.11.3 SELF Request Types Deprecated** Request types which were used to perform SELF operations have been deprecated. These operations include the following:

- Self Modify User
- Self Assign Roles
- Self Remove Roles
- Self Provision Resource
- Self De-provision Resource
- Self Modify Resource

You can continue with these operations by using the corresponding non-self request types.

**24.2.6.11.4 API Methods That Have Changed in Terms of Usage** The only method that have changes in usage is `RequestService.submitRequest()/UnauthenticatedRequestService.submitRequest()`. The API method signature remains the same. However, the way `RequestData Value Objects` are created, have changed. The changes are covered in the following sections:

- [Changes to Entity-Type](#)
- [Changes to Value Objects](#)
- [Code Examples](#)

**24.2.6.11.5 Changes to Entity-Type** Changes to entity-type includes the following:

- Resource entity-type is replaced with `Application Instance`.  
Beginning from Oracle Identity Manager 11g Release 2 (11.1.2.3.0), in order to create any provision, revoke, disable, and enable account type of request, the `entityType` property must be set to `ApplicationInstance` instead of `Resource`.
- A new entity-type called `Entitlement` is introduced in Oracle Identity Manager 11g Release 2 (11.1.2.3.0). Oracle Identity Manager supports creating `Provision Entitlement` and `Revoke Entitlement` type of requests.

**24.2.6.11.6 Changes to Value Objects** Changes to value objects, related to `RequestData` includes the following:

- `requestTemplateName` property which was a part of `oracle.iam.request.vo.RequestData` value objects is deprecated. Even if you set this property, it is not honoured.
- A new property called `operation` is introduced in `oracle.iam.request.vo.RequestEntity` and `oracle.iam.request.vo.RequestBeneficiaryEntity` value objects. It is

mandatory to set this property while creating the value objects. You can use the following constants defined in `oracle.iam.request.vo.RequestConstants` class.

- `MODEL_CREATE_OPERATION` – Create User operation
- `MODEL_MODIFY_OPERATION` – Modify User operation
- `MODEL_DELETE_OPERATION` – Delete User operation
- `MODEL_ENABLE_OPERATION` – Enable User operation
- `MODEL_DISABLE_OPERATION` – Disable User operation
- `MODEL_ASSIGN_ROLES_OPERATION` – Assign Roles operation
- `MODEL_REMOVE_ROLES_OPERATION` – Remove Roles operation
- `MODEL_PROVISION_APPLICATION_INSTANCE_OPERATION` – Provision Application Instance operation
- `MODEL_MODIFY_ACCOUNT_OPERATION` – Modify Account operation
- `MODEL_REVOKE_ACCOUNT_OPERATION` – Revoke Account operation
- `MODEL_ENABLE_ACCOUNT_OPERATION` – Enable Account operation
- `MODEL_DISABLE_ACCOUNT_OPERATION` – Disable Account operation
- `MODEL_PROVISION_ENTITLEMENT_OPERATION` – Provision Entitlement operation
- `MODEL_REVOKE_ENTITLEMENT_OPERATION` – Revoke Entitlement operation
- `MODEL_ACCESS_POLICY_PROVISION_APPINSANCE_OPERATION` – Access Policy based provisioning operation

- While creating `RequestEntity` or `RequestBeneficiaryEntity` value objects, you can also use the following method to set the `entityType` property:

```
public void setRequestEntityType(oracle.iam.platform.utils.vo.OIMType
type)

type - OIMType.Role/ OIMType.ApplicationInstance/OIMType.Entitlement/
OIMType.User
```

#### 24.2.6.11.7 Code Examples

Listed below are some code examples:

- Create a `RequestData` for a Create User operation as follows:

```
RequestData requestData = new RequestData("Create User");
requestData.setJustification("Creating User John Doe");
String usr = "John Doe";

RequestEntity ent = new RequestEntity();
ent.setEntityType(RequestConstants.USER);
ent.setOperation(RequestConstants.MODEL_CREATE_OPERATION); //New in R2
List<RequestEntityAttribute> attrs = new ArrayList<RequestEntityAttribute>();

RequestEntityAttribute attr = new RequestEntityAttribute("Last Name", usr,
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("First Name", usr,
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("User Login", usr,
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("Password", "Welcome123",
```

```

RequestEntityAttribute.TYPE.String);
attrs.add(attr);
attr = new RequestEntityAttribute("Organization", 1L,
RequestEntityAttribute.TYPE.Long);
attrs.add(attr);
attr = new RequestEntityAttribute("User Type", false,
RequestEntityAttribute.TYPE.Boolean);
attrs.add(attr);
attr = new RequestEntityAttribute("Role", "Full-Time",
RequestEntityAttribute.TYPE.String);
attrs.add(attr);
ent.setEntityData(attrs);

List<RequestEntity> entities = new ArrayList<RequestEntity>();
entities.add(ent);
requestData.setTargetEntities(entities);

//Submit the request with the above requestData

```

- **Create a RequestData for an Assign Roles operation as follows:**

```

RequestData requestData = new RequestData();

requestData.setJustification("Assigning IDC ADMIN Role(role key 201) to user
with key 121");

RequestBeneficiaryEntity ent1 = new RequestBeneficiaryEntity();
ent1.setRequestEntityType (oracle.iam.platform.utils.vo.OIMType.Role);
ent1.setOperation(oracle.iam.request.vo.RequestConstants.MODEL_ASSIGN_ROLES_
OPERATION); //New in R2
ent1.setEntitySubType("IDC ADMIN");
ent1.setEntityKey("201");

List<RequestBeneficiaryEntity> entities = new
ArrayList<RequestBeneficiaryEntity>();
entities.add(ent1);

Beneficiary beneficiary = new Beneficiary();
beneficiary.setBeneficiaryKey("121");
beneficiary.setBeneficiaryType (Beneficiary.USER_BENEFICIARY);
beneficiary.setTargetEntities(entities);

List<Beneficiary> beneficiaries = new ArrayList<Beneficiary>();
beneficiaries.add(beneficiary);
requestData.setBeneficiaries(beneficiaries);

//Submit the request with the above requestData

```

- **Create a RequestData for a Provision Application Instance operation as follows:**

```

RequestData requestData = new RequestData();

requestData.setJustification("Creating AD User (app instance key 201) account
to user with key 121");

RequestBeneficiaryEntity ent1 = new RequestBeneficiaryEntity();
ent1.setRequestEntityType
(oracle.iam.platform.utils.vo.OIMType.ApplicationInstance);
ent1.setOperation(oracle.iam.request.vo.RequestConstants.MODEL_PROVISION_
APPLICATION_INSTANCE_OPERATION);
ent1.setEntitySubType("AD User");

```

```

ent1.setEntityKey("201");

List<RequestBeneficiaryEntityAttribute> attrs = new
ArrayList<RequestBeneficiaryEntityAttribute>();
//Update 'attrs' above with all the data specific to AD User form.
ent1.setEntityData(attrs);

List<RequestBeneficiaryEntity> entities = new
ArrayList<RequestBeneficiaryEntity>();
entities.add(ent1);

Beneficiary beneficiary = new Beneficiary();
beneficiary.setBeneficiaryKey("121");
beneficiary.setBeneficiaryType(Beneficiary.USER_BENEFICIARY);
beneficiary.setTargetEntities(entities);

List<Beneficiary> beneficiaries = new ArrayList<Beneficiary>();
beneficiaries.add(beneficiary);
requestData.setBeneficiaries(beneficiaries);
//Submit the request with the above requestData

```

- Create a RequestData for a Provision Entitlement operation as follows:

```

RequestData requestData = new RequestData();
Beneficiary beneficiary1 = new Beneficiary();
beneficiary1.setBeneficiaryKey("222");
beneficiary1.setBeneficiaryType(Beneficiary.USER_BENEFICIARY);

RequestBeneficiaryEntity ent1 = new RequestBeneficiaryEntity();
ent1.setEntityType(RequestConstants.ENTITLEMENT);
ent1.setEntitySubType("AD USER ENTITLEMENT1");
ent1.setEntityKey("122");
ent1.setOperation(RequestConstants.MODEL_PROVISION_ENTITLEMENT_OPERATION);

List<RequestBeneficiaryEntity> entities1 = new
ArrayList<RequestBeneficiaryEntity>();
entities1.add(ent1);
beneficiary1.setTargetEntities(entities1);

List<Beneficiary> beneficiaries = new ArrayList<Beneficiary>();
beneficiaries.add(beneficiary1);
requestData.setBeneficiaries(beneficiaries);
//Submit the request with the above requestData

```

### 24.2.6.12 Verifying the Compatibility of Oracle Identity Manager Integrated with Oracle Access Manager

This post-upgrade step is applicable if your starting point is Oracle Identity Manager 11g Release 1 (11.1.1.5.x).

Perform this task if you have integrated Oracle Identity Manager with Oracle Access Manager for single sign-on. Ensure that Oracle Access Manager is at release 11.1.1.5.2 or later.

After upgrading to Oracle Identity Manager 11.1.2.3.0, upgrade Oracle Access Manager configurations for auto-login functionality to work. After upgrading the configurations, NAP protocol is replaced by TAP protocol for communication between Oracle Identity Manager and Oracle Access Manager.

The following topics provide upgrade instructions for two possible scenarios:

- [Using 10g WebGate for Oracle Identity Manager-Oracle Access Manager Integration](#)
- [Using 11g WebGate for Oracle Identity Manager-Oracle Access Manager Integration](#)

Before you begin with the upgrade configuration procedures, refer to the "Using the `idmConfigTool` Command" for more about the **IdmConfigTool** in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

#### 24.2.6.12.1 Using 10g WebGate for Oracle Identity Manager-Oracle Access Manager Integration

If you are using 10g WebGate, complete the following steps to upgrade Oracle Identity Manager and Oracle Access Manager configurations:

1. In the **idmConfigTool**, run `configOAM`. This creates a 10g WebGate agent and an 11g WebGate agent in Oracle Access Manager. Ensure that the artifacts corresponding to both WebGates are created in `<DOMAIN_HOME>/output` directory.
2. In the **idmConfigTool**, run `configOIM`. In a cross-domain setup where Oracle Identity Manager and Oracle Access Manager are in two different WebLogic domains, specify the following additional properties before running this option:
  - `OAM11G_WLS_ADMIN_HOST`: <host name of OAM admin server machine>
  - `OAM11G_WLS_ADMIN_PORT`: <OAM admin server port>
  - `OAM11G_WLS_ADMIN_USER`: <admin user of OAM domain>

---

**Note:** When running the `configOIM` option, ensure that you provide the same properties that you provided in the `configOAM` option for `OAM_TRANSFER_MODE` and `ACCESS_GATE_ID` properties.

The `WEBGATE_TYPE` property should be specified as `ohsWebgate10g`.

---

3. Restart the Administration and Managed Servers. In the case of a cross domain setup, restart servers from both the domains.

Restart the Oracle Identity Manager Administration Server and Managed server as follows:

**On UNIX:**

```
<MW_HOME>/user_projects/domains/domain_name/startWebLogic.sh
```

```
<MW_HOME>/user_projects/domains/domain_
name/bin/startManagedWebLogic.sh <managed_server1>
```

**On Windows:**

```
<MW_HOME>\user_projects\domains\domain_name\startWebLogic.cmd
```

```
MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd
<oim_server>
```

For more information, see "Restarting Servers" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

#### 24.2.6.12.2 Using 11g WebGate for Oracle Identity Manager-Oracle Access Manager Integration

If you are using 11g WebGate, complete the following steps to upgrade Oracle Identity Manager and Oracle Access Manager configurations:

1. In the **idmConfigTool**, run `configOAM`. This creates a 10g WebGate agent and an 11g WebGate agent in Oracle Access Manager. Ensure that the artifacts corresponding to both WebGates are created in the `<DOMAIN_HOME>/output` directory.
2. In the **idmConfigTool**, run `configOIM`. In cross-domain setup where Oracle Identity Manager and Oracle Access Manager are in two different WebLogic domains, specify the following additional properties before running this option:
  - `OAM11G_WLS_ADMIN_HOST`: <host name of OAM admin server machine>
  - `OAM11G_WLS_ADMIN_PORT`: <OAM admin server port>
  - `OAM11G_WLS_ADMIN_USER`: <admin user of OAM domain>

---

**Note:** When running the `configOIM` option, ensure that you provide the same properties that you provided in the `configOAM` option for `OAM_TRANSFER_MODE` and `ACCESS_GATE_ID` properties.

The `WEBGATE_TYPE` property should be specified as `ohsWebgate11g`.

---

3. Restart the Administration and Managed servers. In the case of a cross domain setup, restart servers from both the domains.

Restart the Oracle Identity Manager Administration Server and Managed server as follows:

**On UNIX:**

```
<MW_HOME>/user_projects/domains/domain_name/startWebLogic.sh
```

```
<MW_HOME>/user_projects/domains/domain_
name/bin/startManagedWebLogic.sh <managed_server1>
```

**On Windows:**

```
<MW_HOME>\user_projects\domains\domain_name\startWebLogic.cmd
```

```
MW_HOME\user_projects\domains\domain_name\bin\startManagedWebLogic.cmd
<oim_server>
```

For more information, see "Restarting Servers" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

### 24.2.6.13 Running the Entitlement List Schedule

You must run the Entitlement List Schedule task in order to use catalog features.

Complete the following steps to run the Entitlement List Schedule job:

1. Log in to the SYSADMIN console using the following URL:  
`http://<OIM_HOST>:<OIM_PORT>/sysadmin`
2. Click **System Management**.
3. Select **Scheduler**.
4. Enter "Entitlement List" in the **Search Scheduled Jobs** field and click **Search**.
5. Select **Entitlement List**.
6. Click **Run Now**. Wait till the job is complete.

#### 24.2.6.14 Running the Evaluate User Policies Scheduled Task

You must run the Evaluate User Policies scheduled task to start provisioning based on access policy after the role grant. This scheduled task can be configured to run every 10 minutes, or you can run this scheduled task manually.

To start the scheduler, see "Starting and Stopping the Scheduler" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

#### 24.2.6.15 Running Catalog Synchronization

Resource objects are transformed during the upgrade process. In order to provision the resource of an object, called App instance, with Oracle Identity Manager 11.1.2.3.0, you must run the Catalog Synchronization job.

For more information, see "Bootstrapping the Catalog" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.

---



---

**Note:** If no Entitlements show up, make sure that the entitlements field in the child tables is set to Entitlement=true and reloaded into the parent form.

---



---

#### 24.2.6.16 UMS Notification Provider

This is a new Oracle Identity Manager 11.1.2.3.0 feature for notification. If you want to use this new notification model, after upgrading to 11.1.2.3.0, complete the following steps:

1. Configure E-mail driver from Enterprise Manager user interface:
  - a. Log in to Oracle Enterprise Manager Fusion Middleware Control and do the following:
    - i. Expand **Application Deployments**.
    - ii. Expand **User Messaging Service**.
    - iii. Select **usermessagingdriver-email (<soa\_server1>)**.
    - iv. Select **Email Driver Properties**.
    - v. Select **in Driver-Specific Configuration**.
  - b. Configure the values, as listed in [Table 24-14](#):

**Table 24-14 UMS Parameters and Description**

Parameter	Description
OutgoingMailServer	Name of the SMTP server. For example: abc.example.com
OutgoingMailServerPort	Port of the SMTP server. For example: 456
OutgoingMailServerSecurity	The security setting used by the SMTP server Possible values can be None/TLS/SSL.

**Table 24–14 (Cont.) UMS Parameters and Description**

Parameter	Description
OutgoingUsername	Provide a valid username. For example: abc.eg@example.com
OutgoingPassword	Complete the following: <ol style="list-style-type: none"> <li>1. Select <b>Indirect Password</b>. Create a new user.</li> <li>2. Provide a unique string for indirect <b>Username/Key</b>. For example: OIMEmailConfig. This mask the password and prevent it from exposing it in cleartext, in the config file.</li> <li>3. Provide valid password for this account.</li> </ol>

2. Configure the Notification provider XML through the Enterprise Manager user interface:
  - a. Log in to Enterprise Manager and do the following:
    - i. Expand **Application Deployments**.
    - ii. Select **OIMAppMetadata(11.1.1.3.0)(oim\_server1)** and right-click.
    - iii. Select **System MBean Browser**.
    - iv. Expand **Application Defined MBeans**.
    - v. Expand **oracle.iam**.
    - vi. Expand **Server\_OIM\_Server1**
    - vii. Expand **Application: oim**.
    - viii. Expand **IAMAppRuntimeMBean**.
    - ix. Select **UMSEmailNotificationProviderMBean**.
  - b. Configure the values, as listed in [Table 24–15](#):

**Table 24–15 Parameter for Configuring Notification Provider**

Parameter	Description
Web service URL	Start the URL of UMS web service. Any SOA server can be used. For example: http://<SOA_host>:<SOA_Port>/ucs/messaging/webservice
Policies	The OWSM Policy is attached to the given web service, leave it blank.
Username	The username is given in the security header of web service. If there is no policy attached, leave it blank.
Password	The password given in the security header of web service. If there is no policy attached, leave it blank.

After upgrading to 11.1.2.3.0, if you want to use SMTP notification provider instead of the default UMS notification provider, do the following:

1. Log in to Enterprise Manager and do the following:
  - a. Expand **Application Deployments**.

- b. Select **OIMAppMetadata(11.1.1.3.0)(oim\_server1)** and Right click.
  - c. Select **System MBean Browser**.
  - d. Expand **Application Defined MBeans**.
  - e. Expand **oracle.iam**.
  - f. Expand **Server\_OIM\_Server1**
  - g. Expand **Application: oim**.
  - h. Expand **IAMAppRuntimeMBean**.
  - i. Select **UMSEmailNotificationProviderMBean**.
2. Ensure that the value of the attribute `Enabled` is set to `true`.
  3. Provide the configuration values in MBean (`username`, `password`, `mailServerName`) or the name of IT Resource in MBean.

The IT Resource name is the name given in `XL.MailServer` system property, before you upgrade Oracle Identity Manager 11.1.1.x.x to Oracle Identity Manager 11.1.2.3.0.

#### 24.2.6.17 Upgrading User UDF

You must have UDF in your environment because if you do not update your User Interface with UDFs, several features like user creation, role creation, and self registration request where UDFs are involved fails.

This section contains the following topics:

- [Rendering the UDFs](#)
- [User Interface Customization for 11.1.1.x.x Mandatory UDF and OOTB Attributes](#)
- [Lookup Query Modification](#)

**24.2.6.17.1 Rendering the UDFs** For an Oracle Identity Manager 11.1.2.3.0 environment that has been upgraded from Oracle Identity Manager 11.1.1.x.x, the custom attributes for user entity already exist in the back-end. These attributes are not present as form fields on the Oracle Identity Manager 11.1.2.3.0 user interface screens until the user screens are customized to add the custom fields.

However, before you can customize the screens, you must first complete upgrading the custom attributes using the Upgrade User Form link in the System Administration console.

After completing the Upgrade User Form, the User value object (VO) instances in various Data Components like DataComponent-Catalog, DataComponent-My Information, DataComponent-User Registration shows the custom attributes. This includes all custom attributes available for Web Composer (Customized) and can be added to User user interface screens.

For more information, see "Customizing the Interface" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

Complete the following steps to render UDFs:

1. Log in to the **Identity System Administration** console.
2. Click **Sandboxes**. Click **Create Sandbox**. A Create Sandbox window appears.
3. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
4. Go to **Upgrade**. Select **Upgrade User Form**. Click **Upgrade Now**.

---

**Note:** If an error message is displayed after clicking **Upgrade Now** button, it is important that you analyze the error. You must also export the Sandbox for analysis and then discard (Delete) the sandbox. This note also applies to **Upgrade Role Form** and **Upgrade Organization Form**.

---

5. Publish the Sandbox.
6. Log out from Identity System Administration console.
7. Log in to **Identity Self Service** console.
8. Click **Create Sandbox**. A **Create Sandbox** window appears.
9. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
10. From the left navigation pane, select **Users**.
11. Click **Create User**. A **Create User** page opens. Fill up all the mandatory fields. Add the same UDFs in **Modify User** and **User Detail** screen. Select the correct **Data Component** and **UserVO Name** as listed in [Table 24–16](#).

For example:

From the left navigation pane, click **Users**. Click **User** to go to the **Create User** screen and fill all mandatory fields.

12. Click **Customize** on top right. Select **View**. Select **Source**.
13. Select **Name** in **Basic Information** and click **Edit** on the confirmation window.
14. Select **panelFormLayout**. Click **Add Content**.
15. Select the correct **Data Component** and **VO Name** as listed in [Table 24–16](#):

**Table 24–16** *UDF Screens and Description*

Screen Name	Data Component	VO Name	Procedure
Create User	Data Component - Catalog	UserVO	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>User</b>.</li> <li>2. Click <b>Create</b>, it launches the <b>Create User</b> screen.</li> </ol>
Modify User	Data Component - Catalog	UserVO	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>User</b> and search.</li> <li>2. Select a single user from search results.</li> <li>3. Click <b>Edit</b>, it launches the <b>Modify User</b> screen.</li> </ol>
View User Details	Data Component - Manage Users	UserVO1	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>User</b> and search.</li> <li>2. Select a single user from search results.</li> </ol>
Bulk Modify User Flow	Data Component - Catalog	UserVO	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>User</b> and search.</li> <li>2. Select more than a single user from search results.</li> </ol>

**Table 24–16 (Cont.) UDF Screens and Description**

Screen Name	Data Component	VO Name	Procedure
My Information	Data Component - My Information	UserVO1	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>Identity</b>.</li> <li>2. Select the <b>My Information</b> sub-tab.</li> </ol>
Customizing Search Results	Data Component - Manage Users	UserVO1	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>Identity</b>.</li> <li>2. Click <b>Users</b>.</li> <li>3. Click <b>Customizations</b>, it opens the <b>Web Composer</b>.</li> </ol>
User Registration	Data Component - User Registration	UserVO1	Do the following: <ol style="list-style-type: none"> <li>1. Click <b>Customize</b> to open <b>Web Composer</b>.</li> <li>2. Enable the left navigation links for unauthenticated pages.</li> <li>3. Click <b>User Registration</b>.</li> <li>4. Select <b>User Registration</b>.</li> </ol>
Adding UDF in Search Panel	NA	NA	Do the following: <ol style="list-style-type: none"> <li>1. Log in to Identity</li> <li>2. Click <b>User</b>.</li> <li>3. Search for "Add Fields" in the search box. It shows all searchable fields to the user.</li> </ol>
Customizing Request Summary/Details	NA	NA	Requests created after Create User, Modify User, My Information, Self Registration.

16. Click **Close**.

17. Click **Sandboxes**. Export the sandbox using **Export Sandbox**.

18. Publish the sandbox.

19. Log out from **Identity Self Service**, and log in again. The added UDF in the screen is seen.

---

**Note:** You can upgrade and customize Role UDF and Organization UDF by following the instructions described in the table "Entities and Corresponding Data Components and View Objects" in the *Oracle Fusion Middleware Administering Oracle Identity Manager*.

---

**24.2.6.17.2 User Interface Customization for 11.1.1.x.x Mandatory UDF and OOTB Attributes** If you have rendered the OOTB attributes as mandatory in Oracle Identity Manager 11.1.1.x.x, you must customize the user interface in order to achieve the same customizations after upgrade.

1. Log in to **Identity System Administration** console.
2. Click **Sandboxes**. Click **Create Sandbox**. A Create Sandbox window appears.

3. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
4. Go to **Upgrade**. Select **Upgrade User Form**. Click **Upgrade Now**.
5. Publish the Sandbox.
6. Log out from Identity System Administration console.
7. Log in to **Identity Self Service** console.
8. Click **Create Sandbox**. A **Create Sandbox** window appears.
9. Enter the **Sandbox Name**. Select **Activate Sandbox**. Click **Save and Close**.
10. From the left navigation pane, click **Users**. Click **User** to go to the **Create User** screen and fill all the mandatory fields.
11. Click **Customize** on top right. Select **View**. Select **Source**.
12. Select **Name** in **Basic Information** and click **Edit** on the confirmation window.
13. Select **panelFormLayout**. Click **Add Content**.
14. Click **Input Component** and click **Edit**.
15. On the Component Properties dialogue, select **Show Required** check box. In the Required field, select **Expression Editor**, and in the **Expression Editor** field, enter the value as **true**.
16. Click **Close**.
17. Click **Sandboxes**. Export the sandbox using **Export Sandbox**.
18. Publish the sandbox.
19. Log out from **Identity Self Service**, and log in again. The added UDF on the screen with an asterix (\*) symbol is seen.

**24.2.6.17.3 Lookup Query Modification** In user customization upgrade, multiple values for the Save Column may exist in `User.xml`. Based on the possible values; single, multiple, and null, do the following in the upgraded environment:

- Use `Single` value for Save Column: User creation is successful, and the value of the field is also saved in database.
- Use `Multiple` or `NULL` value for Save Column: User creation is successful, but the value is not saved in database.

---

**Note:** Lookup by Query is not supported in the Oracle Identity Manager 11g Release 2 (11.1.2) and later releases. Therefore, if your starting point is Oracle Identity Manager 11.1.1.x.x, you must change Lookup by Query to Lookup by Code, post upgrade. If you do not perform this task, the Lookup by Query will be a text field in 11.1.2.3.0.

---

### 24.2.6.18 Upgrading Application Instances

After you complete the upgrade, you must complete the following steps to upgrade Application Instances:

1. Log in to the following console:  

```
http://<OIM_HOST>:<OIM_PORT>/sysadmin
```
2. Expand **Upgrade** on the left navigation pane.

**3. Click Upgrade Application Instances.**

This creates the U/I Forms and Datasets for the Application Instances, and seeds to MDS.

**24.2.6.19 Re XIMDD**

---

---

**Note:** This section is required only if the Diagnostic Dashboard services for AD Password Sync were deployed in 11.1.1.x.x and if your application is deployed in staging mode in 11.1.1.x.x.

---

---

Before you can re-deploy, you must undeploy XIMDD from the 11.1.1.x.x Oracle Identity Manager Managed Server or from the cluster. To do so, complete the following steps:

1. Log in to the WebLogic Server Administration console:  
host:admin port/console
2. If you are running in production mode, click **Lock and Edit**.
3. Click **Deployments**.
4. In the resulting list, look for **XIMDD**.
5. If they are running, select **XIMDD**.
6. Click **Delete**.
7. Activate the changes.

To redeploy, complete the following steps:

1. Log in to the WebLogic Server Administration console:  
host:admin port/console
2. Click **Lock & Edit**.
3. Click **Deployments**.
4. Click **Install**.
5. In the path, provide the path for XIMDD.ear.  
The default path is in the following location:  
On UNIX, \$<OIM\_HOME>/server/webapp/optional  
On Windows, <OIM\_HOME>\server\webapp\optional
6. Select **XIMDD.ear**. Click **Next**.
7. Select **Install this deployment as an application**. Click **Next**.
8. In **Select deployment targets** page, select **oim server**. Click **Next**.
9. In the **Optional Setting** page, click **Finish**.
10. Click **Deployments**.
11. Select **XIMDD**. Click **Start**.
12. From the options, select **Service All Requests**.

### 24.2.6.20 Re SPML-DSML

---

**Note:** This section is required only if the DSML web services for AD Password Sync were deployed in 11.1.1.x.x.

---

Before you can redeploy, you must undeploy SPML-DSML from the 11.1.1.x.x Oracle Identity Manager Managed Server or from the cluster. To do so, complete the following steps:

1. Log in to the WebLogic Server Administration console:  
     `host:admin port/console`
2. If you are running in production mode, obtain the Lock in order to make updates.
3. Click **Deployments**.
4. In the resulting list, look for **spml**.
5. If they are running, select **spml**.
6. Click **Delete**.
7. Activate the changes.

To redeploy, complete the following steps:

1. Log in to WebLogic Server Administration console through the following path:  
     `host:admin port/console`
2. Click **Lock & Edit**.
3. Click **Deployments**.
4. Click **Install**.
5. In the path provide the path for spml.ear.  
     The default path is in the following location:  
     On UNIX, `<OIM_HOME>/server/apps`  
     On Windows, `<OIM_HOME>\server\apps`
6. Select **spml-dsml.ear**. Click **Next**.
7. Select **Install this deployment as an application**. Click **Next**.
8. In **Select deployment targets** page, select **oim server**. Click **Next**.
9. In the **Optional Setting** page, click **Finish**.
10. Click **Deployments**.
11. Select **spml**. Click **Start**.
12. From the options, select **Service All Requests**.

### 24.2.6.21 Customizing Event Handlers

If you have used any event handlers in Oracle Identity Manager 11.1.1.x.x, you must re-customize the event handler for Oracle Identity Manager 11.1.2.3.0.

For more information, see "Developing Custom Event Handlers" in the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

### 24.2.6.22 Upgrading SOA Composites

If your starting point is Oracle Identity Manager 11.1.1.x.x, you must manually upgrade custom composites that you have built. Complete the following steps to upgrade SOA composites:

1. Open the SOA composite project in JDeveloper (Use Jdeveloper 11.1.1.9.0).
2. Open `ApprovalTask.task` file in designer mode.
3. Select **General**.
4. Change **Owner** to **Group, SYSTEM ADMINISTRATORS, STATIC**.
5. Select **Outcomes lookup**. An **Outcomes Dialog** opens.
6. Select **Outcomes Requiring Comment**.
7. Select **Reject** and click **Ok**.
8. Click **Ok** again.
9. Select **Notification**.
10. Click on the update icon under **Notification**. Update any old URLs in notification with the corresponding new URL in 11.1.2.3.0. An example notification content is given below:

```
A <%/task:task/task:payload/task:RequestModel%> request has been assigned to
you for approval. <BR><BR>
Request ID: <%/task:task/task:payload/task:RequestID%> <BR>
Request type: <%/task:task/task:payload/task:RequestModel%> <BR>
<BR>
Access this task in the
<A
style="text-decoration: none; "
href=<%substring-before(/task:task/task:payload/task:url,
"/workflowservice/CallbackService")%>/identity/faces/home?tf=approval_details
>
Identity Self Service
</A>
application or take direct action using the links below. Approvers are
required to provide a justification when rejecting the request
```

11. Click **Advanced**.
12. Deselect **Show worklist/workspace URL in notifications**. Provide the URL to Pending Approvals in identity application as shown in the example in step 10.
13. Repeat step 1 to 12 for other human tasks, if any, in the composite. Save your work.
14. Right click **Project** and select **Deploy -> Deploy to Application Server**.
15. Provide revision ID. Select **Mark revision as default** and **Overwrite any existing composite with same revision ID**.

---



---

**Note:** You can also deploy the composites with different revision ID. In that case you have to modify all approval policies using this composite.

---



---

16. Select your application server connection, if it already exists, and click **Next**. Create an application server connection if it does not exist.

17. Click **Next**.
18. Click **Finish**.
19. Repeat the procedure for the remaining custom composites.

### 24.2.6.23 Authorization Policy Changes

If you have custom Authorization Policies in Oracle Identity Manager in 11g Release 1 (11.1.1.5.0), in order to create or modify users, you must assign new administrator roles in relation to User Administration, Role Administration, or Help Desk.

Table 24–17 lists the Administration roles in Oracle Identity Manager 11g, either removed or consolidated into the System Administrator Administration role for all system administrative operations in Oracle Identity Manager 11.1.2.3.0:

**Table 24–17 Changes in Role from Oracle Identity Manager 11g to 11.1.2.3.0**

SI No.	Roles in Oracle Identity Manager 11g	Roles Removed and Replaced in Oracle Identity Manager 11.1.2.3.0
1	SCHEDULER ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
2	DEPLOYMENT MANAGER ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
3	NOTIFICATION TEMPLATE ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
4	SOD ADMINISTRATORS	Removed and replaced with SYSTEM ADMINISTRATORS.
5	SYSTEM CONFIGURATION ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
6	GENERATE_USERNAME_ROLE	Removed and replaced with SYSTEM ADMINISTRATORS.
7	IDENTITY USER ADMINISTRATORS	Removed and replaced with USER ADMIN.
8	USER CONFIGURATION ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
9	ACCESS POLICY ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
10	RECONCILIATION ADMINISTRATORS	Removed and replaced with SYSTEM ADMINISTRATORS.
11	RESOURCE ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
12	GENERIC CONNECTOR ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
13	APPROVAL POLICY ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
14	REQUEST ADMINISTRATORS	Removed and replaced with SYSTEM ADMINISTRATORS.
15	REQUEST TEMPLATE ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
16	PLUGIN ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.
17	ATTESTATION CONFIGURATION ADMINISTRATORS	Removed and replaced with SYSTEM CONFIGURATORS.

**Table 24–17 (Cont.) Changes in Role from Oracle Identity Manager 11g to 11.1.2.3.0**

<b>SI No.</b>	<b>Roles in Oracle Identity Manager 11g</b>	<b>Roles Removed and Replaced in Oracle Identity Manager 11.1.2.3.0</b>
18	ATTESTATION EVENT ADMINISTRATORS	Removed and replaced with SYSTEM ADMINISTRATORS.
19	ROLE ADMINISTRATORS	Removed and replaced with ROLE ADMIN.
20	USER NAME ADMINISTRATOR	Removed and now depends on administration roles.
21	IDENTITY ORGANIZATION ADMINISTRATORS	Removed and replaced with ORGANIZATION ADMIN.
22	IT RESOURCE ADMINISTRATORS	Removed and replaced with APPLICATION INSTANCE ADMIN.
23	REPORT ADMINISTRATORS	No link to reports from Oracle Identity Manager.
24	SPML_APP_ROLE	There is no change in this enterprise role and a corresponding role with the privileges is seeded in Oracle Entitlements Server.
25	ALL USERS	This is an enterprise role, not an administrator role.
26	SYSTEM CONFIGURATORS	All privileges as System Administrator role, except for the ability to manage Users, Roles, Organizations and Provisioning remains unchanged.
27	SYSTEM ADMINISTRATORS	Remains unchanged.

#### 24.2.6.24 Creating Password Policies

When you upgrade Oracle Identity Manager 11.1.1.x.x to 11.1.2.3.0, a default password policy will be seeded at the TOP organization. As a result, any password policy rules created using the older password policy model in Oracle Identity Manager 11.1.1.x.x environment will not be supported. The upgrade utility does not migrate the password policies of Oracle Identity Manager 11.1.1.x.x to 11.1.2.3.0. If you had made any password policy customizations on the older password policy rules, you must create equivalent password policies using the newer password policy model, and attach it to the respective organization.

For information about creating password policies, see "Password Policy Management" in the *Oracle Fusion Middleware Administering Oracle Identity Manager*.

#### 24.2.6.25 Migrating Customized Oracle Identity Manager Reports Built on BI Publisher 10g to BI Publisher 11g

Customized reports built on Oracle BI Publisher 10g Release 3 (10.1.3.X) or later must be upgraded before they can be consumed by Oracle BI Publisher 11.1.1.7.1. You must use the Upgrade Assistant to upgrade the reports in the BI Publisher 10g repository. For more information, see "Task 5: Upgrade the BI Publisher Repository" in the *Oracle Fusion Middleware Upgrade Guide for Oracle Business Intelligence*.

### 24.2.6.26 Updating the Provider URL For ForeignJNDIProvider-SOA

If the environment is running in SSL mode, you must change the **Provider URL** for **ForeignJNDIProvider-SOA** to SSL Provider URL. To do this, complete the following steps:

1. Log in to the WebLogic Administration console using the following URL:  
`http://weblogic_host:weblogic_port/console`
2. Expand **Services** under **Domain Structure**.
3. Click **Foreign JNDI Providers**.
4. Click **ForeignJNDIProvider-SOA** to bring up the **Settings for ForeignJNDIProvider-SOA** page.
5. Click **Lock & Edit** on the top-left pane.
6. In **Provider URL**, change **t3** to **t3s**.
7. Click **Save**, and then click **Activate Changes**.

### 24.2.6.27 Rebuilding the Indexes of Oracle Identity Manager Table to Change to Reverse Type

For high concurrent load conditions in Oracle Identity Manager, the following indexes if altered as reverse key indexes, will give better performance. These indexes are mainly on Primary columns and unique columns of the OIM table.

#### List of Indexes:

- UK\_PCQ
- PK\_PCQ
- PK\_SCH
- PK\_ORC
- PK\_OSH
- PK\_USR
- PK\_OSI
- IDX\_OIU\_ORC\_KEY
- PK\_AUD\_JMS
- IDX\_UPA\_UD\_FORFIE\_FORMS\_KEY
- PK\_UPA\_UD\_FORMFIELDS
- PK\_UPA\_FIELDS
- IDX\_UPA\_FIELDS\_UPA\_USR\_KEY
- IDX\_UPA\_UD\_FOR\_UPA\_RES\_KEY

To alter the index, execute the following SQL statement for each of the indexes:

```
SQL> ALTER INDEX <index_name> REBUILD REVERSE;
```

It is recommended that you perform this task in Oracle Identity Manager downtime window.

To verify that the indexes were rebuilt successfully, check the `index_type` column value of these indexes from the database data dictionary view `DBA_INDEXES` (from `SYS`

schema) or from `USER_INDEXES` (from OIM DB schema). The `index_type` of these indexes should be `NORMAL/REV`.

#### 24.2.6.28 Reviewing System Property

After you upgrade Oracle Identity Manager to 11.1.2.3.0, review the system property `Allowed Back URLs` and verify if it is set to the correct value.

For information about searching and modifying system properties, see "Managing System Properties" in the *Oracle Fusion Middleware Administering Oracle Identity Manager*.

#### 24.2.6.29 Updating Message Buffer Size for UMSJMSServer

If the Message Buffer Size for UMSJMSServer is missing in the upgraded environment, you can update it by doing the following:

1. Log in to the WebLogic Administration Console using the following URL:  
`http://host:port/console`
2. Click **Services** under **Domain Structure** on the left navigation pane.
3. Click **Messaging** and then click **JMS Servers**.
4. Click **UMSJMServer** and then click **Lock and Edit**.
5. Update the value of **Message Buffer Size** to **200**.

---

---

**Note:** If the value of **Message Buffer Size** is -1, the size will be managed automatically.

---

---

6. Click **Save** to activate the changes.

#### 24.2.6.30 Changing the Authentication Scheme to TAPScheme After Upgrading Oracle Identity Manager in an OIM-OAM Integrated Environment

If you have upgraded Oracle Identity Manager in an Oracle Identity Manager, Access Manager, and Oracle Adaptive Access Manager integrated environment, change the Authentication Scheme from `LDAP Scheme` to `TAPScheme` for both `Protected HigherLevel` and `Protected LowerLevel` Policies under the IAM Suite domain. For more information, see "Changing the Authentication Scheme to TAPScheme for Upgrade of Oracle Identity Manager" in the *Oracle Fusion Middleware Integration Guide for Oracle Identity Management Suite*.

#### 24.2.6.31 Updating the URI of the Human Task Service Component with Oracle HTTP Server Details

This step is for Oracle HTTP Server (OHS) enabled environment, and is applicable for Oracle Identity Manager 11.1.1.x.x, 11.1.2, and 11.1.2.1.0 starting points.

While configuring Oracle Identity Manager 11.1.2.1.0, 11.1.2, or 11.1.1.x.x, if you had specified OIM server host and port for `OIM HTTP URL`, then for all composites deployed, you must complete the following steps after upgrading Oracle Identity Manager to 11.1.2.3.0:

1. Update the task URI information to point to the OHS host and port. For more information, see "Managing the URI of the Human Task Service Component Task Details Application" in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*.

2. Specify the OHS details in the DiscoverConfig MBean by doing the following:
  1. Log in to the Oracle Enterprise Manager Fusion Middleware Control using the following URL:
 

```
http://host:port/em
```
  2. Navigate to **OIMDomain**, right-click on it, and click **System MBean Browser**.
  3. Click the search icon, enter **DiscoveryConfig**, and click **Search**.
  4. Set the value of the **OimExternalFrontEndURL** property to:
 

```
http://OHS_HOST:OHS_PORT
```
  5. Save the changes.

#### 24.2.6.32 Migrating Approval Policies to Approval Workflow Rules

After upgrading to Oracle Identity Manager 11.1.2.3.0, the approval policies will continue to work. However, you also have an option of enabling the approval workflow introduced in 11.1.2.3.0, and migrating the approval policies to approval workflow policies.

---

**Note:** Once you enable workflow policies, the approval policies will be disabled permanently

---

For information about enabling approval workflow rules, see "Enabling the Approval Workflow Rules Feature" in the *Oracle Fusion Middleware Administering Oracle Identity Manager*.

#### 24.2.6.33 Disabling Oracle SOA Suite Server

After upgrading to Oracle Identity Manager 11.1.2.3.0, you can choose to disable Oracle SOA Suite (SOA) server, if required. If you do so, the Oracle Identity Manager features that are dependent on SOA will not be available.

For information about disabling SOA server, see "Disabling SOA Server" in the *Oracle Fusion Middleware Administering Oracle Identity Manager*.

#### 24.2.6.34 Adjusting the Width of UDF Components

If you had added User Defined Fields (UDF) to page(s) in Oracle Identity Manager 11.1.2.x.x or 11.1.1.x.x pre-upgrade, you would have updated the display width of the UDF components (for example, `inputText`, `inputListOfValues`) to fit them in a page. This display width is not preserved post-upgrade. Therefore, you must adjust the width of the UDF components post-upgrade. To do this, complete the following steps:

1. Log in to the Identity console using the following URL:
 

```
http://host:port/identity
```
2. Click **Sandboxes** on the top navigation pane, and then click **Create Sandbox**.
3. Enter the **Sandbox Name** and the **Sandbox Description**. Select the check box **Activate Sandbox**, and then click **Save and Close**. Click **OK** to confirm.
4. Open the page that needs to be adjusted.
5. Click **Customize**.
6. Switch to **Structure** mode.

7. Select the component that needs to be adjusted.
8. Open Component Properties.
9. Set the value of the **Columns** property. For example, you can set it to 20.
10. Verify the changes, and click **Publish** to publish the sandbox.

### 24.2.6.35 Enabling Certification Using the System Property `OIG.IsIdentityAuditorEnabled`

If you had enabled certification in Oracle Identity Manager 11g Release 2 (11.1.2.2.0) or 11g Release 2 (11.1.2.1.0) using the system property "Display Certification or Attestation" (`OIM.ShowCertificationOrAttestation`), you must re-enable the certification using the new system property "Identity Auditor Feature Set Availability" (`OIG.IsIdentityAuditorEnabled`) after upgrading to Oracle Identity Manager 11.1.2.3.0.

To re-enable the certification, set the system property "Identity Auditor Feature Set Availability" (`OIG.IsIdentityAuditorEnabled`) to `TRUE` post-upgrade.

### 24.2.6.36 Updating the OHS Configuration File After Upgrading OIM 11.1.1.x.x Highly Available Environments

After you upgrade Oracle Identity Manager 11g Release 1 (11.1.1.7.0) or 11g Release 1 (11.1.1.5.0) highly available environments, you must update the Oracle HTTP Server (OHS) configuration file `mod_wl_ohs.conf`, as the web context used through OHS to access self-service and `sysadmin` have changed in 11.1.2.3.0. To do this, complete the following steps:

1. Open the `mod_wl_ohs.conf` file in an editor.
2. Remove the `/oim` location. The following is an example of `/oim` location:

```
<Location /oim>
  SetHandler weblogic-handler
  WLCookieName oimjessionid
  WebLogicCluster OIMHOST1:OIMHOST1_Port,OIMHOST2:OIMHOST2_Port
  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
  WProxySSL ON
  WProxySSLPassThrough ON
</Location>
```

3. Add the locations for `/identity` and `/sysadmin` as shown in the following example:

```
<Location /identity>
  SetHandler weblogic-handler
  WLCookieName oimjessionid
  WebLogicCluster OIMHOST1:OIMHOST1_Port,OIMHOST2:OIMHOST2_Port
  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
  WProxySSL ON
  WProxySSLPassThrough ON
</Location>
```

```
<Location /sysadmin>
  SetHandler weblogic-handler
  WLCookieName oimjessionid
  WebLogicCluster OIMHOST1:OIMHOST1_Port,OIMHOST2:OIMHOST2_Port
  WLogFile "${ORACLE_INSTANCE}/diagnostics/logs/mod_wl/oim_component.log"
  WProxySSL ON
  WProxySSLPassThrough ON
```

</Location>

### 24.2.6.37 Observing the UI Changes in the Catalog Page

For the new applications created in 11.1.2.3.0 and for some of the application which were created before the upgrade, **Update** button is seen in place of **Ready to Submit** button on the **Catalog** page. This is a design level change made in 11.1.2.3.0. **Update** button is a replacement for **Ready to Submit** button.

For some of the existing applications which were created pre-upgrade, both **Ready to Submit** and **Update** buttons appear on the Catalog page. For such cases, create a new version of the form for their respective resource types. This removes the **Ready to Submit** button.

### 24.2.6.38 oimclient.jar Needs Update and ipf.jar for Some passwordmgmt VOs

Custom client applications using the previous version of the oimclient.jar will get an error similar to the following: "oracle.iam.passwordmgmt.vo.Challenge; local class incompatible: stream classdesc serialVersionUID = 7026677945288353246, local class serialVersionUID = -5258470952025280257"

To resolve this issue, update the client application to use the new version of the oimclient.jar included with this release in OIM\_ORACLE\_HOME/server/client/oimclient.zip, and include the additional OIM\_ORACLE\_HOME/modules/oracle.idm.ipf\_11.1.2/ipf.jar in the lib/classpath.

## 24.3 Oracle Access Management Specific Topics

This section includes the topics common to various Oracle Access Manager upgrade starting points. This section contains the following topics:

- [Extending the 11.1.2.3.0 Access Manager Domain to Include Mobile Security Suite and Policy Manager](#)
- [Enabling Oracle Mobile Security Suite](#)
- [Upgrading Oracle Access Management Identity Federation](#)

### 24.3.1 Extending the 11.1.2.3.0 Access Manager Domain to Include Mobile Security Suite and Policy Manager

You must extend the Access Manager WebLogic domain to use Oracle Mobile Security Suite and Policy Manager features available with Access Manager 11.1.2.3.0.

In case of a highly available Oracle Access Management setup, follow the instructions described in "Configuring Oracle Mobile Security Manager on OAMHOST1" in the *Oracle Fusion Middleware High Availability Guide*, to extend the Access Manager WebLogic domain to include Oracle Mobile Security Suite and Policy Manager.

In case of a single node Oracle Access Management setup, complete the following steps to extend the Access Manager WebLogic domain to include Oracle Mobile Security Suite and Policy Manager:

1. Create the Oracle Mobile Security Manager (OMSM) schema using the Repository Creation Utility 11.1.1.9.0, if you have not done already.

For information about creating schemas, see [Section 24.1.3, "Creating Database Schemas Using Repository Creation Utility"](#).

2. Ensure that you have stopped the WebLogic Administration Server and the Access Manager Managed Server(s).

For information about stopping the servers, [Section 24.1.9, "Stopping the Servers"](#).

3. Start the Oracle Fusion Middleware Configuration Wizard by running the following command from the location `WL_HOME/common/bin`:

On UNIX: `./config.sh`

---

---

**Note:** OMSS is not supported on Windows.

---

---

The Configuration Wizard's **Welcome** screen is displayed.

4. Select **Extend an existing WebLogic domain**, and click **Next**.

The **Select a WebLogic Domain Directory** screen is displayed.

5. Use the navigation tree to select the existing Access Manager domain directory, and click **Next**.

The **Select Extension Source** screen is displayed.

6. Select **Extend my domain automatically to support the following added products**, and select the following component:

- **Oracle Access Management and Mobile Security Suite - 11.1.2.3.0**

When you select Oracle Access Management and Mobile Security Suite - 11.1.2.3.0, the following components are automatically selected:

- **Oracle Enterprise Manager - 11.1.1.0**
- **Oracle WSM Policy Manager - 11.1.1.0**

---

---

**Note:** The **Keep Existing Component** message will be displayed depending on your upgrade starting point. Therefore, you may or may not see the message, depending on the OAM version you are upgrading.

If the message is displayed, you must select the **Keep Existing Component** check box for all such occurrences.

---

---

Click **Next**.

The **Specify Domain Name and Location** screen is displayed.

7. Ensure that the Domain Name, Domain Location, and the Application Location is correct. Click **Next**.

The **Configure JDBC Data Sources** screen is displayed if there are any custom application datasources configured in the domain. Click **Next**.

The **Configure JDBC Component Schema** screen is displayed.

8. Specify the following details for all of the component schemas listed:

- **Vendor** - Select the database vendor.
- **Driver** - Select the JDBC driver to use to connect to the database. The list includes common JDBC drivers for the selected database vendor.
- **Schema Owner** - Enter the username for connecting to the database.

- **Schema Password** - Enter the password for the specified schema owner.
- **DBMS/Service** - Enter a database DBMS name, or service name if you selected a service type driver.
- **Host Name** - Enter the name of the server hosting the database.
- **Port** - Enter the port number to be used to connect to the server that hosts the database.

After you enter the details, click **Next**.

The **Test JDBC Component Schema** screen is displayed.

9. Use the screen to test the configurations that you specified for the data sources in the previous screen. Select the check boxes adjacent to the names of the schemas to test, and then click **Test Connections**.

The wizard tests the configuration for each schema by attempting to connect to a URL that is constructed by using the driver, host, port, and other information that you specified while configuring the schema. The result of the test is indicated in the **Status** column. Details are displayed in the **Connection Result Log** section.

After the test connection process is completed, click **Next**.

The **Select Optional Configuration** screen is displayed.

10. Use this screen to add new managed servers, clusters, and machines. You can also modify the deployments and services using this screen. Depending on your action on this screen, you might have to enter additional details like the name of the new managed server, cluster and so on

---

**Note:** Ensure that you assign the new OMSS and OAM Policy Servers to the Node Manager, if they are included in the your setup. If you do not perform this, the OMSS and OAM Policy Server cannot be started via the WebLogic Administration Console.

---

Complete all the required steps, and click **Next**.

The **Configuration Summary** screen is displayed.

11. Review the detailed configuration settings of your domain, and click **Extend**.

The **Extending Domain** screen is displayed.

12. Monitor the progress of the domain extension process. Once completed, click **Done** to close the Configuration Wizard.

For more information about using the Configuration Wizard to extend your existing WebLogic domain, see "Extending WebLogic Domains" in the *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard*.

---

**Note:** To start using the features of Oracle Mobile Security Suite, you must enable it using the instructions described in [Section 24.3.2, "Enabling Oracle Mobile Security Suite"](#).

---

## 24.3.2 Enabling Oracle Mobile Security Suite

If you wish to use the functionality of Oracle Mobile Security Suite, you must configure Oracle Mobile Security Suite after extending the Access Manager domain with Oracle Mobile Security Suite component.

To configure Oracle Mobile Security Suite, complete the following steps:

1. Ensure that the upgraded environment is using JDK7.
2. Restart the WebLogic Administration Server and the Access Manager Managed Servers.

For information about stopping the servers, see [Section 24.1.8, "Starting the Servers"](#).

For information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

3. If your environment is SSL enabled, ensure that the certificate for LDAP is imported into JDK7 keystore. To do this, run the following command:

```
keytool -import -alias alias -file path_to_ldapcert.pem -keystore jdk7_location/jre/lib/security/cacerts
```

Enter the password as *changeit*, when prompted.

For example,

```
keytool -import -alias trust -file /ldapcert.pem -keystore /jdk7/jre/lib/security/cacerts
```

4. Increase the heap size of the JVM. To do this, open the `setDomainEnv.sh` file located at `DOMAIN_HOME/bin/`, and specify the correct values for the following memory arguments:

```
XMS_SUN_64BIT="256"  
export XMS_SUN_64BIT  
XMS_SUN_32BIT="256"  
export XMS_SUN_32BIT  
XMX_SUN_64BIT="512"  
export XMX_SUN_64BIT  
XMX_SUN_32BIT="512"  
export XMX_SUN_32BIT  
XMS_JROCKIT_64BIT="256"  
export XMS_JROCKIT_64BIT  
XMS_JROCKIT_32BIT="256"  
export XMS_JROCKIT_32BIT  
XMX_JROCKIT_64BIT="512"  
export XMX_JROCKIT_64BIT  
XMX_JROCKIT_32BIT="512"  
export XMX_JROCKIT_32BIT
```

---

---

**Note:** For the 64BIT parameters, specify the value that is twice the existing value.

For example, if the existing value of `XMS_SUN_64BIT="256"`, edit it as:

```
XMS_SUN_64BIT="512".
```

---

---

5. Configure Oracle Mobile Security Suite. This step involves tasks like configuring Access Manager for Oracle Mobile Security Suite, configuring Oracle Mobile Security Manager, installing and configuring Oracle Mobile Security Access Server.

For information about configuring Oracle Mobile Security Suite, see "Configuring Oracle Mobile Security Suite" in the *Oracle Installation Guide for Oracle Identity and Access Management*.

6. Update the authentication module `LDAPNoPasswordAuthModule` to point to the identity store used by the Oracle Mobile Security Access Server. To do this, complete the following steps:
  1. Log in to the Oracle Access Management console using the following URL:  
`http://oam_host:oam_port/oamconsole`
  2. Click **Application Security** at the top of the window.
  3. In the Application Security console, click **Authentication Modules** in the **Plug-ins** section.
  4. In the Search Results list, select for `LDAPNoPasswordAuthModule` to open its properties page.
  5. On the properties page, update the **User Identity Store** to point to the OUD user store.
  6. Click **Apply** to submit the changes and close the Confirmation window.

### 24.3.3 Upgrading Oracle Access Management Identity Federation

If your starting point is Access Manager 11.1.2.x.x and if you have configured Oracle Access Management Identity Federation, you must upgrade Oracle Access Management Identity Federation to 11.1.2.3.0 by complete the following steps:

1. Launch the WebLogic Scripting Tool (WLST) by running the following command from the location `ORACLE_HOME/common/bin`:  
On UNIX: `./wlst.sh`  
On Windows: `wlst.cmd`
2. Connect to the WebLogic Administration Server by running the following command:  
`connect()`
3. Navigate to the Domain Runtime by running the following command:  
`domainRuntime()`
4. Upgrade the Oracle Access Management Identity Federation to by running the following command:  
`upgradeFedSTS111230()`
5. Exit the WLST using the following command:  
`exit()`



---

---

## Troubleshooting Upgrade Issues

This chapter describes the common issues that you may encounter during the Oracle Identity and Access Management upgrade process, and their corresponding workaround.

This chapter includes the following sections:

- [Section 25.1, "Troubleshooting Oracle Identity Manager Upgrade Issues"](#)
- [Section 25.2, "Troubleshooting Oracle Access Management Upgrade Issues"](#)

### 25.1 Troubleshooting Oracle Identity Manager Upgrade Issues

This section describes the workaround for the common issues that you may encounter during the Oracle Identity Manager upgrade process. This section includes the following topics:

- [Pre-Upgrade Report Generation Fails](#)
- [Pre-Upgrade Utility Reports Invalid Objects in OIM Schema](#)
- [Oracle Identity Manager Binary Upgrade Fails](#)
- [Patch Set Assistant \(PSA\) Fails](#)
- [Upgrade Assistant \(UA\) Fails](#)
- [Backups Taken by OIM Middle Tier Upgrade Utility](#)
- [Errors or Warnings During Oracle Identity Manager Middle Tier Offline Upgrade](#)
- [Reviewing Autodiscovery.properties File Created During the OIM Middle Tier Upgrade](#)
- [Errors or Warning During Oracle Identity Manager Middle Tier Online Upgrade](#)
- [MDS Patching Issues](#)
- [Some MDS Documents not Merged Correctly](#)
- [JDBC Errors](#)
- [Exception in Log When Creating Users](#)
- [All Features not Upgraded During Oracle Identity Manager Middle Tier Upgrade](#)
- [Oracle Identity Manager Upgrade Control Points](#)
- [Performing Basic Sanity Checks](#)
- [Exception While Starting Administration Server After OIM Middle Tier Upgrade in an OIM-OAM-OAAM Integrated Environment](#)

- [OIM Incremental Reconciliation Not Working After Upgrading OIM in an OIM-OAM-OAAM Integrated Environment](#)
- [Unable to Access Pending Approvals After OIM Middle Tier Online Upgrade](#)
- [Exception While Running upgradeOpss Command](#)
- [OIM Middle Tier Online Upgrade Fails in Examine Phase in SSL Environment](#)
- [OIM Schema Upgrade Fails When Upgrading OIM 11.1.2.2.0](#)
- [OPSS Authorization Fails After Upgrading to OIM 11.1.2.3](#)

## 25.1.1 Pre-Upgrade Report Generation Fails

This section lists the issues you might encounter while generating pre-upgrade report for Oracle Identity Manager. This section includes the following topics:

- [Validation Failure While Generating Pre-Upgrade Report](#)
- [Plugin Failure While Generating Pre-Upgrade Report](#)

### 25.1.1.1 Validation Failure While Generating Pre-Upgrade Report

If you get a validation error while generating the pre-upgrade report for Oracle Identity Manager, check if you have specified the correct values in the `preupgrade_report_input.properties` file.

[Table 25–1](#) lists the log messages displayed during validation failure, and their respective solutions.

**Table 25–1 Log Messages for Validation Failures During Pre-Upgrade Report Generation for OIM**

Log Message	Cause	Solution
Not able to connect to the Database with the Provided Information Host:oimhost.example.com:152 1/oimdb.example.com , User Name : < OIM	If Database is not in running state.	Start the Database.
Not able to connect to the Database with the Provided Information Host:oimhost.example.com:152 1/oimdb.example.com , User Name :<OIM schema user>	If OIM schema password is incorrect.	Check the OIM schema username and password that you have specified in the <code>preupgrade_report_input.properties</code> file.
Not able to connect to the Database with the Provided Information Host:oimhost.example.com:152 1/oimdb.example.com , User Name : < MDS schema user>	If MDS schema password is incorrect.	Check the MDS schema username and password that you have specified in the <code>preupgrade_report_input.properties</code> file.

### 25.1.1.2 Plugin Failure While Generating Pre-Upgrade Report

If you get a plugin failure error while generating pre-upgrade report for Oracle Identity Manager, skip the failing plugin and re-run pre-upgrade report utility. Raise a Service Request (SR) for the failed plugin. To skip the failed plugin, you must edit the `PreUpgrade_Report_Directory/server/upgrade/UpgradeMetadata.xml` file to remove the failed plugin.

Table 25–2 lists the log messages displayed during plugin failure, and their respective solutions.

**Table 25–2 Log Messages for Plugin Failures During Pre-Upgrade Report Generation for OIM**

Log Message	Cause	Solution
Caused by: java.lang.reflect.InvocationTargetException at sun.reflect.NativeMethodAccessorImpl.invoke0 (Native Method)	Check the <i>PreUpgrade_Report_</i> <i>Directory/logs/PreUpgradeReport&lt;time-stamp&gt;.log</i> .	Edit the <i>PreUpgrade_Report_Directory/server/upgrade/UpgradeMetadata.xml</i> file to remove the failed plugin.

Table 25–3 provides the list of plugins and reports.

**Table 25–3 List of Plugins and Reports**

Plugin	Report
COMMON_PREUPGRADE.REPORT	APPROVALPOLICYPreUpgradeReport.html ChallengeQuesPreUpgradeReport.html CYCLIC_GROUP_MEMBERSHIP_CHKPreUpgradeReport.html DomainReassocAuthorization.html EVENT_HANDLERPreUpgradeReport.html ORACLE_MANDATORY_COMPONENT_CHKPreUpgradeReport.html ORACLE_ONLINE_PURGE_PreUpgradeReport.html PROVISIONINGBYREQUESTPreUpgradeReport.html PROVISIONINGPreUpgradeReport.html REQUESTPreUpgradeReport.html
DATABASE_PRIVILEGES.REPORT	MANDATORY_DATABASE_PRIVILEGE_CHECKPreUpgradeReport.html
PasswordPolicy.Upgrade	PasswordPolicyPreUpgradeReport.html
DomainConfig.Upgrade	DOMAIN_CONFIG_CHECKPreUpgradeReport.html
UDF_PREUPGRADE.REPORT	UDFPreUpgradeReport.html
WLSMBEAN_TYPE_PREUPGRADE.REPORT	WLSMBEANPreUpgradeReport.html
R2PS2R2PS3.UI	UISimplificationUpgradeImpactReport.html
AuthorizationPreUpgradeReportR2PS3.REPORT	AUTHORIZATION_R2PS3PreUpgradeReport.html
R2PS1R2PS2.Certification	CertificationUpgradeReport.html

### 25.1.2 Pre-Upgrade Utility Reports Invalid Objects in OIM Schema

The following invalid triggers are found in the Oracle Identity Manager schema:

UD_EBS_RLO_ENT_TRG	INVALID
UD_EBS_RSO_ENT_TRG	INVALID

These are the triggers of Resource Form which are no longer used. Therefore, you can ignore this.

### 25.1.3 Oracle Identity Manager Binary Upgrade Fails

Oracle Identity Manager binary upgrade fails if you are not using the correct OPatch version. The OPatch version supported for Oracle Identity Manager 11.1.2.3.0 is Oracle Interim Patch Installer version 11.1.0.10.3. Therefore, verify the OPatch version before you upgrade Oracle Identity Manager binaries.

For any other issues during Oracle Identity Manager binary upgrade, check the installation log files. For information about locating the installation log files, see "Locating Installation Log Files" in the *Oracle Fusion Middleware Installation Guide for Oracle Identity and Access Management*.

### 25.1.4 Patch Set Assistant (PSA) Fails

If Patch Set Assistant (PSA) is stuck for a long time, you can check the block that is currently being executed. The last block at the end of the PSA log file is the block that is currently being executed. The following is the location of the PSA logs:

- On UNIX: `MW_HOME/oracle_common/upgrade/logs/psa<time_stamp>.log`
- On Windows: `MW_HOME\Oracle_common\upgrade\logs\psa<time_stamp>.log`

For any other issues encountered during upgrading schemas using PSA, check the PSA logs, fix the issue, and run the PSA again.

### 25.1.5 Upgrade Assistant (UA) Fails

If Upgrade Assistant (UA) fails during Oracle Identity Manager upgrade, check the UA logs at the following location:

- On UNIX: `ORACLE_HOME/upgrade/logs/ua<time_stamp>.log`
- On Windows: `ORACLE_HOME\upgrade\logs\ua<time_stamp>.log`

Fix the issue, and run the UA again.

### 25.1.6 Backups Taken by OIM Middle Tier Upgrade Utility

The Oracle Identity Manager middle tier upgrade utility backs up the domain configuration, before and after middle tier offline upgrade which can be used for debugging. These backed up files are located in the `ORACLE_HOME/server/upgrade/logs/MT/OIMUpgrade_backup/` directory.

You can restore these backups if required.

Table 25–4 lists the backups taken by the OIM middle tier offline upgrade utility.

**Table 25–4 Backups Taken by Middle Tier Offline Upgrade Utility**

File Name	Description	Timing
<code>afterOfflineMT&lt;timestamp&gt;domain-info.xml</code>	This is the backup of the <code>DOMAIN_HOME/init-domain/domain-info.xml</code> file.	After the OIM middle tier offline execution.
<code>afterOfflineMT&lt;timestamp&gt;.zip</code>	This is the backup of the <code>DOMAIN_HOME/config</code> folder.	After the OIM middle tier offline execution.
<code>beforeOfflineMT&lt;timestamp&gt;domain-info.xml</code>	This is the backup of <code>DOMAIN_HOME/init-domain/domain-info.xml</code> file.	Before the OIM middle tier offline execution.

**Table 25–4 (Cont.) Backups Taken by Middle Tier Offline Upgrade Utility**

File Name	Description	Timing
beforeOfflineMT<timestamp>.zip	This is the backup of the <i>DOMAIN_HOME</i> /config folder.	Before the OIM middle tier offline execution.
PolicyBackup<timestamp>jazn.xml	This is the backup of policies. This back up is taken if you are upgrading OIM 11.1.2.x.x environments.	Before the OIM middle tier offline execution.

## 25.1.7 Errors or Warnings During Oracle Identity Manager Middle Tier Offline Upgrade

If Oracle Identity Manager middle tier offline upgrade fails, you must do the following:

- Check the HTML reports generated at *ORACLE\_HOME*/server/upgrade/logs/MT/oimUpgradeReportDir\_offline. If there are any issues, fix them and run the Oracle Identity Manager middle tier offline upgrade tool again.
- Check the logs files located at *ORACLE\_HOME*/server/upgrade/logs/MT/. For the list of logs generated for Oracle Identity Manager middle tier offline upgrade, see [Table 24–11, "Logs Generated for OIM Middle Tier Offline Upgrade"](#). Fix the issue, if any, and re-run the middle offline upgrade.

This section includes the following topics:

- [Validation Failures During OIM Middle Tier Offline Upgrade](#)
- [Plugin Failures During OIM Middle Tier Offline Upgrade](#)
- [Other Failures During OIM Middle Tier Offline Upgrade](#)

### 25.1.7.1 Validation Failures During OIM Middle Tier Offline Upgrade

For any validation failures during Oracle Identity Manager middle tier offline upgrade, see the log messages listed in [Table 25–5](#) and perform the necessary action.

**Table 25–5 Log Messages for Validation Failure During OIM Middle Tier Offline Upgrade**

Log Message	Cause	Workaround
Not able to connect to the Database with the Provided Information Host :oimhost.example.com:152 1/oimdb.example.com, User Name : < OIM schema user>	If Database is not up and running.	Start the Database.
Not able to connect to the Database with the Provided Information Host :oimhost.example.com:152 1/oimdb.example.com , User Name :<OIM schema user>	If OIM schema credentials are incorrect.	Check the OIM schema username and password in the oim_upgrade_input.properties file located at <i>ORACLE_HOME</i> /server/bin/.

**Table 25–5 (Cont.) Log Messages for Validation Failure During OIM Middle Tier Offline**

<b>Log Message</b>	<b>Cause</b>	<b>Workaround</b>
Not able to connect to the Database with the Provided Information Host :oimhost.example.com:152 1/oimdb.example.com , User Name : < MDS schema user>	If Metadata Services (MDS) schema credentials are incorrect.	Check the MDS schema username and password in the oim_upgrade_input.properties file located at <i>ORACLE_HOME</i> /server/bin/.
Not able to connect to the Database with the Provided Information Host :oimhost.example.com:152 1/oimdb.example.com , User Name : < SOA schema user>	If Oracle SOA Suite (SOAINFRA) schema credentials are incorrect.	Check the username and password of the SOAINFRA schema.
Target version property is not in correct format like 11.1.2.2.0	If the target version specified in the <i>preupgrade_report_input.properties</i> is not in correct format.	Specify the target version as 11.1.2.3.0.
Please shutdown the admin server for running Mid-Tier Upgrade in offline mode  or  Please shutdown the soa server for running Mid-Tier Upgrade in offline mode  or  Not able to run the Mid-Tier Upgrade Using above data	If the WebLogic Administration Server or Oracle SOA Suite Managed Server(s) or Oracle Identity Manager Managed Server(s) are in running state.	Shut down the WebLogic Administration Server, Oracle SOA Suite Managed Server(s), and Oracle Identity Manager Managed Server(s) before running the OIM middle tier offline upgrade.

**Table 25–5 (Cont.) Log Messages for Validation Failure During OIM Middle Tier Offline**

Log Message	Cause	Workaround
<pre>Error in reading the properties filenull Exception in thread "main" java.lang.NullPointerExc eption at oracle.iam.oimupgrade.st andalone.utils.WriteLog. write(WriteLog.java:47) at oracle.iam.oimupgrade.st andalone.utils.OfflineUp gradeUtil.checkTemplateA ppplied(OfflineUpgradeUti l.java:325) at oracle.iam.oimupgrade.st andalone.OIMONEHOPUpgrad e.getInputsFromPropertie sFile(OIMONEHOPUpgrade.j ava:436) at oracle.iam.oimupgrade.st andalone.OIMONEHOPUpgrad e.main(OIMONEHOPUpgrade. java:158)</pre>	<p>If the Domain Home specified in the oim_upgrade_input.properties file is incorrect.</p>	<p>Specify the correct OIM domain home for the property oim.domain in the oim_upgrade_input.properties file located at <i>ORACLE_HOME</i>/server/bin/.</p>
<p>Domain present at &lt;domain_home&gt; does not have write permissions. Please give write permission on the Domain Directory and run again</p>	<p>If the OIM domain directory does not have write permission</p>	<p>Provide Write permission to the OIM domain home directory.</p>
<p>Please Delete the JARS OIMAuthenticator.jar, oim sigmbean.jar, oimsignature embean.jar, oimbean.jar, available in server/lib/mbeantypes/oim mbean.jar from all nodes in cluster. Before Executing Mid-Tier Upgrade</p>	<p>If OIMAuthenticator.jar, oim sigmbean.jar, oimsignature embean.jar, oimbean.jar are present in the specified directory.</p>	<p>Delete the OIMAuthenticator.jar, oim sigmbean.jar, oimsignature embean.jar, oimbean.jar files from the location <i>WL_HOME</i>/server/lib/mbeantypes.</p>
<p>OIM MT Upgrade Prerequisite Failed .Examine for feature &lt;Plugin Feature ID&gt; failed</p>	<p>If prerequisite of any plug-in fails.</p>	<p>Fix the issue for the plugin feature ID &lt;Plugin Feature ID&gt; and re-run the OIM middle tier offline upgrade again.</p>

### 25.1.7.2 Plugin Failures During OIM Middle Tier Offline Upgrade

For any plugin failures during Oracle Identity Manager offline upgrade, do the following for the depending on the log message listed in [Table 25–6](#):

1. Open the file *ORACLE\_HOME*/server/upgrade/oim-upgrade-plugin.xml, and comment out the body of the target mentioned in the **Log Message** column in

Table 25–6.

2. Launch the WebLogic Scripting Tool (WLST) by running the following command from the location `ORACLE_HOME/common/bin`:  
 On UNIX: `./wlst.sh`  
 On Windows: `wlst.cmd`
3. Run the python command mentioned in column **Workaround** with the appropriate parameters, for the corresponding log message.
4. After the python command is successfully executed, resume the OIM middle tier offline upgrade. If it fails, raise a Service Request.

**Table 25–6 Log Messages for Validation Failure During OIM Middle Tier Offline Upgrade**

Log Message	Ant Log File	Workaround
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : migrateJazn	ant_MigrateJazn_oim-bi-policystore-appPoliciesMigrate.xml.log	Run the following command:  <pre>migrateSecurityStore(type="appPolicies", configFile="ORACLE_HOME/server/upgrade/logs/MT/oimUpgradeReportDir_MODE/migrationDir/jps-config-jse.xml", srcApp="obi", overwrite="false", src="oim-bi-policystore-appPoliciesMigrate.xml", dst="default" )</pre> <p>In the above command, <code>ORACLE_HOME</code> is the absolute path to the OIM Oracle Home, and <code>MODE</code> if the OIM middle tier upgrade mode. In case of OIM middle tier offline upgrade, the value of <code>MODE</code> should be offline. In case of OIM middle tier online upgrade, the value of <code>MODE</code> should be online.</p>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : create-bip-server	ant_createBipServer.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade</code> :  <pre>createBIPserver.py DOMAIN_HOME MW_HOME BIP_SERVER_NAME BIP_SERVER_HOST BIP_SERVER_PORT BIP_SERVER_SSL_PORT BIP_SERVER_SSL_ENABLED BIP_JDBC_URL BIP_DATASOURCE_NAME BIP_SCHEMA_NAME BIP_SCHEMA_PASSWORD BIP_CLUSTER_NAME</pre>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : target-bip-resources	ant_targetBIPResources.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade</code> :  <pre>targetingResourceBIP.py DOMAIN_HOME BIP_CLUSTER_NAME OPSS_RAC_LIST MDS_OWSM_RAC_LIST</pre>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : apply-bip	ant_applyBip.log	Run the following command from the location <code>BIP_HOME/bifoundation/install</code> :  <pre>applyBIP.py DOMAIN_HOME BIP_SERVER_NAME</pre>

**Table 25–6 (Cont.) Log Messages for Validation Failure During OIM Middle Tier Offline**

Log Message	Ant Log File	Workaround
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : upgradeClassPath	ant_ ApplicationDB.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade:</code>  <code>createDSoffline.py DOMAIN_HOME IS_CLUSTER "ApplicationDB" OIM_SERVER_NAME "jdbc/ApplicationDBDS" "oimApplicationDBDS" "OIMSchema_dbPassword" "OIMSchema_dbURL" "oracle.jdbc.OracleDriver" "OIMSchema_dbUser" "10000" "0" "0" "50"</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : configureSecurityStore	ant_ configureSecurityStore.log	Run the following command from the location <code>ORACLE_HOME/common/tools:</code>  <code>configureSecurityStore.py -d DOMAIN_HOME -m create -t DB_ORACLE -c IDM -p OPSSSchemaPassword</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : deployAppOffline	ant_ deploySCIMWebapp.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade:</code>  <code>deployAppOffline.py DOMAIN_HOME OIM_SERVER_NAME "SCIM REST service for OIM" "OIM_HOME/server/apps/scim-oim-services.war" "WAR" "57"</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : enableJsseSsl	ant_ enableJsseSsl.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade:</code>  For single node environment: <code>enableJsseSsl.py DOMAIN_HOME OIM_SERVER_NAME "false"</code>  For cluster environment: <code>enableJsseSsl.py DOMAIN_HOME OIM_CLUSTER_NAME "true"</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : applyOPSSTemplate	ant_ extendOPSSDomain.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade:</code>  <code>applyOPSSTemplate.py DOMAIN_HOME OIM_HOME OPSSSchemaUser OPSSSchemaPassword OPSSSchemaConnectString</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : checkClusterOIM	ant_ isClusterOIM.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade:</code>  <code>checkClusterOIM.py DOMAIN_HOME OIM_HOME</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : JMSModuleTarget	ant_ JMSModuleTargetScript.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade:</code>  <code>target_jrfasyncws.py DOMAIN_HOME OIMServerName</code>

**Table 25–6 (Cont.) Log Messages for Validation Failure During OIM Middle Tier Offline**

Log Message	Ant Log File	Workaround
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : addTemplate	ant_JRF_WsAsync.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade:</code>  <code>addTemplate.py DOMAIN_HOME MW_HOME/oracle_common/common/templates/applications/oracle.jrf.ws.async_template_11.1.1.jar</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : migrateJazn	ant_MigrateJazn_jazn-data-oim.xml.log	Run the following command from the location <code>MW_HOME/oracle_common/modules/oracle.jps_11.1.1/common/wlstscripts:</code>  <code>migrateSecurityStore.py -type policyStore -dst default -configFile ORACLE_HOME/server/upgrade/logs/MT/oimUpgradeReportDir_offline/migrationDir/jps-config-jse.xml -src jazn-data-oim.xml</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : migrateJazn	ant_MigrateJazn_jazn-data-self.xml.log	Run the following command from the location <code>MW_HOME/oracle_common/modules/oracle.jps_11.1.1/common/wlstscripts:</code>  <code>migrateSecurityStore.py -type policyStore -dst default -configFile ORACLE_HOME/server/upgrade/logs/MT/oimUpgradeReportDir_offline/migrationDir/jps-config-jse.xml -src jazn-data-self.xml</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : miscUpgrade	ant_MiscUpgrade.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade:</code>  <code>miscUpgrade.py DOMAIN_HOME OIM_SERVER_OR_CLUSTER_NAME</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : upgradeOPSS	ant_OPSS.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade:</code>  <code>upgradeOPSS.py JPSCONF SYSJAZN</code>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : upgradeOPSS-r2	ant_OPSS-r2.log	Run the following command from the location <code>ORACLE_HOME/server/upgrade:</code>  <code>upgradeOPSS_R2.py JPSCONF SYSJAZN DOMAIN_HOME OPSSSchemaPassword opssUrl opssjdbcDriverName opssUser</code>

**Table 25–6 (Cont.) Log Messages for Validation Failure During OIM Middle Tier Offline**

Log Message	Ant Log File	Workaround
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : deployAppOffline	ant_ oracle.idm.ids.config.ui#11.1.2@11.1.2.1 og	Run the following command from the location <i>ORACLE_HOME</i> /server/upgrade:  deployAppOffline.py <i>DOMAIN_HOME</i> <i>OIM_SERVER_NAME</i> "oracle.idm.ids.config.ui#11.1.2@11.1.2" " <i>ORACLE_HOME</i> /modules/oracle.idm.ids.config.ui_11.1.2/oracle.idm.ids.config.ui.war" "JAR" "300"
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : deployAppOffline	ant_ oracle.idm.ipf#11.1.2@11.1.2.log	Run the following command from the location <i>ORACLE_HOME</i> /server/upgrade:  deployAppOffline.py <i>DOMAIN_HOME</i> <i>ADMIN_SERVER_NAME</i> "oracle.idm.ipf#11.1.2@11.1.2" " <i>ORACLE_HOME</i> /modules/oracle.idm.ipf_11.1.2/ipf.jar" "JAR" "300"
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : upgradeClassPath	ant_ soaOIMLookupDB.log	Run the following command from the location <i>ORACLE_HOME</i> /server/upgrade:  createDSoffline.py <i>DOMAIN_HOME</i> <i>IS_CLUSTER</i> "soaOIMLookupDB" <i>SOA_SERVER_NAME</i> "jdbc/soaOIMLookupDB" "soaOIMLookupDB" " <i>OIMSchema_dbPassword</i> " " <i>dbPassword</i> " " <i>OIMSchema_dbURL</i> " "oracle.jdbc.OracleDriver" " <i>OIMSchema_dbUser</i> " "10000" "20" "20" "20"
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : addTemplate	ant_Update_ setDomainEnv.log	Run the following command from the location <i>ORACLE_HOME</i> /server/upgrade:  addTemplate.py <i>DOMAIN_HOME</i> <i>ORACLE_HOME</i> /server/upgrade/ templates/oracle.oim_r2ps2StartScript_ upgrade_template.jar
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : upgradeJRF	ant_UpgardeJRF.log	Run the following command from the location <i>ORACLE_HOME</i> /server/upgrade:  upgradeJRF.py <i>DOMAIN_HOME</i>
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : addTemplate	ant_Workmanager.log	Run the following command from the location <i>ORACLE_HOME</i> /server/upgrade:  addTemplate.py <i>DOMAIN_HOME</i> <i>ORACLE_HOME</i> /server/upgrade/ templates/oracle.oim_r2ps3WorkManager_ upgrade_template.jar

### 25.1.7.3 Other Failures During OIM Middle Tier Offline Upgrade

Table 25–7 lists the log messages for issues other than validation and plugin issues, log filename, and corresponding solutions.

**Table 25–7 Other Failures During OIM Middle Tier Offline Upgrade**

Log Message	Ant Log File / Cause	Workaround
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : oimr1ps1_upgrade_package_dogwood_top_and_oim_suite	ant_ oimUpgradeDomainPackage s.log	Run the following java commands:  java -cp <i>MW_HOME</i> /utils/config/10.3/config-1aunch.jar: <i>OIM_ORACLE_HOME</i> /oaam/upgrade/com.oracle.cie.domain-update_1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <i>DOMAIN_HOME</i> oracle.dogwood.top:11.1.1.5.0,:11.1.2.2.0  java -cp <i>MW_HOME</i> /utils/config/10.3/config-1aunch.jar: <i>OIM_ORACLE_HOME</i> /oaam/upgrade/com.oracle.cie.domain-update_1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <i>DOMAIN_HOME</i> oracle.oim.suite:11.1.1.5.0,:11.1.2.2.0
copy_bip_reports		Complete the following steps:  <b>1.</b> Copy the oim_product_BIP11gReports_11_1_2_3_0.zip file from the location <i>MW_HOME</i> /server/reports to <i>DOMAIN_HOME</i> /config/bipublisher/repository/Reports.  <b>2.</b> Extract the files of oim_product_BIP11gReports_11_1_2_3_0.zip from the destination location.  <b>3.</b> Provide read, write, and execute permissions to the file datasourceconfig.sh (on UNIX) or datasourceconfig.cmd (on Windows).
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : create-bip-datasource	BIP plugin fails with error in log file: ant_ createBIPDatasources_ OIM.log	Run the following command from the location <i>ORACLE_HOME</i> /server/upgrade/logs/MT/oimUpgradeReportDir_offline/biptemp/bin/:  datasourceconfig.sh jdbc create 'OIM JDBC' JDBC_DRIVER_TYPE=ORACLE11G JDBC_DRIVER_CLASS=oracle.jdbc.OracleDriver JDBC_URL= <i>JDBC_URL</i> USE_SYSTEM_USER=false JDBC_USERNAME= <i>SCHEMA_OWNER</i> JDBC_PASSWORD= <i>SCHEMA_PASSWORD</i> USE_PROXY_AUTHENTICATION=false ALLOWED_GUEST_ACCESS=false

**Table 25–7 (Cont.) Other Failures During OIM Middle Tier Offline Upgrade**

Log Message	Ant Log File / Cause	Workaround
OIMUpgradeException: Error in running target : create-bip-datasource	BIP plugin fails with error in log file: ant_ createBIPDatasources_ BPEL.log	Run the following command from the location <code>ORACLE_ HOME/server/upgrade/logs/MT/oim UpgradeReportDir_ offline/biptemp/bin/:</code>  <pre>datasourceconfig.sh jdbc create 'BPEL JDBC' JDBC_DRIVER_ TYPE=ORACLE11G JDBC_DRIVER_ CLASS=oracle.jdbc.OracleDriver JDBC_URL=JDBC_URL USE_SYSTEM_ USER=false JDBC_ USERNAME=SCHEMA_OWNER JDBC_ PASSWORD=SCHEMA_PASSWORD USE_ PROXY_AUTHENTICATION=false ALLOWED_GUEST_ACCESS=false</pre>
Some plugins are yet not upgraded, please check logs and re-run MToffline or disable those plugins	If some plugins are not populated in the <code>upgrade_ feature_state</code> table.	Run OIM middle tier offline upgrade or disable the plugins that are not populated in the <code>upgrade_ feature_state_table</code> .
Upgrade Failed. Please check the logs for further details. Please re-run OIMUpgrade offline utility after fixing the problem. Avoid following any other step before successfully running OIMUpgrade offline utility		
./ant_MigrateJazn_ bi-policystore-systemro le-jazn.xml.log:WARNING : Application role BIAdministrator does not exist	ant_MigrateJazn_ bi-policystore-systemro le-jazn.xml.log	This warning can be ignored.
./ant_MigrateJazn_ bi-policystore-systemro le-jazn.xml.log:WARNING : Application role BIConsumer does not exist		
./ant_MigrateJazn_ bi-policystore-systemro le-jazn.xml.log:WARNING : Application role BIAuthor does not exist		

**Table 25–7 (Cont.) Other Failures During OIM Middle Tier Offline Upgrade**

Log Message	Ant Log File / Cause	Workaround
<pre> oracle.iam.platform.entitymgr.impl.EntityManagerConfigImpl getEntityConfig  WARNING: Cannot load entity definition - java.lang.NullPointerException  at  oracle.iam.platform.entitymgr.impl.EntityManagerConfigImpl.getEntityConfig(EntityManagerConfigImpl.java:1148)  at  oracle.iam.platform.entitymgr.impl.EntityManagerConfigImpl.loadMetadata(EntityManagerConfigImpl.java:960)  at  oracle.iam.platform.entitymgr.impl.EntityManagerConfigImpl.&lt;init&gt;(EntityManagerConfigImpl.java:203)  at  oracle.iam.platform.entitymgr.impl.EntityManagerImpl\$ConfigManager.&lt;init&gt;(EntityManagerImpl.java:191)  at  oracle.iam.platform.entitymgr.impl.EntityManagerImpl.&lt;init&gt;(EntityManagerImpl.java:226)  at  sun.reflect.NativeConstructorAccessorImpl.newInstance(Native Method)  at  sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java:57) </pre>	<p>This warning is displayed on the console during reconciliation feature upgrade.</p>	<p>This warning can be ignored.</p>

**Table 25–7 (Cont.) Other Failures During OIM Middle Tier Offline Upgrade**

Log Message	Ant Log File / Cause	Workaround
Command FAILED, Reason: JPS-00027: There was an internal error: java.sql.SQLException: ORA-12801: error signaled in parallel query server P001 ORA-01460: unimplemented or unreasonable conversion requested	ant_OPSS.log This error occurs when you upgrade Oracle Identity Manager 11g Release 2 (11.1.2.1.0) with Bundle Patch.	To resolve this issue, either apply Patch 13099577 or use the following workaround: Set the properties <code>parallel_max_servers</code> and <code>parallel_min_servers</code> to 0 in Database. For example: <pre>parallel_max_servers integer 0 parallel_min_servers integer 0</pre>
oracle.security.jps.internal. api.common.JpsPolicyStoreLdapNodeCreationException: JPS-00027: There was an internal error: java.sql.SQLException: ORA-12801: error signaled in parallel query server P001 ORA-01460: unimplemented or unreasonable conversion requested		

### 25.1.8 Reviewing Autodiscovery.properties File Created During the OIM Middle Tier Upgrade

Some properties are auto-discovered by the Oracle Identity Manager middle tier upgrade utility to reduce the number of properties that you need to specify manually during upgrade. When the middle tier upgrade for OIM is run for the first time, Autodiscovery.properties file is created at the location `ORACLE_HOME/server/upgrade`. This file contains the following parameters that are auto-discovered by the middle tier upgrade utility:

- `opssDBSslArgs`
- `opssjdbcDriverName`
- `is_cluster_oim`
- `soaProtocol`
- `oim_target`
- `weblogicProtocol`
- `OPSSSchemaPassword <encrypted value>`
- `opssUser`
- `opssUrl`
- `soa_target`
- `admin_target`

Autodiscovery module is executed and the `Autodiscovery.properties` file is created only the first time the middle tier upgrade script is run. Once this file is created, autodiscovery is not executed again. Next time when you run the middle tier upgrade script, the properties are read from the existing `Autodiscovery.properties` file.

If you encounter any issues during OIM middle tier upgrade, review the properties in the `Autodiscovery.properties` file and verify if the values are correct. If any of the values are incorrect, update them and run the middle tier upgrade utility again.

If you want all of the properties to be auto discovered again, remove the `Autodiscovery.properties` file from the directory `ORACLE_HOME/server/upgrade`, and run the Oracle Identity Manager middle tier upgrade (online or offline) again.

### 25.1.9 Errors or Warning During Oracle Identity Manager Middle Tier Online Upgrade

If Oracle Identity Manager middle tier online upgrade fails, you must do the following:

- Check the HTML reports generated at `ORACLE_HOME/server/upgrade/logs/MT/oimUpgradeReportDir_online`.
- Check the following logs files generated at `ORACLE_HOME/server/upgrade/logs/MT/`:
  - `OIMUpgrade_online<timestamp>.log`
  - `ant_createUserInSecurityRealm_BISystemUser.log`
  - `ant_updateBIPJmsSecurity.log`
  - `ant_importOwSMPolicySCIM.log`

This section includes the following topics:

- [Validation Failures During OIM Middle Tier Online Upgrade](#)
- [Plugin Failures During OIM Middle Tier Online Upgrade](#)

#### 25.1.9.1 Validation Failures During OIM Middle Tier Online Upgrade

For any validation failures during Oracle Identity Manager middle tier online upgrade, see the log messages listed in [Table 25–8](#) and perform the necessary action.

**Table 25–8 Log Messages for Validation Failure During OIM Middle Tier Online Upgrade**

Log Message	Cause	Workaround
Not able to connect to the admin server with Provided Information Host : oimhost.example.com , User Name :weblogic , Port :7001	If the value specified for Administration Server host property in the <code>oim_upgrade_input.properties</code> file is incorrect.	Update the correct value for Administration Server host property in the <code>oim_upgrade_input.properties</code> file at the location <code>ORACLE_HOME/server/bin/</code> .
Not able to connect to the soa server with Provided Information Host : oimhost.example.com , User Name :weblogic , SOA Port :7001	If the values specified for SOA Server properties are incorrect in the <code>oim_upgrade_input.properties</code> file is incorrect.	Update the correct value for SOA server properties in the <code>oim_upgrade_input.properties</code> file at the location <code>ORACLE_HOME/server/bin/</code> .

**Table 25–8 (Cont.) Log Messages for Validation Failure During OIM Middle Tier Online**

Log Message	Cause	Workaround
<pre>Following plugins are yet not upgraded, please Check logs and re-run MT online or disable these plugins in UpgradeMetadata.xml Feature_ID : List &lt;Feature ID 1&gt; &lt;Feature ID2&gt; ... &lt;Feature IDN&gt;</pre>	If some plugins are not upgraded.	Disable the plugins in the UpgradeMetadata.xml file that are not upgraded.
<pre>OIM MT Upgrade Prerequisite Failed .Examine for feature &lt;Plugin Feature ID&gt; failed</pre>	If prerequisite of any plug-in fails.	Fix the issue for the plugin feature ID <Plugin Feature ID> and re-run the OIM middle tier online upgrade again.

### 25.1.9.2 Plugin Failures During OIM Middle Tier Online Upgrade

For any plugin failures during Oracle Identity Manager online upgrade, do the following for the depending on the log message listed in [Table 25–9](#):

1. Open the file `ORACLE_HOME/server/upgrade/oim-upgrade-plugin.xml`, and comment out the body of the target mentioned in the **Log Message** column in [Table 25–9](#).
2. Launch the WebLogic Scripting Tool (WLST) by running the following command from the location `ORACLE_HOME/common/bin`:
3. Run the python command mentioned in column **Workaround** with the appropriate parameters, for the corresponding log message.
4. After the python command is successfully executed, resume the OIM middle tier online upgrade. If it fails, raise a Service Request.

**Table 25–9 Log Messages for Validation Failure During OIM Middle Tier Online Upgrade**

Log Message	Ant Log File	Workaround
<pre>SEVERE: oracle.iam.oimupgra de.exceptions.OIMUp gradeException: Error in running target : import-OWSM-policy</pre>	<pre>ant_ importOwSMPolicySCIM .log</pre>	<p>Run the following command from the location <code>ORACLE_HOME/server/upgrade</code>:</p> <pre>createScimOwsmPolicy.py WEBLOGIC_USER WEBLOGIC_PASSWORD WEBLOGIC_ADMIN_URL DOMAIN_HOME OIM_ HOME/server/features/multitoken-noauth -rest-policy.zip</pre>
<pre>SEVERE: oracle.iam.oimupgra de.exceptions.OIMUp gradeException: Error in running target : create-user-securit y-realm</pre>	<pre>ant_ createUserInSecurity Realm_ BISystemUser.log</pre>	<p>Run the following command from the location <code>ORACLE_HOME/server/upgrade</code>:</p> <pre>createUserInRealm.py WEBLOGIC_USER WEBLOGIC_PASSWORD ADMIN_URL DOMAIN_ HOME REALM_NAME REALM_USER_NAME REALM_ USER_PASSWORD</pre>

**Table 25–9 (Cont.) Log Messages for Validation Failure During OIM Middle Tier Online**

Log Message	Ant Log File	Workaround
SEVERE: oracle.iam.oimupgrade.exceptions.OIMUpgradeException: Error in running target : update-bip-jms-security	ant_ updateBIPJmsSecurity.log	Run the following command from the location <i>BIP_HOME/bifoundation/install/updateBIPJMSecurity.py</i> <i>WEBLOGIC_USER</i> <i>WEBLOGIC_PASSWORD</i> <i>ADMIN_URL</i>  In case of SSL environment, use the following properties as well:  env key="WLST_PROPERTIES" value=" <i>ssl_args</i> "

### 25.1.10 MDS Patching Issues

If you encounter any issues related to Metadata Services (MDS) patching, check the MDS patching reports generated at the following location:

- On UNIX: *ORACLE\_HOME/server/logs/MDS\_REPORT\_DIRECTORY/MDSReport.html*
- On Windows: *ORACLE\_HOME\server\logs\MDS\_REPORT\_DIRECTORY\MDSReport.html*

For information about re-running MDS patching, see My Oracle Support Document ID 1536894.1.

### 25.1.11 Some MDS Documents not Merged Correctly

If any of the MDS documents are not merged correctly, merge them manually from the following locations:

- On UNIX:  
*ORACLE\_HOME/server/logs/sourceDir* - This is the OOTB MDS data location.  
*ORACLE\_HOME/server/logs/targetDir* - This is the target MDS data location.
- On Windows:  
*ORACLE\_HOME\server\logs\sourceDir* - This is the OOTB MDS data location.  
*ORACLE\_HOME\server\logs\targetDir* - This is the target MDS data location.

### 25.1.12 JDBC Errors

If you encounter the following JDBC error, add an additional environment variable TZ, which is the time zone name, like GMT.

```
ORA-01882: timezone region not found
```

The environment variable has to be set with older database or you will get an error.

For more information, see My Oracle Support Document ID 1068063.1.

### 25.1.13 Exception in Log When Creating Users

After you upgrade Oracle Identity Manager 11.1.1.5.0 high availability environments to Oracle Identity Manager 11.1.2.3.0, you might see the following exception in the logs when you create users:

```
[2013-11-19T23:41:51.507-08:00] [oim_server1] [ERROR] []  
[oracle.ods.virtualization.exception] [tid: UCP-worker-thread-19] [userId:
```

```
oiminternal] [ecid: 004utMMAEYz1VcP5Ifp2if00023p000Tdf,0] [APP:
oim#11.1.1.3.0] Could not initialize default mapping config[[
javax.xml.bind.UnmarshalException
- with linked exception:
[java.io.FileNotFoundException:
/scratch/Oracle/Middleware/user_
projects/domains/IDMDomain/config/fmwconfig/ovd/oim/mappings.os_xml
(No such file or directory)
```

This does not cause the user creation task to fail. However, to eliminate this exception, you must manually copy the file `mappings.os_xml` from the location `$MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/templates/mappings.os_xml` to the directory `$DOMAIN_HOME/config/fmwconfig/ovd/oim`.

### 25.1.14 All Features not Upgraded During Oracle Identity Manager Middle Tier Upgrade

If any of the Oracle Identity Manager features are not upgraded during the Oracle Identity Manager middle tier upgrade, check the upgrade reports generated at the following location:

Middle tier offline upgrade reports: `ORACLE_HOME/upgrade/logs/MT/oimUpgradeReportDir_offline/index.html`

Middle tier online upgrade reports: `ORACLE_HOME/upgrade/logs/MT/oimUpgradeReportDir_online/index.html`

### 25.1.15 Oracle Identity Manager Upgrade Control Points

To re-run the middle tier upgrade for a specific feature after analyzing and fixing the cause of failure, set the force option of the specific feature upgrade plugin to true or false accordingly in the `UpgradeMetadata.xml` file located at `ORACLE_HOME/server/upgrade/`.

Oracle Identity Manager upgrade provides control points in the `oimupgrade.properties` file located at `ORACLE_HOME\server\bin`. If any feature upgrade fails, you can continue with the upgrade by disabling the failed feature by setting the corresponding feature upgrade property to false. To enable a specific feature for upgrade, you must the property to true.

By default, all the properties are set as true.

- Set the following property to false if you do not want to run Oracle Identity Manager configuration upgrade:
 

```
oim.ps1.config.patch=true
```
- Set the following property to false if you do not want to run SOA composite upgrade:
 

```
oim.ps1.soacomposite.patch=true
```

#### Domain Extension Properties

- Set the following property to false if you do not want to run Patch JNDI provider:
 

```
oim.domainextension.jndiprovider.patch=true
```
- Set the following property to false if you do not want to run Patch ClassPath:
 

```
oim.domainextension.classpath.patch=true
```
- Set the following property to false if you do not want to run Patch OPSS:

`oim.domainextension.opss.patch=true`

- Set the following property to false if you do not want to run Patch ears:

`oim.domainextension.ear.patch=true`

- Set the following property to false if you do not want to run Patch JRF:

`oim.domainextension.jrf.patch=true`

## 25.1.16 Performing Basic Sanity Checks

This section describes how to check a new data source added, SOA Foreign JNDI provider, and the order of EARs on the WebLogic Administration Console.

### 25.1.16.1 Checking New Data Source Added

To check the new data source added, do the following:

1. Log in to WebLogic Administration Console using the following URL:

`http://host:port/console`

2. Click **Data Sources**.
3. Verify the data source given below:

Name	Type	JNDI Name	Targets
ApplicationDBDS	Generic	jdbc/ApplicationDBDS	oim_server1 (for single node upgrade) oim_cluster (for cluster upgrade)

### 25.1.16.2 Checking for SOA Foreign JNDI Provider

To check for SOA Foreign JNDI provider, do the following:

1. Log in to WebLogic Administration Console using the following URL:

`http://host:port/console`

2. Click **Foreign JNDI Providers**.
3. Verify the existence of Foreign JNDI providers given below:

Name	Initial Context Factory	Provider URL	User	Targets
ForeignJNDIProvider-SOA	weblogic.jndi.WLInitialContextFactory	For single node upgrade: t3://soa_server_host:soa_server_port  For cluster upgrade: t3://soa_server1_host:soa_server1_port,soa_server2_host:soa_server2_port	WebLogic	oim_server1 (for single node upgrade) oim_cluster (for cluster upgrade)

**Note:** If you are upgrading Oracle Identity Manager High Availability environments, the Provider URL may contain the host and port of soa\_server1 only. In that case, you must add the host and port of soa\_server2 to the Provider URL manually.

### 25.1.16.3 Checking the Order of EARs

To check the order of the EARs, do the following:

1. Log in to WebLogic Administration Console using the following URL:  
`http://host:port/console`
2. Click **Deployments**.
3. Verify the deployment order for the following list respectively:

Name	State	Health	Type	Deployment Order
oim (11.1.1.3.0)	Active	OK	Enterprise Application	48
OIMAppMetadata (11.1.2.0.0)	Active	OK	Enterprise Application	47
OIMMetadata (11.1.1.3.0)	Active	OK	Enterprise Application	46
oracle.iam.console.identity.sysadmin.ear (V2.0)	Active	OK	Enterprise Application	406
oracle.iam.console.identity.self-service.ear (V2.0)	Active	OK	Enterprise Application	405
oracle.iam.ui.custom(11.1.1,11.1.1)	Active		Library	404
oracle.iam.ui.oa-view(11.1.1,11.1.1)	Active		Library	403

Name	State	Health	Type	Deployment Order
oracle.iam.ui.vie w(11.1.1,11.1.1)	Active		Library	402
oracle.iam.ui.mo del(1.0,11.1.1.5.0)	Active		Library	401

### 25.1.17 Exception While Starting Administration Server After OIM Middle Tier Upgrade in an OIM-OAM-OAAM Integrated Environment

After you upgrade Oracle Identity Manager middle tier in an Oracle Identity Manager, Oracle Access Manager, and Oracle Adaptive Access Manager integrated highly available environment, when you start the Administration Server, the following exception is displayed in the AdminServer.log file:

```
<Warning> <RMI> <slc04ugw> <AdminServer>
<[ACTIVE] ExecuteThread: '6' for queue: 'weblogic.kernel.Default
(self-tuning) '> <<WLS Kernel>> <>
<1f1bf9f1ae475b6d:25e02b64:14c48129185:-8000-0000000000000005>
<1427138521873> <BEA-080003> <RuntimeException thrown by rmi server:
javax.management.remote.rmi.RMIConnectionImpl.getAttribute(Ljavax.management.O
bjectName;Ljava.lang.String;Ljavax.security.auth.Subject;)
    java.lang.NullPointerException.
java.lang.NullPointerException
    at
java.util.concurrent.ConcurrentHashMap.get(ConcurrentHashMap.java:768)
    at
weblogic.management.mbeanservers.internal.JMXContextInterceptor.getMBeanContext
Loader(JMXContextInterceptor.java:475)
    at
weblogic.management.mbeanservers.internal.JMXContextInterceptor.getAttribute(J
MXContextInterceptor.java:146)
```

This warning can be ignored.

### 25.1.18 OIM Incremental Reconciliation Not Working After Upgrading OIM in an OIM-OAM-OAAM Integrated Environment

After upgrading Oracle Identity Manager in an Oracle Identity Manager, Access Manager, and Oracle Adaptive Access Manager integrated environment, if Oracle Identity Manager incremental reconciliation is not working, complete the following steps:

1. Disable all of the incremental reconciliation jobs (total 6 in all), if not already disabled.
2. Run the following full reconciliation jobs:
  - LDAP Role Delete Full Reconciliation
  - LDAP User Delete Full Reconciliation
  - LDAP Role Create and Update Full Reconciliation
  - LDAP Role Hierarchy Full Reconciliation
  - LDAP User Create and Update Full Reconciliation
  - LDAP Role Membership Full Reconciliation

3. Get the latest changelog from Oracle Unified Directory (OUD) by using the following command:

```
ldapsearch -h OUD_HOST -p OUD_PORT -D "cn=Directory Manager" -w
PASSWORD -b "" -s base "objectclass=*" lastExternalChangelogCookie
```

In the above command,

- *OUD\_HOST* refers to the host on which OUD is running.
  - *OUD\_PORT* refers to the port of the OUD.
4. Update all the six incremental reconciliation jobs with the changelog value and enable them.

### 25.1.19 Unable to Access Pending Approvals After OIM Middle Tier Online Upgrade

After you perform Oracle Identity Manager middle tier online upgrade, you may not be able to access pending approvals if you had accessed "Pending Approvals" page on the browser before upgrading OIM middle tier.

The workaround for this issue is to clear out the browser cache and access the pending approvals again.

### 25.1.20 Exception While Running upgradeOpss Command

The following exception is seen in the MT logs when you upgrade Oracle Platform Security Services using upgradeOpss command:

```
java.util.MissingResourceException: Can't find bundle for base name
oracle.adf.share.wlst.resources.WlstHelp, locale en_US
Error execing the Python script
"C:\work\mw748\oracle_common\common\wlst\mdsWLSTCommands.py" caused an error
"Traceback (innermost last):
  File "C:\work\mw748\oracle_common\common\wlst\mdsWLSTCommands.py", line
108, in ?
ImportError: no module named common
"
Error execing the Python script
"C:\work\mw748\oracle_common\common\wlst\URLConnWLST.py" caused an error
"Traceback (innermost last):
  File "C:\work\mw748\oracle_common\common\wlst\URLConnWLST.py", line 12, in
?
ImportError: no module named wlst
```

This exception is seen in the following logs:

- ant\_Update\_setDomainEnv.log
- ant\_UpgardeJRF.log
- ant\_configureSecurityStore.log
- ant\_extendOPSSDomain.log
- ant\_isClusterOIM.log

This exception can be ignored.

### 25.1.21 OIM Middle Tier Online Upgrade Fails in Examine Phase in SSL Environment

Oracle Identity Manager middle tier online upgrade fails in examine phase in SSL environment with the following error, even though the WebLogic Server is up and running:

```
"Could not connect to admin server with details <host>:<port>"
```

The workaround for this issue is as follows:

1. Remove `OIM_HOME/server/upgrade/Autodiscovery.properties` file.
2. Re run the middle tier online upgrade.

### 25.1.22 OIM Schema Upgrade Fails When Upgrading OIM 11.1.2.2.0

When you upgrade Oracle Identity Manager 11.1.2.2.0, OIM schema upgrade fails with the following error, if the Oracle Identity Manager database contains access policies:

```
oracle.iam.oimupgrade.exceptions.OIMUpgradeException: SQL Exception in
running Upgrade Scripts
    at
oracle.iam.oimupgrade.onehop.SchemaUpgradeManager.upgrade(SchemaUpgradeManager
.java:281)
...
Caused by: java.sql.SQLException: ORA-22160: element at index [438] does not exist
ORA-06512: at line 66
```

The workaround for this issue is as follows:

1. After you upgrade the Oracle Identity Manager binaries to 11.1.2.3.0, open the `oim_upg_R2PS2_R2PS3_common_policy_engine.sql` file located at `OIM_HOME/server/db/oim/oracle/Upgrade/oim11gR2PS2_2_R2PS3`, in a text editor.
2. Replace the line# 280:

```
EXECUTE IMMEDIATE sqlstr USING v_pol_owner(idx);
with
EXECUTE IMMEDIATE sqlstr USING v_pol_owner_type(idx);
```

3. Save the modified file, and run the schema upgrade.

### 25.1.23 OPSS Authorization Fails After Upgrading to OIM 11.1.2.3

OPSS authorization may fail for some OIM operations after you upgrade OIM to 11.1.2.3 from an older release. For example, you may find that OIM PS policy is not seeded to the OPSS policy store.

The workaround for this issue is as follows:

1. Backup the existing JAZN data from MDS.
2. Upgrade OIM.
3. Re-seed the JAZN data from the backup.

For detailed procedure, see Doc ID 2138965.1 on My Oracle Support.

## 25.2 Troubleshooting Oracle Access Management Upgrade Issues

This section describes the workaround for the common issues that you may encounter during the Oracle Access Manager upgrade process. This section includes the following topics:

- [Exception While Running ImportAccessData Command](#)
- [Exception While Accessing OAM Console Before Upgrading System Configuration](#)
- [Exception While Deploying Application](#)
- [PolicyValidationException While Restarting Administration Server](#)
- [Exception While Restarting Managed Server](#)
- [Component Version Shows 11.1.1.5.0 After Upgrade](#)
- [Errors While Starting the Administration Server After Upgrade](#)
- [Memory Issues While Running upgradeConfig\(\) Command](#)
- [Null Exception While Creating IDS Profile](#)
- [Post Authentication Rules Tab is Disabled on Oracle Access Management Console After Upgrade](#)
- [Exception While Running importAccessData Command](#)
- [.oamkeystore File Size Reduced to 0 Byte After Extending the OAM Domain](#)
- [upgradeConfig Fails with NullPointerException](#)

### 25.2.1 Exception While Running ImportAccessData Command

During Oracle Access Manager 11.1.1.x.x upgrade, if you get a `class not found` exception, it is because you have not exited from the WLST console after running the `exportAccessData` command.

Exit the WLST console using the `exit ()` command.

### 25.2.2 Exception While Accessing OAM Console Before Upgrading System Configuration

During Oracle Access Manager 11.1.1.x.x upgrade, when you try to access the Oracle Access Management Access Manager Administration Console before you upgrade system configurations as described in [Section 12.16, "Upgrading System Configuration"](#), the following exceptions are seen in the WebLogic Domain log file:

```
<Error> <oracle.oam.proxy.oam>
<ADC2120940> <oam_server1> <[ACTIVE] ExecuteThread: '2' for queue:
'weblogic.kernel.Default (self-tuning) '> <<anonymous>> <>
<b65aed48d5cfc0f4:25dd78c3:14b85e72198:-8000-00000000000033cc>
<1423899074190> <OAM-04020> <Exception encountered while processing the
request message:
oracle.security.am.proxy.oam.requesthandler.OAMProxyException: Event Response
status is STATUS_FAIL for GET_AUTHN_SCHEME event. Error code OAM-02073 status
fail isExcluded false
at
oracle.security.am.proxy.oam.requesthandler.NGProvider.checkProtected(NGProvid
er.java:4851)

<Error> <oracle.oam.agent-default>
```

```

<OAMAGENT-00411> <Failed to access server: MajorCode: FATAL_ERROR, MinorCode:
FATAL_ERROR>
<Feb 13, 2015 11:31:14 PM PST> <Warning> <oracle.oam.agent-default>
<OAMAGENT-00410> <OAM Server can not be accessed, fallback to container
policy: OpCode = 1 [IsResrcOpProtected], Returned Status = Major code:
3(FatalError) Minor code: 2(NoCode) , extraInfo = [prefHost:IAMSuiteAgent,
resource:/oamconsole/afra/alta-v1/dialog_close_ena.png]>
<Feb 13, 2015 11:31:14 PM PST> <Error> <oracle.oam.agent-default>
<BEA-000000> <OAM Server fatal error: OpCode = 1 [IsResrcOpProtected],
Returned Status = Major code: 3(FatalError) Minor code: 2(NoCode) , extraInfo
[prefHost:IAMSuiteAgent
resource:/oamconsole/afra/alta-v1/dialog_resize-se.png]>
<Feb 13, 2015 11:31:14 PM PST> <Error> <oracle.oam.agent-default>
<OAMAGENT-00411> <Failed to access server: MajorCode: FATAL_ERROR, MinorCode:
FATAL_ERROR>
<Feb 13, 2015 11:31:14 PM PST> <Warning> <oracle.oam.agent-default>
<OAMAGENT-00410> <OAM Server can not be accessed, fallback to container
policy: OpCode = 1 [IsResrcOpProtected], Returned Status = Major code:
3(FatalError) Minor code: 2(NoCode) , extraInfo = [prefHost:IAMSuiteAgent,
resource:/oamconsole/afra/alta-v1/d
ialog_resize-se.png]>

```

This is because compatibility mode is not supported for Oracle Access Manager 11.1.1.x.x upgrade. Therefore, it is mandatory to upgrade the system configurations in order to complete the Access Manager upgrade process.

The issue described in this section will be resolved after upgrading the system configurations by running the WLST command `upgradeConfig()` as described in [Section 12.16, "Upgrading System Configuration"](#).

### 25.2.3 Exception While Deploying Application

- If you get the following exception when you deploy `sdpcclient.jar` application, then the SDP library is already installed.

```

<Month <Date>, <Year> <Time> <Time Zone> <Info> <J2EE Deployment SPI>
<BEA-260121> <Initiating deploy operation for application,
oracle.sdp.client#11.1.1@11.1.1 [archive: <ORACLE_
HOME>/communications/modules/oracle.sdp.client_11.1.1/sdpcclient.jar], to oam_
server1 .>
weblogic.management.ManagementException: [Deployer:149007]New source location,
'<ORACLE_HOME>/communications/modules/oracle.sdp.client_11.1.1/sdpcclient.jar',
cannot be deployed to configured application, 'oracle.sdp.client
[LibSpecVersion=11.1.1,LibImplVersion=11.1.1]'. The application source is at
'<ORACLE_SOA_HOME>/communications/modules/oracle.sdp.client_
11.1.1/sdpcclient.jar'. Changing the source location is not allowed for a
previously attempted deployment. Try deploying without specifying the
source.Failed to deploy the application with status failed
Current Status of your Deployment:
Deployment command type: deploy
Deployment State : failed
Deployment Message : weblogic.management.ManagementException:
[Deployer:149007]New source location, '<ORACLE_
HOME>/communications/modules/oracle.sdp.client_11.1.1/sdpcclient.jar', cannot be
deployed to configured application, 'oracle.sdp.client
[LibSpecVersion=11.1.1,LibImplVersion=11.1.1]'. The application source is at
'<ORACLE_SOA_HOME>/communications/modules/oracle.sdp.client_
11.1.1/sdpcclient.jar'. Changing the source location is not allowed for a
previously attempted deployment. Try deploying without specifying the source.
Error occurred while performing deploy : Target exception thrown while deploying

```

```
application: Error occured while performing deploy : Deployment Failed. : Error
occured while performing deploy : Deployment Failed.
Use dumpStack() to view the full stacktrace
Deploying application from <ORACLE_HOME>/oam/server/apps/oam-admin.ear to
targets AdminServer (upload=false) ...
```

Complete the following steps to recover:

1. Log into the WebLogic console.
2. Check for the following library:  
**oracle.sdp.client(11.1.1,11.1.1)**
3. Target this library to oam\_server1
4. Run the following command:

```
deployOAMServer ("<ORACLE_
HOME>", adminTarget="AdminServer", serverTarget="oam_server1")
```

- If you get the following error after the Access Manager server deployment, it is because the tmp and stage directories still exist in your environment.

Ignore it:

```
[HTTP:101216]Servlet: "AMInitServlet" failed to preload on startup in Web
application: "oam".
java.lang.ExceptionInInitializerError
at java.lang.J9VMInternals.initialize(J9VMInternals.java:222)
at
oracle.security.am.engines.sso.adapter.AbstractSessionAdapterImpl.checkAndInit(
AbstractSessionAdapterImpl.java:97)
at
oracle.security.am.engines.sso.adapter.AbstractSessionAdapterImpl.<init>(Abstra
ctSessionAdapterImpl.java:75)
at
oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapterImpl.<init>(Mu
ltipleUserSessionAdapterImpl.java:56)
at
oracle.security.am.engines.sso.adapter.MultipleUserSessionAdapterImpl.<clinit>(
MultipleUserSessionAdapterImpl.java:45)
at java.lang.J9VMInternals.initializeImpl(Native Method)
at java.lang.J9VMInternals.initialize(J9VMInternals.java:200)
at
oracle.security.am.engines.sso.adapter.SessionManagementAdapterFactory.getAdapt
er(SessionManagementAdapterFactory.java:46)
```

## 25.2.4 PolicyValidationException While Restarting Administration Server

During Oracle Access Manager 11.1.1.x.x upgrade, when you restart the Administration Server, the following error occurs if the 11.1.2.3.0 Repository Creation Utility is not new and has data.

```
oracle.security.am.common.policy.admin.impl.PolicyValidationException:
OAMSSA-06045: An object of this type named "HTTP" already exists.
at
oracle.security.am.common.policy.admin.impl.ResourceTypeManagerImpl.isValidWrite(R
esourceTypeManagerImpl.java:482)
at
oracle.security.am.common.policy.admin.impl.ResourceTypeManagerImpl.createResource
Type(ResourceTypeManagerImpl.java:165)
at
```

```

oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.createResourceType(
OAMPolicyStoreBootstrap.java:554)
at
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.addOAMObjs(OAMPolic
yStoreBootstrap.java:328)
at
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.addPolicyObjects(OA
MPolicyStoreBootstrap.java:280)
at
oracle.security.am.common.policy.tools.OAMPolicyStoreBootstrap.bootstrap(OAMPolic
yStoreBootstrap.java:233)
at oracle.security.am.install.OAMInstaller.bootstrapOES(OAMInstaller.java:1064)
at oracle.security.am.install.OAMInstaller.bootstrapPolicy(OAMInstaller.java:1423)
at oracle.security.am.install.OAMInstaller.upgradePolicy(OAMInstaller.java:1513)

```

Check if a new Repository Creation Utility schema is created for Access Manager. Also check if the domain has been updated to use the new 11.1.2.3.0 Repository Creation Utility.

### 25.2.5 Exception While Restarting Managed Server

After you upgrade Oracle Access Manager 11.1.1.x.x to 11.1.2.3.0, when you restart the Access Manager Managed Server, you might see the following error if the folders `tmp` and `stage` still exist:

```

Caused by:
com.bea.security.ParameterException: Invalid configuration: cannot locate class:
com.bea.security.ssal.micro.MicroSecurityServiceManagerWrapper
at
com.bea.security.impl.SecurityRuntimeImpl.getNewInstance(SecurityRuntimeImpl.java:
263)
at
com.bea.security.impl.SecurityRuntimeImpl.initialize(SecurityRuntimeImpl.java:313)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:39)
at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:
25)
at java.lang.reflect.Method.invoke(Method.java:597)
at com.bea.security.SecurityRuntime.initialize(SecurityRuntime.java:140)
at com.bea.security.impl.MicroSMImpl.getInstance(MicroSMImpl.java:167)

```

This error is resolved once you remove the `tmp` and `stage` folders, as instructed in [Section 12.15, "Deleting Folders"](#).

### 25.2.6 Component Version Shows 11.1.1.5.0 After Upgrade

This issue occurs during the following upgrade scenarios:

- If you upgraded Oracle Access Manager 11g Release 1 (11.1.1.5.0) to Access Manager 11.1.2.3.0
- If you upgraded Oracle Access Manager 11g Release 1 (11.1.1.5.0) to 11g Release 2 (11.1.2) first, and then to Access Manager 11.1.2.3.0

If the component versions of the packages `oracle.dogwood.top` and `oracle.oam.server` show 11.1.1.5.0 after upgrade, run the domain updater utility (`com.oracle.cie.domain-update_1.0.0.0.jar`) to update the `domain-info.xml`.

To upgrade the necessary Oracle Access Manager packages to 11.1.2.3.0, complete the following steps:

1. Go to the directory `$ORACLE_HOME/oaam/upgrade`. The domain updater utility `com.oracle.cie.domain-update_1.0.0.0.jar` file is located in this directory.
2. Upgrade the package `oracle.dogwood.top` 11.1.1.5.0 to 11.1.2.3.0 by running the following command:

```
java -cp $MW_
HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
_1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
oracle.dogwood.top:11.1.1.5.0, :11.1.2.3.0
```

For example:

```
java -cp
/scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.or
acle.cie.domain-update_1.0.0.0.jar
com.oracle.cie.external.domain.DomainUpdater
/scratch/Oracle/Middleware/user_projects/domains/OAMDomain
oracle.dogwood.top:11.1.1.5.0, :11.1.2.3.0
```

3. Upgrade the package `oracle.oam.server` 11.1.1.5.0 to 11.1.2.3.0 by running the following command:

```
java -cp $MW_
HOME/utils/config/10.3/config-launch.jar:./com.oracle.cie.domain-update
_1.0.0.0.jar com.oracle.cie.external.domain.DomainUpdater <DOMAIN_HOME>
oracle.oam.server:11.1.1.5.0, :11.1.2.3.0
```

For example:

```
java -cp
/scratch/Oracle/Middleware/utils/config/10.3/config-launch.jar:./com.or
acle.cie.domain-update_1.0.0.0.jar
com.oracle.cie.external.domain.DomainUpdater
/scratch/Oracle/Middleware/user_projects/domains/OAMDomain
oracle.oam.server:11.1.1.5.0, :11.1.2.3.0
```

## 25.2.7 Errors While Starting the Administration Server After Upgrade

When you start the WebLogic Administration Server after you upgrade Access Manager to 11.1.2.3.0, you might see the following errors:

### Error 1:

```
<Error> <Default> <BEA-000000> <Failed to
communicate with any of configured Access Server, ensure that it is up and
running.>
<Error> <Default> <BEA-000000> <Failed to
communicate with any of configured Access Server, ensure that it is up and
running.>
<Warning> <oracle.oam.agent-default>
<OAMAGENT-00410> <OAM Server can not be accessed, fallback to container policy:
fetchConfig failed, will keep trying ...>
```

This happens when the Administration Server is operational and the Access Manager Managed Servers are yet to be started.

You can ignore this error.

**Error-2:**

```
<Error> <oracle.mds> <BEA-000000> <exception thrown failed getMBeanServernull>
```

This error can be ignored.

## 25.2.8 Memory Issues While Running upgradeConfig() Command

The `upgradeConfig()` command performs policy operations to seamlessly migrate the policy stores. This requires higher memory. Therefore, if you see encounter memory issues while running `upgradeConfig()` command, do the following to increase the memory:

1. Go to the directory `WL_HOME/common/bin`, and open the `wlst.sh` file in an editor.
2. Update the memory argument in `wlst.sh` file with the following value:

```
MEM_ARGS="-Xms1024m -Xmx2048m -XX:MaxPermSize=1024m"
```

3. Save the `wlst.sh` file, and rerun the `upgradeConfig()` command.

If you are performing upgrade on IPV6 machine, complete the following steps to resolve memory issues:

1. Go to the directory `WL_HOME/common/bin`, and open the `wlst.sh` file in an editor.
2. Update `JVM_ARGS` to include `-Djava.net.preferIPv4Stack=true` argument as shown in the following example:

```
JVM_ARGS="-Dprod.props.file='${WL_HOME}'/.product.properties
-Djava.net.preferIPv4Stack=true ${WLST_PROPERTIES} ${JVM_D64} ${MEM_ARGS}
${CONFIG_JVM_ARGS}"
```

3. Save the `wlst.sh` file, and rerun the `upgradeConfig()` command.

## 25.2.9 Null Exception While Creating IDS Profile

After you upgrade Oracle Access Manager 11.1.1.x.x to Access Manager 11.1.2.3.0, if you see a null exception while creating Identity Directory Service (IDS) or Enterprise Single Sign-On (ESSO) profile, do the following:

1. Create the directory `DOMAIN_HOME/config/fmwconfig/ovd/ids`.
2. Copy all the files from the directory `MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/domain_config/ovd/ids/` to `DOMAIN_HOME/config/fmwconfig/ovd/ids/` by running the following command:

```
cp MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/domain_config/ovd/ids/* to DOMAIN_HOME/config/fmwconfig/ovd/ids/
```

3. Copy the file `ovd-ids-mbeans.xml` from the location `MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/domain_config/mbeans` to `DOMAIN_HOME/config/fmwconfig/mbeans/` by running the following command:

```
cp MW_HOME/oracle_common/modules/oracle.ovd_11.1.1/domain_config/mbeans/ovd-ids-mbeans.xml DOMAIN_HOME/config/fmwconfig/mbeans/
```

4. Update the Credential Store Framework (CSF) for IDS by running the following command from the location `MW_HOME/oracle_common/bin/`:

```
libovdconfig.sh -domainPath DOMAIN_HOME -contextName ids -host AdminServer_host -port AdminServer_port -userName AdminServer_username
```

In this command,

- `DOMAIN_HOME` is the absolute path to the Access Manager domain.
  - `AdminServer_host` is the hostname of the WebLogic Administration Server.
  - `AdminServer_port` is the port of the WebLogic Administration Server.
  - `AdminServer_username` is the username of the WebLogic Administration console.
5. Restart the WebLogic Administration Server and the Access Manager Managed Server(s).

For information about stopping the servers, see [Section 24.1.9, "Stopping the Servers"](#). For information about starting the servers, see [Section 24.1.8, "Starting the Servers"](#).

### 25.2.10 Post Authentication Rules Tab is Disabled on Oracle Access Management Console After Upgrade

The Post Authentication Rules tab is disabled post-upgrade. The post authentication rules part of the Adaptive Authentication Services in 11.1.2.3.0. Therefore, you must explicitly enable the Adaptive Authentication Services post-upgrade, if required.

For information about enabling and using the Adaptive Authentication Services, see "Using the Adaptive Authentication Service" in the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*.

### 25.2.11 Exception While Running importAccessData Command

When you upgrade Oracle Access Manager 11.1.1.x.x to 11.1.2.3.0, the following exception is seen when you import the access data using `importAccessData` command:

```
OutOfMemoryError
SEVERE: Could not get an access to PolicyAdmin java.lang.NullPointerException
```

To resolve this, complete the following steps:

1. Open the `oam_upgrade.properties` file located at `ORACLE_HOME/oam/server/wlst/scripts/sample_properties/oam_upgrade.properties`, in a text editor.
2. Remove the line `OAM_OFFLINE_POLICY_MIGRATION=true` or set the value of this attribute to `false`.
3. Run the command `importAccessData()` to import the access data.

### 25.2.12 .oamkeystore File Size Reduced to 0 Byte After Extending the OAM Domain

After you extend the OAM domain during the upgrade from 11.1.2.1.0 to 11.2.1.3.0, the `.oamkeystore` file size reduces to zero.

To resolve this, complete the following steps:

1. Take a backup of the `.oamkeystore` file before extending the domain. The `.oamkeystore` file is located in the `DOMAIN_HOME/config/fmwconfig` directory.
2. Extend the OAM domain.
3. Restore the `.oamkeystore` file.
4. Start the servers and processes.

### 25.2.13 upgradeConfig Fails with NullPointerException

When you upgrade OAM from R2PS2 to R2PS3, the upgradeConfig fails with the following error:

```
oracle.security.am.upgrade.framework.psf.plugin.PolicyEntityPlugin process  
SEVERE: Exception while running PSFE PolicyEntityPlugin :  
java.lang.NullPointerException at  
oracle.security.am.common.policy.admin.impl.PolicyUtil.cleanUpPolicy(PolicyUtil.jav  
a:2002
```

To fix this issue, set **OAMEntityStoreR2PS3=true** in the **UpgradeConfig.properties** file.