Oracle® Fusion Middleware

System Integrator's Guide for Oracle Identity Analytics

11*g* Release 1, Patch Set 1 (11.1.1.5)

E23377-02

March 2014

ORACLE

Oracle Fusion Middleware System Integrator's Guide for Oracle Identity Analytics 11*g* Release 1, Patch Set 1 (11.1.1.5)

E23377-02

Primary Author: Deena Purushothaman

Contributing Author: Kevin Kessler

Contents

Preface vii

Audience vii
Documentation Accessibility vii
Related Documents vii
Conventions viii

1 Integrating With Oracle Identity Manager, Preferred Method

1.1 Overview 1-1
1.2 Introduction 1-2
1.3 Understanding Terminology in Oracle Identity Analytics and Oracle Identity Manager 1-2
1.4 To Configure Oracle Identity Analytics and Oracle Identity Manager to Work Together (Preferred Integration Method) 1-2
1.4.1 Step 1: Copy the Required Files From the OIM Server 1-4
1.4.2 Step 2: Edit the Oracle Identity Analytics Configuration Files 1-5
1.4.3 Step 3: Modify the Oracle Identity Manager Forms Using the Form Designer 1-6
1.4.4 Step 4: Configure the Oracle Identity Manager Data Collection Scheduler 1-8
1.4.5 Step 5: Configure Oracle Identity Analytics to Connect to Oracle Identity Manager 1-9
1.4.6 Step 6: Import the Oracle Identity Manager (OIM) Data Into Oracle Identity Analytics (OIA) 1-9
1.4.6.1 To Import Resource Metadata 1-10
1.4.6.2 To Validate That the Parent Attribute for Each Attribute Category is Set 1-11
1.4.6.3 To Import Resources 1-12
1.4.6.4 To Import Glossary Data 1-13
1.4.6.5 To Import Policies 1-13
1.4.6.6 To Import Roles 1-14
1.4.6.7 To Import Users, Accounts, User Role Memberships, and Entitlements 1-15
1.4.6.8 To Verify That Each Import Job Completed Successfully 1-16
1.4.7 Step 7: Configure the Oracle Identity Analytics (OIA) Workflows to Export Data to Oracle Identity Manager (OIM) 1-16
1.4.8 Step 8: Review Oracle Identity Manager Automatic Role Assignment and Role Management Settings 1-18
1.5 To Migrate From the Deprecated OIM-OIA Integration to the Preferred OIM-OIA Integration 1-18
1.6 Understanding Closed Loop Compliance 1-19

1.6.1 To Configure Resources in Oracle Identity Analytics for Remediation 1-20
1.6.2 To Configure Certifications in Oracle Identity Analytics for Remediation 1-20
1.7 Scheduling Incremental Updates of Users, Accounts, User-Role Memberships, and Entitlements 1-20
1.8 Troubleshooting 1-22
1.9 User Attribute Mappings Between OIM and OIA 1-24

2 Integrating With Oracle Identity Manager, Deprecated Method

2.1 Introduction 2-1
2.2 Overview 2-1
2.3 Understanding Terminology in Oracle Identity Analytics and Oracle Identity Manager..... 2-2
2.4 To Configure Oracle Identity Analytics and Oracle Identity Manager to Work Together (Deprecated Integration Method) 2-2
2.4.1 Step 1: Enable Oracle Identity Manager as a Provisioning Server Option..... 2-3
2.4.2 Step 2: Copy the Required .jar Files 2-5
2.4.3 Step 3: Designate Oracle Identity Manager as the Provisioning Server 2-7
2.4.4 Step 4: Enable Real-Time Updates from Oracle Identity Analytics to Oracle Identity Manager 2-7
2.5 Populating Oracle Identity Analytics With User Information From Oracle Identity Manager 2-8
2.5.1 Use Case 1: Importing Global Users From Oracle Identity Manager Into Oracle Identity Analytics 2-8
2.5.1.1 To Import Users From Oracle Identity Manager Into Oracle Identity Analytics..... 2-8
2.5.2 Use Case 2: Importing Resource Metadata From Oracle Identity Manager Into Oracle Identity Analytics 2-9
2.5.2.1 To Import Resource Metadata From Identity Manager Into Oracle Identity Analytics 2-9
2.5.3 Use Case 3: Importing Resources From Identity Manager Into Oracle Identity Analytics 2-10
2.5.3.1 To Import Resources From Identity Manager Into Oracle Identity Analytics 2-10
2.5.4 Use Case 4: Importing Roles From Identity Manager Into Oracle Identity Analytics 2-10
2.5.4.1 To Import Role From Identity Manager Into Oracle Identity Analytics 2-10
2.6 Populating Oracle Identity Manager With Roles Information From Oracle Identity Analytics 2-11
2.6.1 Use Case 1: Exporting Roles From Oracle Identity Analytics to Identity Manager 2-11
2.6.1.1 To Export Roles to Identity Manager 2-11
2.7 Understanding Closed Loop Compliance..... 2-12
2.7.1 To Configure Resources in Oracle Identity Analytics for Remediation 2-12
2.7.2 To Configure Certifications in Oracle Identity Analytics for Remediation 2-13

3 Integrating With Oracle Waveset (Sun Identity Manager)

3.1 Overview 3-1
3.2 Integration Architecture..... 3-3
3.3 Integrating Oracle Identity Analytics With Oracle Waveset..... 3-4
3.3.1 To Configure Oracle Identity Analytics and Oracle Waveset to Work Together 3-4

3.3.1.1 Step 1: To Import the Oracle Waveset SPML Exchange File 3-5
3.3.1.2 Step 2: To Create a Oracle Identity Analytics User That Oracle Waveset Will use to Connect 3-5
3.3.1.3 Step 3: To Create an Oracle Waveset User That Oracle Identity Analytics Will use to Connect 3-6
3.3.1.4 Step 4: To Designate Oracle Waveset as the Provisioning Server 3-6
3.3.1.5 Step 5: To Configure Oracle Waveset to use Oracle Identity Analytics Web Services 3-7
3.3.1.6 Step 6: To Configure the User Deferred Task Scanner 3-8
3.3.1.7 Step 7: To Configure the User Form so That Oracle Identity Analytics can Authenticate Over SPML 3-9
3.4 Populating Oracle Identity Analytics With User Information From Oracle Waveset 3-9
3.4.1 Use Case 1: Importing Global Users From Oracle Waveset Into Oracle Identity Analytics 3-9
3.4.1.1 To Import Users From Oracle Waveset Into Oracle Identity Analytics 3-9
3.4.2 Use Case 2: Importing Resource Metadata From Oracle Waveset Into Oracle Identity Analytics 3-10
3.4.2.1 To Import Resource Metadata From Oracle Waveset Into Oracle Identity Analytics 3-10
3.4.3 Use Case 3: Importing Resources From Oracle Waveset Into Oracle Identity Analytics . 3-11
3.4.3.1 To Import Resources From Oracle Waveset Into Oracle Identity Analytics ... 3-11
3.4.4 Use Case 4: Importing User Accounts From Oracle Waveset Into Oracle Identity Analytics 3-12
3.4.4.1 To Import Accounts From Oracle Waveset Into Oracle Identity Analytics..... 3-12
3.4.5 Use Case 5: Importing Roles From Oracle Waveset Into Oracle Identity Analytics 3-12
3.4.5.1 To Import Role From Oracle Waveset Into Oracle Identity Analytics 3-12
3.5 Populating Oracle Waveset With Roles Information From Oracle Identity Analytics.. 3-13
3.5.1 Use Case 1: Exporting Roles From Oracle Identity Analytics to Oracle Waveset... 3-13
3.5.1.1 To Export Roles to Oracle Waveset..... 3-13
3.6 Understanding Closed Loop Compliance..... 3-14
3.6.1 To Configure Resources in Oracle Identity Analytics for Remediation 3-15
3.6.2 To Configure Certifications in Oracle Identity Analytics for Remediation 3-16
3.7 Oracle Waveset Sample Workflows..... 3-16
3.8 Oracle Identity Analytics Web Services..... 3-17
3.9 Troubleshooting 3-17
3.9.1 System Logs..... 3-17

4 Configuring Oracle Identity Analytics for Web Access Control

4.1 Overview 4-1
4.2 Configuring Oracle Identity Analytics For Web Access Control..... 4-1
4.2.1 To Set Up the http Reader 4-1
4.2.2 To Set Up the Logout URL 4-2
4.3 To Access Oracle Identity Analytics When Using Web Access Control..... 4-3

5 Customizing the Oracle Identity Analytics User Interface

5.1 Overview 5-1

5.2 Before You Begin 5-1
5.3 Configuring Logos 5-1
5.3.1 To Configure a Custom Logo 5-2
5.4 Configuring Labels 5-2
5.4.1 To Modify Menu Labels 5-2
5.4.2 To Modify User Labels 5-3
5.5 Configuring Error Messages 5-4
5.5.1 To Modify My Requests Error Messages 5-4
5.5.2 To Modify Identity Certification Error Messages 5-5
5.6 Configuring the Maximum Number of Identity Certification Records That Should Display in the UI 5-5
5.6.1 To Modify Identity Certification Batch Sizes in the UI 5-6
5.7 Enabling Hidden Pages in the UI 5-6
5.7.1 To Enable the Workflow Tab on the Identity Warehouse Pages 5-6
5.7.2 To Enable the Exclusion Roles Tab on the Identity Warehouse Pages 5-7
A.1 To Integrate OIM and OIA on WebSphere A-1

Preface

This guide describes how to integrate Oracle® Identity Analytics software with other applications in a heterogeneous IT environment. Included in this guide is information about how to integrate with Oracle Identity Manager, which is Oracle's resource provisioning solution.

Audience

The Oracle Identity Analytics 11*g*R1 System Integrator's Guide is written for deployment engineers and service providers who are responsible for integrating Oracle Identity Analytics with other IT systems.

- System administrators and service providers who need information about how to monitor and administer the Oracle Identity Analytics software at a systems level should see the System Administrator's section of the *Administrator's Guide for Oracle Identity Analytics*.
- Compliance officers and IT specialists who need to configure and maintain role management and compliance functionality should see the Business Administrator's section of the *Administrator's Guide for Oracle Identity Analytics*.
- Business managers and other users in a supervisory role who need information about how to use the Oracle Identity Analytics 11*g*R1 software to grant employees and partners access to applications, check for access violations, and so on should see the *User's Guide for Oracle Identity Analytics*.

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 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 Analytics Release 11g R1 PS1 documentation set:

- *Oracle Identity Analytics Release Notes*
- *Oracle Identity Analytics Installation and Upgrade Guide*
- *Oracle Identity Analytics Administrator's Guide*
- *Oracle Identity Analytics User's Guide*
- *Oracle Identity Analytics API Guide*
- *Oracle Identity Analytics Database Administrator's Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	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.

1

Integrating With Oracle Identity Manager, Preferred Method

This chapter contains the following sections:

- Section 1.1, "Overview"
- Section 1.2, "Introduction"
- Section 1.3, "Understanding Terminology in Oracle Identity Analytics and Oracle Identity Manager"
- Section 1.4, "To Configure Oracle Identity Analytics and Oracle Identity Manager to Work Together (Preferred Integration Method)"
- Section 1.5, "To Migrate From the Deprecated OIM-OIA Integration to the Preferred OIM-OIA Integration"
- Section 1.6, "Understanding Closed Loop Compliance"
- Section 1.7, "Scheduling Incremental Updates of Users, Accounts, User-Role Memberships, and Entitlements"
- Section 1.8, "Troubleshooting"
- Section 1.9, "User Attribute Mappings Between OIM and OIA"

1.1 Overview

Oracle® Identity Analytics software and Oracle Identity Manager (OIM) software work together seamlessly when integrated using the Thor-API connection mechanism. When integrated, Oracle Identity Manager serves as the automated provisioning and identity synchronization solution, while Oracle Identity Analytics defines the Role-based Access Control (RBAC) framework, the attestation process, and the approach to Segregation of Duties (SoD) policy enforcement. Rather than assigning individual access entitlements, the RBAC framework allows organizations to assign and unassign roles as a means of controlling user access on various applications.

In a fully-integrated scenario, provisioning and role management works in the following manner:

- OIM is the authoritative source for users, accounts, and entitlements. Any update made to the users or their corresponding accounts is done in OIM.
- Oracle Identity Analytics is the authoritative source for role management and role membership. Oracle Identity Analytics is also the authoritative source for policy entitlement definitions. (*Roles* in Oracle Identity Analytics correspond to *roles* in

OIM 11.*x*, and *groups* in OIM 9.*x*. Further, *policies* in Oracle Identity Analytics correspond to *access policies* in OIM.)

- All roles are defined and created in Oracle Identity Analytics. All entitlements for policies and role-to-user relationships are managed from Oracle Identity Analytics.
- Role, Policy, and Role-Membership updates should no longer be made in Oracle Identity Manager.

1.2 Introduction

This section describes how to configure Oracle Identity Analytics (OIA) and Oracle Identity Manager (OIM) so that the two products can be used together. This newer, preferred integration method uses database imports for users, accounts, and user-role memberships, which allows for incremental imports from Oracle Identity Manager.

Oracle Identity Analytics 11gR1 PS1 (11.1.1.5.0) supports the following versions of Oracle Identity Manager:

- Oracle Identity Manager version 9.1.0.2 BP17 (and higher)
- Oracle Identity Manager 11gR1 PS1 (11.1.1.5.0) (and higher)

The 11.1.1.5.0 release of Oracle Identity Analytics does not support Oracle Identity Manager 11gR1 (version 11.1.1.3.0).

1.3 Understanding Terminology in Oracle Identity Analytics and Oracle Identity Manager

The following table maps Oracle Identity Analytics terminology to Oracle Identity Manager terminology.

Table 1–1 Comparing Oracle Identity Analytics Terminology and Oracle Identity Manager 9.x and 11g Terminology

Oracle Identity Analytics Terminology	Oracle Identity Manager Terminology
Resource Type	Resource Object
Resource Type Attributes (NameSpace Attributes)	Provisioning Attributes and Entitlements
Resource	IT Resource
Global Users	Users or Xellerate End Users
Roles	Groups (9.x) / Roles (11g)
Policies	Access Policies

1.4 To Configure Oracle Identity Analytics and Oracle Identity Manager to Work Together (Preferred Integration Method)

Before You Begin -

- **At least Oracle Identity Manager version 9.1.0.2 BP17 or version 11.1.1.5.0 (11gR1 PS1) is required. (Oracle Identity Manager 11gR1 (version 11.1.1.3.0) is not supported.**)
- **At least Oracle Identity Analytics 11.1.1.5.0 is required.**

- **This integration does not support XL.UserIDReuse=true in OIM.**
- If you will be deploying Oracle Identity Analytics and Oracle Identity Manager to separate WebSphere servers, then complete the steps in Appendix A, "Preparing to Integrate Oracle Identity Manager and Oracle Identity Analytics on WebSphere," before continuing with these steps.
- Both Oracle Identity Manager and Oracle Identity Analytics should be installed on servers running the same version of the application server software, as well as the same version of the Java® Virtual Machine (JVM).

Note: If Oracle Identity Manager and Oracle Identity Analytics are installed on a WebLogic cluster (WebLogic versions 10.3.3 or 10.3.4, only), follow these steps to patch WebLogic before continuing. You do not need to patch WebLogic version 10.3.5.

1. Go to the My Oracle Support website (`https://support.oracle.com`) and choose **Patches & Updates** in the menu.
2. Download Patch Number 10155450 for WebLogic 10.3.3.

   You can also download the patch by searching for Smart Update Patch ID **JUS4**.
3. Use the SmartUpdate tool to install the patch to all nodes of the cluster for both OIM and OIA.
4. Regenerate the OIM server `wlfullclient.jar` file and copy the new JAR file to all OIA server instances.

---

1. Copy the required Oracle Identity Manager API JAR files to Oracle Identity Analytics.

   See Section 1.4.1, "Step 1: Copy the Required Files From the OIM Server."
2. In Oracle Identity Analytics, edit the required and optional configuration files.

   See Section 1.4.2, "Step 2: Edit the Oracle Identity Analytics Configuration Files."
3. In Oracle Identity Manager, log on to the Design Console and edit the required forms.

   See Section 1.4.3, "Step 3: Modify the Oracle Identity Manager Forms Using the Form Designer."
4. In Oracle Identity Manager, configure the data collection scheduler.

   See Section 1.4.4, "Step 4: Configure the Oracle Identity Manager Data Collection Scheduler."
5. In Oracle Identity Analytics, create a connection to Oracle Identity Manager. Establish a connection by entering authentication details.

   See Section 1.4.5, "Step 5: Configure Oracle Identity Analytics to Connect to Oracle Identity Manager."
6. In Oracle Identity Analytics, import data from Oracle Identity Manager.

   See Section 1.4.6, "Step 6: Import the Oracle Identity Manager (OIM) Data Into Oracle Identity Analytics (OIA)."
7. To send real time changes from Oracle Identity Analytics to Oracle Identity Manager, change the Oracle Identity Analytics configuration files related to workflows.

See Section 1.4.7, "Step 7: Configure the Oracle Identity Analytics (OIA) Workflows to Export Data to Oracle Identity Manager (OIM)."

8. In Oracle Identity Manager, review automatic role assignment and role management.

   See Section 1.4.8, "Step 8: Review Oracle Identity Manager Automatic Role Assignment and Role Management Settings."

1.4.1 Step 1: Copy the Required Files From the OIM Server

- Copy the following Oracle Identity Manager Java API JAR files located in the *<OIMDesignConsole>*`/lib` folder to the Oracle Identity Analytics *$RBACX_HOME*`/WEB-INF/lib` folder:
  - `xlAPI.jar`
  - `xlCache.jar`
  - `xlDataObjectBeans.jar`
  - `xlDataObjects.jar`
  - `xlScheduler.jar`
  - `xlUtils.jar`
  - `xlVO.jar`
- Copy the following JAR files located in the *<IDM-HOME>*`/server/lib` folder to the Oracle Identity Analytics *$RBACX_HOME*`/WEB-INF/lib` folder:
  - `xlCrypto.jar`
  - `wlXLSecurityProviders.jar`
  - `xlAuthentication.jar`
  - `xlLogger.jar`
- Copy the `config` folder located at *<OIMDesignConsole>*`/config` and paste it in the Oracle Identity Analytics *$RBACX_HOME*`/xellerate` folder. Create the `xellerate` folder if it does not exist.

  Note: The "config" folder must be copied from an OIM Design Console directory that has been preconfigured to communicate with Oracle Identity Manager.

  In other words, even if the operating systems of the computers hosting the OIM Design Console and Oracle Identity Manager are different, the "config" folder must be copied from an OIM Design Console directory which is configured to communicate with Oracle Identity Manager.

- If using at least Oracle Identity Manager 11.1.1.5.0 (11gR1 PS1), copy the following OIM files to the Oracle Identity Analytics *$RBACX_HOME*`/WEB-INF/lib` folder:
  - `oimclient.jar`

    Use the version located in the *<OIMDesignConsole>*`/lib` folder. (**Important:** Do not use a copy of this JAR file located in any other directory.)

- `iam-platform-utils.jar`

  This file is located in the <*OIMDesignConsole*>`/lib` folder.

- If Oracle Identity Manager 11.1.2.*x* (11gR2), copy the following OIM files to the Oracle Identity Analytics *$RBACX_HOME*/rbacx_staging`/WEB-INF/lib` folder
  - `jrf-api.jar`

    This file is located at *MIDDLEWARE_HOME*//oracle_common/modules/oracle.jrf_11.1.1 folder.
- If deploying to a WebLogic application server, *and if Oracle Identity Analytics and Oracle Identity Manager are on different WebLogic domains*, copy the <*WLS-HOME*>`/server/lib/wlfullclient.jar` file to the Oracle Identity Analytics *$RBACX_HOME*`/WEB-INF/lib` folder.

  Note - If the `wlfullclient.jar` file is not present, follow these steps to generate it:

  1. Type cd<*WLS-HOME*>`/server/lib`, where <*WLS-HOME*> is the base WebLogic installation directory
  2. Type `java -jar wljarbuilder.jar`
  3. Copy the `wlfullclient.jar` file to the *$RBACX_HOME*`/WEB-INF/lib` folder

1.4.2 Step 2: Edit the Oracle Identity Analytics Configuration Files

1. Stop Oracle Identity Analytics.
2. Enable Oracle Identity Manager as a supported provisioning server by editing `iam-context.xml` in the *$RBACX_Home*`/WEB-INF` folder as follows:

   a. Uncomment the following lines at the start of `iam-context.xml`:

   ```
   <import resource="oim-commons-context.xml"/>
   <import resource="oim-11g-context.xml"/> <!-- This also works with at least
   Oracle Identity Manager 9.1.0.2 BP17-->
   ```

   b. Enable the following:

   ```
   <entry key="oracle">
   <ref bean="oimSolution"/>
   </entry>
   ```

   c. Save your changes.
3. (Optional) To map Oracle Identity Manager extended attributes to Oracle Identity Analytics custom properties, add the following mappings to `oim-commons-context.xml` as appropriate:

   - For Users, complete the mapping by updating the value attribute with the Oracle Identity Manager extended attribute name, as follows:

   ```
   <util:map id="iamUserToUserCustomProperties">
   <!--entry key="customProperty1" value="USR_UDF_CUSTOM1"/>
   <entry key="customProperty2" value="usr_udf_cust2"/>
   <entry key="customProperty19" value="usr_udf_cust19"/-->
   </util:map>
   ```

   - For Roles, complete the mapping by updating the value attribute with the Oracle Identity Manager extended attribute name, as follows:
     - For OIM 9.*x* use capital letters for the value:

```
<util:map id="iamRoleCustProperties">
<!--entry key="customProperty1" value="UGP_UDF_CUSTOM1"/-->
</util:map>
```

– For OIM 11.*x* use lowercase letters for the value:

```
<util:map id="iamRoleCustProperties">
<!--entry key="customProperty1" value="ugp_udf_custom1"/-->
</util:map>
```

Save your changes.

4. Start Oracle Identity Analytics.
5. Edit *$RBACX_HOME*/conf/oimjdbc.properties. This should contain the Oracle Identity Manager database information.
   a. Run the OIA Property Encryption Utility to encrypt the database password located in the oimjdbc.properties file.

      For details, see the *Administrator's Guide for Oracle Identity Analytics*, "Securing Oracle Identity Analytics" chapter, "Understanding the Property Encryption Utility" section.

   b. Open the oim-11g-context.xml file for editing and search for the word *password*.
   c. Comment out the oim.jdbc.password line and uncomment the oim.jdbc.password.encrypted line.

      The XML should look like the following sample:

```
<property name="URL" value="${oim.jdbc.url}"/>
<property name="user" value="${oim.jdbc.username}"/>
<!--<property name="password" value="${oim.jdbc.password}"/>-->
<property name="password" value="${oim.jdbc.password.encrypted}"/>
```

   d. Save your changes.

1.4.3 Step 3: Modify the Oracle Identity Manager Forms Using the Form Designer

In this step you will open Form Designer and, for each OIM resource, add the properties that OIA needs to exchange data with OIM.

1. Log in to the Oracle Identity Manager Design Console.
2. Open the Form Designer.
3. For each Resource, the following properties need to be added to some identified feed for accounts, policies, and entitlements imports:
   - **AccountName** - Identifies the unique account in the target system
   - **ITResource** - Identifies the unique IT Resource field for the target system
   - **Entitlement** - Identifies the account attribute designated for privileges
   - **OIAParentAttribute** - This property identifies the parent or mandatory entitlement attributes.

     Add this property only if you have installed at least **OIM 11.1.1.5.0** or at least **OIM 9.1.0.2 BP17**.

     Complete this step as follows:

   a. Locate the Process Form for the given resource.

Note: The `AccountName` and `ITResource` properties are on the parent form, and the `Entitlement` and `OIAParentAttribute` properties are on the child form.

b. Open the child Process Form and create a new version.

c. Click the **Properties** tab.

d. Locate *ONLY ONE* entitlement field per form, click **Add Property**, and add the `Entitlement = true` property setting.

If there are multiple Entitlement child forms, add one `Entitlement = true` property setting per Entitlement form.

e. If you have installed at least **OIM 11.1.1.5.0** or at least **OIM 9.1.0.2 BP17**, add the `OIAParentAttribute` property.

Note: For OIM 11.1.1.5.0, first create the `OIAParentAttribute` property as a custom property. You only need to do this once.

1. In the Design Console, expand **Administration** and click **Lookup Definition**.
2. In the **Code** text box, type `Lookup.FormField.Custom.Properties` and click **Search**.

   The available custom properties are displayed.
3. Click **Add** to add the `OIAParentAttribute` property.

To add the `OIAParentAttribute` property to the form, do the following:

Locate *ONLY ONE* entitlement field per form, click **Add Property**, and add the `OIAParentAttribute = true` property setting. (If you cannot find the `OIAParentAttribute` property, create it as a custom property. See the steps in the note box.)

If there are multiple Entitlement child forms, add one `OIAParentAttribute = true` property setting per Entitlement form.

f. Save the child form and make it active.

Note: If there are multiple child forms, update all of them by repeating steps d, e, and f, before going to the next step.

g. Locate the parent process form and create a new version.

h. Click the **Properties** tab.

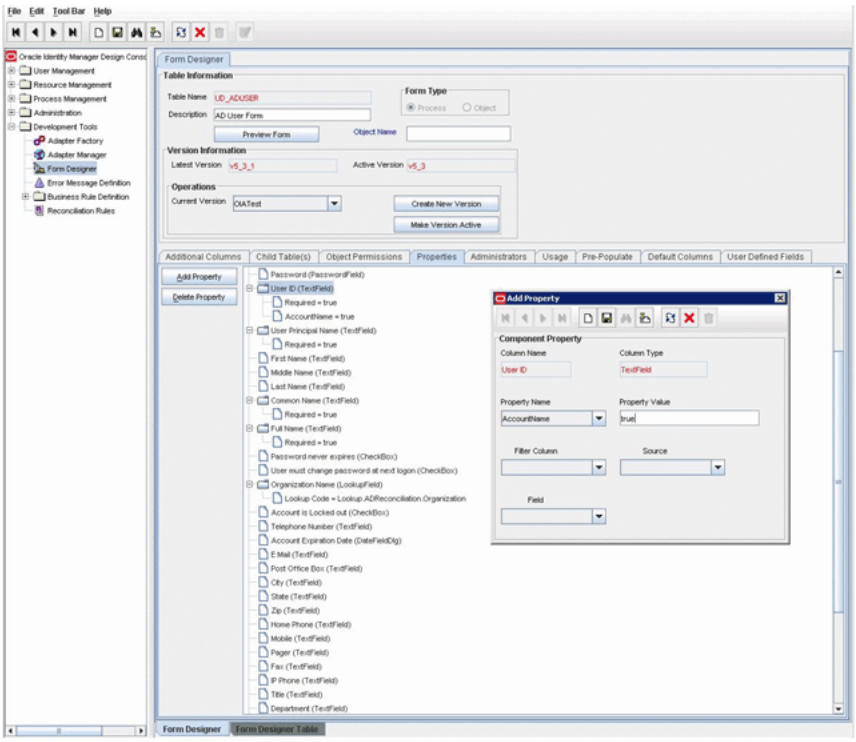
i. Locate the field that uniquely identifies the account in the target system, click **Add Property**, and add the `AccountName = true` property setting. See the following screen capture for an example.

j. Locate the `ITResource` field for the target system, click **Add Property**, and add the `ITResource = true` property setting.

k. Save the parent form and make it active.

4. Repeat for each Resource.
5. Restart the Oracle Identity Analytics server.

Figure 1–1 Modifying the OIM Form Using Form Designer



1.4.4 Step 4: Configure the Oracle Identity Manager Data Collection Scheduler

Use the following steps to register the Oracle Identity Manager scheduled task that is required to support the OIA-OIM integration.

Before You Begin - Verify that the OIM installation/upgrade script created the *DataCollection Schedule Job* in OIM and that the job is enabled but not scheduled for execution. Your integration will not work without this important job.

Follow these steps to register the task with OIM:

1. Enable the DataCollection Schedule task if you are using Oracle Identity Manager 9.1.0.2. (If you are using at least Oracle Identity Manager 11.1.1.5.0, the DataCollection Schedule task is already enabled so you should skip this step.)

   To enable the DataCollection Schedule task, open the Design Console, search for the DataCollection Schedule task, and make it Active.

2. Enable the following system property in Oracle Identity Manager by setting the value to TRUE:

   ```
   OIM.IsOIAIntegrationEnabled = TRUE
   ```

> **Note:** The OIM.IsOIAIntegrationEnabled system property needs to be enabled before role memberships are added in OIM. If the property is not turned on, incremental role memberships will not work. You will need to do a full import of role memberships at least once after this property is enabled.

1.4.5 Step 5: Configure Oracle Identity Analytics to Connect to Oracle Identity Manager

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Configuration**.
3. Click **Provisioning Servers**.
4. Click **New Provisioning Server Connection**.

   The New Provisioning Server Connection wizard asks you to choose the type of provisioning server connection that you want to create.
5. From the **Type of Provisioning Server Connection** drop-down menu, select **oracle** and click **Next**.
6. Complete the form:
   - **Server Name -** Type the Oracle Identity Manager server name.
   - **Xellerate Home -** Type the path to the `xellerate` folder in OIM. (Example: `C:\oracle\xellerate`)

     If Oracle Identity Manager is on a separate machine, create a local `xellerate` folder and copy the `config` folder from `<OIMDesignConsole>` in the `xellerate` folder.
   - **Login Config -** Type the path to the authentication configuration (`auth<AS>.conf`) file. (Example: `C:\oracle\xellerate\config\authwl.conf`)
   - **User Name -** Enter the OIM user name. (For example, `xelsysadm`.) The specified OIM user needs to have system administrator privileges.
   - **Password -** Enter the OIM password.
7. Click Save.

1.4.6 Step 6: Import the Oracle Identity Manager (OIM) Data Into Oracle Identity Analytics (OIA)

Complete this step if you have data in Oracle Identity Manager that you want to use to populate the Oracle Identity Analytics Identity Warehouse. Importing data about Users, Resources, Entitlements, and so on, eliminates the need to manually create this information in Oracle Identity Analytics.

> **WARNING: Importing data from Oracle Identity Manager into Oracle Identity Analytics using this procedure should be a one-time event that takes place when first configuring the systems or when new objects are added in OIM.**

Schedule or run the import jobs in the following order:

1. Import **Resource Metadata**. See Section 1.4.6.1, "To Import Resource Metadata" for details.
2. Validate that the Parent attribute is set. See Section 1.4.6.2, "To Validate That the Parent Attribute for Each Attribute Category is Set" for details
3. Import **Resources**. See Section 1.4.6.3, "To Import Resources" for details.
4. Import the **Glossary Data**. See Section 1.4.6.4, "To Import Glossary Data" for details.

5. Import **Policies**. See Section 1.4.6.5, "To Import Policies" for details.
6. Import **Roles**. See Section 1.4.6.6, "To Import Roles" for details.
7. Import **Users, Accounts, User Role Memberships, and Entitlements**. See Section 1.4.6.7, "To Import Users, Accounts, User Role Memberships, and Entitlements" for details.
8. Verify each import. See Section 1.4.6.8, "To Verify That Each Import Job Completed Successfully" for details.

Understanding how Resource-Attribute Value Import Methods Affect Item-Risk Settings in OIA: You can import Resource-Attribute Values (also called *Entitlements*) when you import Glossary data, when you import Accounts, and when you import Policies.

When you import an Attribute Value as part of a *Glossary import*, and the Attribute Value does not have a specified Item-Risk level, OIA uses the default Entitlements Risk-Mapping level instead. If you later change the Entitlements Risk-Mapping setting, the Item-Risk level for the Attribute Value is not affected.

When you import an Attribute Value as part of either an *Account import* or a *Policy import*, you cannot specify an Item-Risk level. Furthermore, OIA does not assign an Item-Risk level to the Attribute Value (the Item-Risk level remains null). After import, until you directly assign an Item-Risk level to the Value, the Attribute Value inherits the default Risk-Mapping value for Entitlements. This means that if you change the Entitlements Risk-Mapping value, the Attribute Value will inherit the new risk value. To prevent an Attribute Value from continuing to inherit the default Risk-Mapping value, directly assign an Item-Risk level to the Value.

For more information about Item-Risk and Risk-Mapping settings, see the *Administrator's Guide for Oracle Identity Analytics*, "Oracle Identity Analytics Identity Warehouse" chapter, "Understanding Item Risk and Risk-Factor Mappings."

1.4.6.1 To Import Resource Metadata

Before You Begin - You should only import resource metadata when you first configure the systems or when new resource objects are added in OIM.

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Configuration**.
3. Click **Import/Export**.
4. To start a new import job, choose **Schedule Job > Import > Import Resource Metadata**.
5. Under **Data Selection Source**, select the OIM connection that you created in "Step 5: Configure Oracle Identity Analytics to Connect to Oracle Identity Manager" and click **Next**.
6. Complete the form by entering the **Name** and **Description** of the Job.
7. Choose one of the following:
   - To run the job immediately, select the **Run the Job Now** option.

- To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.

8. Click **Finish** to generate the Import Job.

   The import resource metadata job runs on the scheduled date and time.

9. Set (or validate) the parent attribute for each attribute category by following the steps in Section 1.4.6.2, "To Validate That the Parent Attribute for Each Attribute Category is Set."

   Complete this step as a validation step to verify that the parent attribute for each attribute category has been set appropriately.

10. Verify that the resource metadata was properly imported into Oracle Identity Analytics either by accessing the Oracle Identity Analytics Resources Types tab (choose **Configuration > Resources Types**), or by following the steps in Section 1.4.6.8, "To Verify That Each Import Job Completed Successfully."

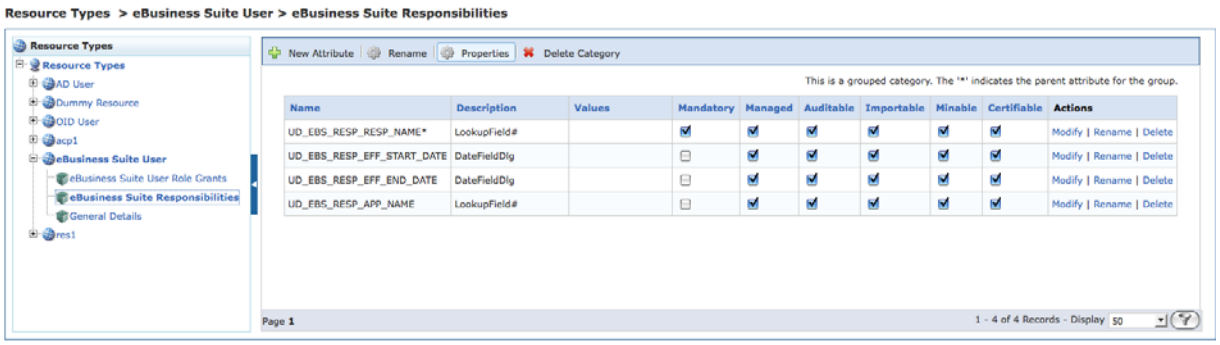
1.4.6.2 To Validate That the Parent Attribute for Each Attribute Category is Set

After Importing Resource Metadata, complete this step as a validation step to verify that the parent attribute for each attribute category has been set appropriately.

Note - This procedure is required if you are running at least OIA 11.1.1.5.0 and OIM 9.1.0.2 BP17, *or* if you are running at least OIA 11.1.1.5.0 and at least OIM 11.1.1.5.0. Follow these steps to manually assign the parent attribute for each attribute category.

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Resource Types**.
4. Click the **+** for each namespace to see the attribute categories for the selected Resource Type.
5. Click an attribute category. Attribute categories correspond to the child forms in OIM.

Figure 1–2 Viewing the Attribute Categories for the Selected Resource Type



6. Click **Properties** in the menu.

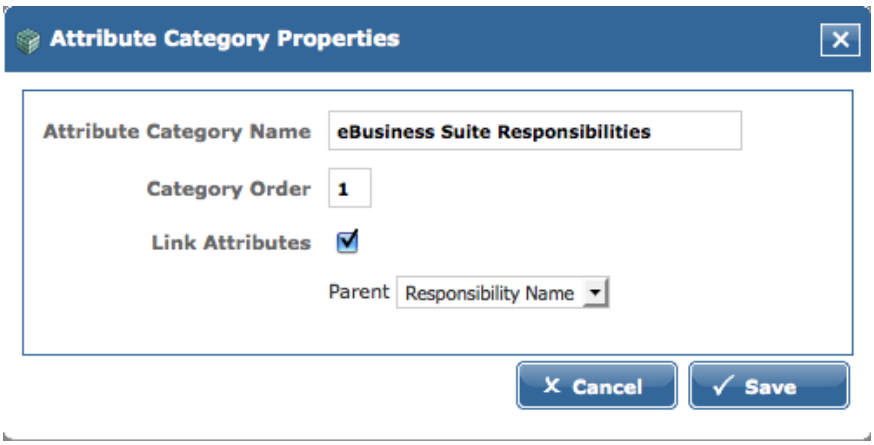
   The Attribute Category Properties dialog box opens.

7. Do the following:

   - Verify that the **Link Attributes** option is selected and that the **Parent** list is set to the field that was marked as the `OIAParentAttribute` in OIM.

- If the correct field is not selected, choose the correct parent attribute from the **Parent** list and click **Save**.

Figure 1–3 Viewing the Attribute Category Properties Dialog Box



1.4.6.3 To Import Resources

Before You Begin - You should only import resources when you first configure the systems or when new Resources are added in OIM.

> **Note:** An *ITResource* in OIM corresponds to a Resource in Oracle Identity Analytics.

1. If necessary, log in to Oracle Identity Analytics, choose **Administration > Configuration**, and click **Import/Export**.
2. To start the import resources job, choose **Schedule Job > Import > Import Resources**.
3. Under **Data Selection Source**, select the OIM connection that you created in "Step 5: Configure Oracle Identity Analytics to Connect to Oracle Identity Manager" and click **Next**.
4. Complete the form by typing a name and description for the job.
5. Choose one of the following tasks:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
6. Click **Finish** to generate the import job.

   The import resources job runs on the scheduled date and time.
7. Verify that the resources are imported into Oracle Identity Analytics from Identity Manager either by accessing the Oracle Identity Analytics Resources tab (choose **Identity Warehouse > Resources**), or by following the steps in Section 1.4.6.8, "To Verify That Each Import Job Completed Successfully."

1.4.6.4 To Import Glossary Data

Before You Begin - You should only import glossary data when you first configure the systems or when new entitlements are discovered in OIM through reconciliation.

Be sure that you understand how the various Resource-Attribute Value import methods affect Item-Risk settings in OIA. See the note in Section 1.4.6 for more information.

1. If necessary, log in to Oracle Identity Analytics, choose **Administration > Configuration**, and click **Import/Export**.
2. To start the import glossary job, choose **Schedule Job > Import > Import Glossary**.
3. Under **Data Selection Source**, select the OIM connection that you created in "Step 5: Configure Oracle Identity Analytics to Connect to Oracle Identity Manager" and click **Next**.
4. Complete the form by typing a name and description for the job.
5. Choose one of the following tasks:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
6. Click **Finish** to generate the import job.

   The import glossary job runs on the scheduled date and time.
7. Verify that the glossary data imported into Oracle Identity Analytics from Identity Manager either by following the steps in Section 1.4.6.8, "To Verify That Each Import Job Completed Successfully."

1.4.6.5 To Import Policies

Before You Begin - Oracle recommends that you only import policy data when you first integrate OIM and OIA.

Be sure that you understand how the various Resource-Attribute Value import methods affect Item-Risk settings in OIA. See the note in Section 1.4.6 for more information.

> **Note:** A policy in OIA cannot represent more than one resource type, whereas in OIM a single access policy can represent multiple resource types. Consequently, when you import an OIM policy that represents multiple resource types, OIA creates a policy instance for each resource type, and appends the name of the resource type to the policy name (for example, *policy1-AD*).
>
> Following integration, you should deprecate the old OIM policies and stop using them. Instead, use the new OIA policies, which will be used for provisioning going forward.

1. If necessary, log in to Oracle Identity Analytics, choose **Administration > Configuration**, and click **Import/Export**.
2. To start the import policies job, choose **Schedule Job > Import > Import Policies**.

3. Under **Data Selection Source**, select the OIM connection that you created in "Step 5: Configure Oracle Identity Analytics to Connect to Oracle Identity Manager" and click **Next**.
4. Complete the form by typing a name and description for the job.
5. Choose one of the following tasks:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
6. Click **Finish** to generate the import job.

   The import policies job runs on the scheduled date and time.
7. Verify that the policies are imported into Oracle Identity Analytics from Identity Manager either by accessing the Oracle Identity Analytics Policies tab (choose **Identity Warehouse > Policies**), or by following the steps in Section 1.4.6.8, "To Verify That Each Import Job Completed Successfully."

1.4.6.6 To Import Roles

Before You Begin - Oracle recommends that you only import roles when you first integrate OIM and OIA.

Note:

- When integrating with Oracle Identity Analytics, Oracle recommends that you no longer use OIM Automatic Role Assignment and Role Management.
- Groups defined in OIM are imported as Roles within Oracle Identity Analytics. In addition, the OIM Group-to-Access-Policy relationship is imported as a Roles-Policy relationship in Oracle Identity Analytics. For the import to work, you should have already successfully completed a Policy import.
- In addition, the OIM Group-User relationship is imported and recreated as a Role-User relationship in Oracle Identity Analytics. To establish the Role-User relationship, verify that you have already imported Users.

---

1. If necessary, log in to Oracle Identity Analytics, choose **Administration > Configuration**, and click **Import/Export**.
2. To start the import roles job, choose **Schedule Job > Import > Import Roles**.
3. Under **Data Selection Source**, select the OIM connection that you created in "Step 5: Configure Oracle Identity Analytics to Connect to Oracle Identity Manager" and click **Next**.
4. Complete the form by typing a name and description for the job.
5. Choose one of the following tasks:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
6. Click **Finish** to generate the import job.

The import resources job runs on the scheduled date and time.

7. Verify that the roles are imported into Oracle Identity Analytics from Identity Manager either by accessing the Oracle Identity Analytics Roles tab (choose **Identity Warehouse > Resources**), or by following the steps in Section 1.4.6.8, "To Verify That Each Import Job Completed Successfully."

1.4.6.7 To Import Users, Accounts, User Role Memberships, and Entitlements

---

Note: Oracle Identity Analytics does not allow the same account instance to be assigned to more than one user, whereas Oracle Identity Manager *does allow* the same account instance to be assigned to more than one user. When importing accounts from OIM, if the same account is assigned to more than one user, OIA will only import the account for the first user.

Before you Begin - Be sure that you understand how the various Resource-Attribute Value import methods affect Item-Risk settings in OIA. See the note in Section 1.4.6 for more information.

1. If necessary, log in to Oracle Identity Analytics, choose **Administration > Configuration**, and click **Import/Export**.
2. To start a new import job, choose **Schedule Job > Import > Import Users, Accounts, User Role Memberships and Entitlements**.
3. Under **Data Selection Source**, select the OIM connection that you created in "Step 5: Configure Oracle Identity Analytics to Connect to Oracle Identity Manager" and click **Next**.
4. Choose one of the following:
   - **Load all resources defined in the system at the time the job is run** - Choose this option to import data from all resources.
   - **Load only those resources selected in the table** - Choose this option to import data only from select resources. If you choose this option, select one or more resources in the table.
5. Complete the form as follows:
   a. Type a name and description for the job.
   b. In the **Data to Load** section, select the **Entitlements** option if you did not perform the Glossary Import job in Section 1.4.6.4. (Selecting **Entitlements** here refers to the list of all available entitlements in a system, and not individual user entitlements. Individual user entitlements are imported when accounts are imported regardless of how you set the **Entitlements** option.)

      Select the **User Role Membership** option to import User-Role membership data.
   c. In the **Import Type** section, choose one of the following:
      – **Full** - All entities found on the OIM server will be imported.
      – **Incremental** - All OIM entities updated since the last successful import will be imported.
   d. Choose one of the following:
      – To run the job immediately, select the **Run the Job Now** option.

- To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.

6. Click **Finish** to generate the import job.

   The import job runs on the scheduled date and time.

7. Verify that the users, accounts, user role memberships, and entitlements are imported into Oracle Identity Analytics from Identity Manager either by accessing the Users View in Oracle Identity Analytics (choose **Identity Warehouse > User**), or by following the steps in Section 1.4.6.8, "To Verify That Each Import Job Completed Successfully."

1.4.6.8 To Verify That Each Import Job Completed Successfully

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Auditing & Events**.
3. Click **Import/Export Logs**.
4. In the table, find the entries for your import jobs.
5. Click the entry in the **Description** column to view the Import Log Details page.
6. Verify that the number or Oracle Identity Manager export records (Number of Output Records) and the number of Oracle Identity Analytics import records (Number of Input Records) are the same.

1.4.7 Step 7: Configure the Oracle Identity Analytics (OIA) Workflows to Export Data to Oracle Identity Manager (OIM)

This section describes how to configure workflows to export data in near real-time from Oracle Identity Analytics (OIA) to Oracle Identity Manager (OIM). As noted earlier, all roles are defined and created in Oracle Identity Analytics. Hence, Oracle Identity Analytics is the authoritative source for role management, role membership, and policy entitlement definitions.

For information about closed loop compliance, see Section 1.6, "Understanding Closed Loop Compliance."

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Workflows**.

   A list of workflows displays.

4. The following workflows need to be modified:
   - Role-creation
   - Role-modification
   - Role-membership
   - Policy Modification

   Modify each configuration file as follows:

   a. Click the workflow name.

   b. In the **Steps** table, scroll down and click the **Finish** step.

      The Edit Workflow Step page opens.

c. Click **Add Pre-Functions**

The Pre-Functions pop-up opens.

d. In the pop-up, select "Export IAM Role Function."

e. Choose the Oracle Identity Manager connection name that you created previously.

f. Click Save.

Repeat these steps until the Role-creation, Role-modification, Role-membership, and Policy Modification workflows have been modified.

5. The "Role-User Membership Activation" workflow needs to be modified as follows:

a. Open the following file in a text editor:

```
$RBACX_HOME/conf/workflows/role-user-membership-activation-workflow.xml
```

b. Search for `step id="5"`.

c. Update the XML fragment to match the following and save your changes:

Note: Replace the placeholder *oimConnectionName* with the provisioning server name that points to the OIM server.

```
<step id="5" name="Finish">
            <meta name="role.status.key">1</meta>
            <meta name="rolestatuslabel">Active</meta>
            <meta name="isMandetory">true</meta>
            <meta name="isEditable">false</meta>
            <pre-functions>
                <function type="spring">
                    <arg
name="bean.name">addSIMRoleMembershipFunction</arg>
                </function>
                <function type="spring">
                    <arg name="bean.name">updateRequestStatusFunction</arg>
                    <arg name="requestStatus">APPROVED</arg>
                </function>
                <function name="addIAMRoleMembershipFunction"
type="spring">
                    <arg
name="bean.name">addIAMRoleMembershipFunction</arg>
                    <arg name="iamConnectionName">oimConnectionName</arg>
                </function>
            </pre-functions>
```

6. The "Mass Modification" workflow needs to be modified as follows:

a. Open the following file in a text editor:

```
$RBACX_HOME/conf/workflows/mass-modification-workflow.xml
```

b. Locate the following section of XML:

```
<!--<function name="exportIAMRoleBatchFunction" type="spring">
    <arg name="bean.name">exportIAMRoleBatchFunction</arg>
    <arg name="iamConnectionName"/>
</function>-->
```

c. Uncomment the XML section, edit it to match the following, and save your changes:

Note: Replace the placeholder *oimConnectionName* with the provisioning server name that points to the OIM server.

```
<function name="exportIAMRoleBatchFunction" type="spring">
    <arg name="bean.name">exportIAMRoleBatchFunction</arg>
    <arg name="iamConnectionName">oimConnectionName</arg>
</function>
```

d. Restart OIA so that changes to the "Role-User Membership Activation" workflow and the "Mass Modification" workflow take effect.

7. The "Mass Membership Modification" workflow needs to be modified as follows:

a. Open the following file in a text editor:

```
$RBACX_HOME/conf/workflows/mass-membership-modification-workflow.xml
```

b. Add the following section of XML to the end of the list of pre-functions within the "Finish" step of the workflow:

```
<function name="exportIAMRoleMembershipBatchFunction" type="spring">
    <arg name="bean.name">exportIAMRoleMembershipBatchFunction</arg>
    <arg name="iamConnectionName"/>
</function>
```

Note: Replace the placeholder *oimConnectionName* with the provisioning server name that points to the OIM server.

c. Restart OIA so that changes to the "Mass Membership Modification" workflow take effect.

8. If OIA is installed in a clustered configuration, repeat step 5, 6, and 7 for each additional cluster node.

1.4.8 Step 8: Review Oracle Identity Manager Automatic Role Assignment and Role Management Settings

When integrating with Oracle Identity Analytics, Oracle recommends that you no longer use OIM Automatic Role Assignment and Role Management.

1.5 To Migrate From the Deprecated OIM-OIA Integration to the Preferred OIM-OIA Integration

If you have an older integration, the following steps must be performed before using the Oracle Identity Analytics 11.1.1.5.0 release. Otherwise, your data will be corrupted and you will end up with many unusable objects in the system.

Before You Begin - Synchronize your Oracle Identity Manager data with your Oracle Identity Analytics data. This step is important!

1. In Oracle Identity Analytics, rename the namespace names from the "Resource Type" names in OIM to the "Resource Object" names in OIM.

Note: You will need to perform the following steps for each OIA namespace that is synchronized with the OIM namespace.

a. Log in to Oracle Identity Analytics.

b. Choose **Administration > Configuration**.

c. Click **Resource Types**.

d. Select the namespace in the tree on the left side of the page, then click **Rename**.

e. Type the new value in the pop-up.

Refer to the `iam-context.xml` file in your OLDER installation, and go to the section with the namespaceMap:

```
<property name = "namespaceMap">
<map>
<entry key = "AD Server">
<value>AD User</value>
</entry>
</map>
</property>
```

Previously, the namespace name in Oracle Identity Analytics used to be `AD Server`, which corresponds to the key value. For the new integration to work, the namespace name in OIA should be `AD User`, which is present in the value element.

f. Repeat these steps to manually replace the key with the OIA value for each namespace specified in the older `iam-context.xml` file.

2. Import your Oracle Identity Manager data into Oracle Identity Analytics. \

This step is required because some minor changes need to be imported into OIA. Going forward, the way data is represented (accounts and policies, especially) can be updated and maintained.

1.6 Understanding Closed Loop Compliance

With the integration of Oracle Identity Analytics and Oracle Identity Manager, it is possible to directly revoke roles and entitlements from Oracle Identity Analytics if the results of the certification process require it. This integration eliminates the need for manual de-provisioning of access for managed resources. In addition, roles and entitlements can still be manually revoked by leveraging the information stored in the remediation configuration module. This takes into account non-managed applications.

If certification remediation is enabled, changes are propagated to Oracle Identity Manager either when the certification is complete, or when the certification end-date is reached (depending on configuration). OIM revokes or re-provisions target system accounts based on the revocations and certifications that occurred during the certification process.

Note: When creating Data Owner certifications, you should only certify parent-level attributes imported from Oracle Identity Manager (attributes with the `OIAParentAttribute` property), not child-level attributes. If a child attribute is certified in a Data Owner certification, closed-loop remediation with OIM will not work.

Child-level attributes that were imported in a text file can be certified provided that the attributes are marked as certifiable using the **Administration > Configuration > Resource Types >** ***Resource*** page.

1.6.1 To Configure Resources in Oracle Identity Analytics for Remediation

Every resource type in Oracle Identity Analytics can be separately configured for automatic or manual remediation.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse> Resources**.
3. Click the resource for which remediation action needs to be configured, and go to the **Remediation** tab.
4. Select the **Select Provisioning Mode** check box.
5. Choose the mode of provisioning desired for the particular resource.
   - **Auto -** Automatically send role/entitlement updates linked with this resource to Oracle Identity Manager.

     Select the appropriate connection name of the provisioning server and save the changes.
   - **Manual -** Use the manual steps for revocation of roles and entitlements using a text editor. List the steps to be followed for non-managed system remediation and save the changes.

1.6.2 To Configure Certifications in Oracle Identity Analytics for Remediation

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Settings**.
3. Click **Identity Certification**.
4. Expand the Revoke and Remediation section, and, under the Remediation section, choose one of the following options:
   - **Display Remediation Instructions -** Select to display instructions about how to perform manual remediation of nonmanaged resources.
   - **Perform Closed Loop Remediation on -** Select to specify that the remediation be completed by either the Certification End Date or the Certification Completion Date.

1.7 Scheduling Incremental Updates of Users, Accounts, User-Role Memberships, and Entitlements

The OIM-OIA Preferred Integration Method allows for incremental imports of users, accounts, user-role memberships, and entitlements from Oracle Identity Manager. Scheduled imports of users, accounts, user-role memberships, and entitlements are

initially configured as part of the OIM-OIA configuration process. (See Section 1.4.6.7, "To Import Users, Accounts, User Role Memberships, and Entitlements" for more information.) Use the steps in this section to schedule additional imports, or to change an existing scheduled import.

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Import/Export**.
4. To start a new import job, choose **Schedule Job > Import > Import Users, Accounts, User Role Memberships and Entitlements**.
5. Under **Data Selection Source**, select the appropriate Connection Name and click **Next**.
6. Choose one of the following:
   - **Load all resources defined in the system at the time the job is run** - Choose this option to import data from all resources.
   - **Load only those resources selected in the table** - Choose this option to import data only from select resources. If you choose this option, select one or more resources in the table.
7. Complete the form as follows:
   a. Type a name and description for the job.
   b. In the **Data to Load** section, select the **Entitlements** option if, in addition to accounts and users, you also want to import the users' entitlements data. Otherwise, clear the **Entitlements** option box and only the accounts, users, and user-role membership data will be imported.
   c. In the **Import Type** section, choose the following option:

      Incremental - All OIM entities updated since the last successful import will be imported.

   d. Choose one of the following:
      – To run the job immediately, select the **Run the Job Now** option.
      – To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.

      Note: For help understanding cron expressions, see "Oracle Identity Analytics Scheduling" in the System Integrator's section of the *Administrator's Guide for Oracle Identity Analytics*.

8. Click **Finish** to generate the import job.

   The import job runs on the scheduled date and time.
9. Verify that the users, accounts, user role memberships, and entitlements are imported into Oracle Identity Analytics from Identity Manager either by accessing the Users View in Oracle Identity Analytics (choose **Identity Warehouse > User**), or by following the steps in Section 1.4.6.8, "To Verify That Each Import Job Completed Successfully."

1.8 Troubleshooting

Issue 1

When OIA tries to connect to OIM, the following error is returned:

```
Illegal Argument Exception thrown ( No Configuration was registered that can
handle the configuration named "xellerate" )
```

Solution: Manually set the security property `auth.login.conf` through `JAVA OPTIONS` before starting the application server:

```
JAVA_OPTIONS="-Djava.security.auth.login.config= /..path../config/authwl.conf
```

Issue 2

When starting OIA, the following error is returned:

```
Caused By: java.lang.LinkageError: loader constraint violation: loader (instance
of weblogic/utils/classloaders/ChangeAwareClassLoader) previously initiated
loading for a different type with name "javax/xml/namespace/QName"
```

Solution: If Oracle Identity Analytics and Oracle Identity Manager are deployed to the same WebLogic domain, remove the `wlfullclient.jar` file from the Oracle Identity Analytics *$RBACX_HOME*`/WEB-INF/lib` folder. This file is only required if Oracle Identity Analytics and Oracle Identity Manager are on different WebLogic domains. The `wlfullclient.jar` file allows client applications, such as Oracle Identity Analytics, to communicate with the WebLogic Server over the T3 protocol.

Issue 3

The following exception is received during integrated operations:

```
java.lang.NoClassDefFoundError:oracle/iam/platform/OIMClient at
Thor.API.tcUtilityFactory.<init>(tcUtilityFactory.java:154) at
com.vaau.rbacx.iam.oracle.OIMIAMSolution.getUtilityFactory(OIMIAMSolution.java:
2595) at com.vaau.rbacx.iam.oracle.OIMIAMSolution.readUsers(OIMIAMSolution.java)
```

Solution: Copy the following 11g Oracle Identity Manager Java API JAR file to the `$OIA-HOME/WEB-INF/lib` folder in Oracle Identity Analytics:

<*OIMDesignConsole*>`/lib/oimclient.jar`

Issue 4

The following error is received during integrated operations:

```
Caused by: java.lang.NoClassDefFoundError: com/thortech/util/logging/Logger at
Thor.API.tcUtilityFactory.<clinit>(tcUtilityFactory.java:80) at
com.vaau.rbacx.iam.oracle.OIMIAMSolution.getUtilityFactory(OIMIAMSolution.java:
2595) at com.vaau.rbacx.iam.oracle.OIMIAMSolution.readUsers(OIMIAMSolution.
java:770) at com.vaau.rbacx.iam.service.impl.RbacxIAMServiceImpl.importUsers
(RbacxIAMServiceImpl.java:119)
```

Solution: Copy the OIM 11g logger JAR file `xlLogger10g.jar` to $RBACX_HOME`/WEB-INF/lib`

Issue 5

Errors similar to the following are written to the OIM log file while any import job is running. OIA does not report any errors.

```
<Warning> <RMI> <BEA-080003> <RuntimeException thrown by rmi server:
```

```
weblogic.jndi.internal.AdminRoleBasedDispatchServerRef@9,
implementation: 'weblogic.jndi.internal.RootNamingNode@fb777e3', oid: '9',
implementationClassName: 'weblogic.jndi.internal.RootNamingNode'
java.lang.SecurityException: [Security:090398]Invalid Subject:
principals=[weblogic, Administrators].
java.lang.SecurityException: [Security:090398]Invalid Subject:
principals=[weblogic, Administrators] at
weblogic.security.service.SecurityServiceManager.seal(SecurityServiceManager.java:
835) at weblogic.security.service.SecurityServiceManager.getSealedSubjectFromWire
(SecurityServiceManager.java:524) at
weblogic.rjvm.MsgAbbrevInputStream.getSubject(MsgAbbrevInputStream.java:351)
at weblogic.rmi.internal.BasicServerRef.acceptRequest(BasicServerRef.java:875)
at weblogic.rmi.internal.BasicServerRef.dispatch(BasicServerRef.java:310)
Truncated. see log file for complete stacktrace
```

Solution:

If Oracle Identity Manager and Oracle Identity Analytics are installed on a WebLogic cluster, follow these steps to patch WebLogic.

1. Go to the My Oracle Support website (https://support.oracle.com) and choose **Patches & Updates** in the menu.
2. Download Patch Number 10155450 for WebLogic 10.3.3.

   You can also download the patch by searching for Smart Update Patch ID **JUS4**.
3. Use the SmartUpdate tool to install the patch to all nodes of the cluster for both OIM and OIA.
4. Regenerate the OIM server `wlfullclient.jar` file and copy the new JAR file to all OIA server instances.

Issue 6

User imports from OIM will fail if the `userbatchsize` is set to a value greater than `1000` in the `iam.properties` files.

Solution:

For User imports from OIM to work, Oracle recommends setting the batch size to a value of `1000` or lower.

Issue 7

When integrating OIA with OIM 9.*x* the following error is logged:

```
ERROR [UDP] failed handling incoming message
java.lang.OutOfMemoryError
at java.util.ArrayList.<init>(ArrayList.java:138)
at org.jgroups.protocols.TP.readMessageList(TP.java:1167)
at org.jgroups.protocols.TP.access$500(TP.java:52)
at org.jgroups.protocols.TP$IncomingPacket.run(TP.java:1417)
at
java.util.concurrent.ThreadPoolExecutor$Worker.runTask(ThreadPoolExecutor.java:665
)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:690)
at java.lang.Thread.run(Thread.java:810)
```

There are two solutions for this issue. Solution 1 is the recommended solution.

Solution 1:

1. Stop Oracle Identity Analytics.

2. Edit the $RBACX/WEB-INF/classes/oscache.properties file by uncommenting the following two lines

   ```
   cache.event.listeners=com.opensymphony.oscache.plugins.clustersupport.JavaGroup
   sBroadcastingListener,com.opensymphony.oscache.extra.CacheMapAccessEventListene
   rImpl
   ```

   and the last

   ```
   cache.cluster.properties= ....
   ```

   (Uncomment the line that has the last property as discard_incompatible_packets=true.)

3. Open the xlconfig.xml file on the OIA server that was copied in Step 1 and search for the following line:

   ```
   <MultiCastAddress>xxx.xxx.xxx.xxx</MultiCastAddress>
   ```

   Comment out the line as follows:

   ```
   <!-- <MultiCastAddress>xxx.xxx.xxx.xxx</MultiCastAddress> -->
   ```

4. Add the following lines, taking care to replace the xxx with the value of the IP address present in the XML file:

   ```
   <MultiCastConfiguration>UDP(mcast_addr=xxx.xx.xxx.xxx;mcast_port=45566;ip_ttl=3
   2;mcast_send_buf_size=150000;mcast_recv_buf_size=80000):PING(timeout=2000;
   num_initial_members=3):MERGE2(min_interval=5000;max_interval=10000):FD_SOCK:VER
   IFY_SUSPECT(timeout=1500):pbcast.NAKACK(gc_lag=50;retransmit_timeout=300,600,12
   00,2400,4800;
   max_xmit_size=8192):UNICAST(timeout=300,600,1200,2400):pbcast.STABLE(desired_av
   g_gossip=20000):FRAG(frag_size=8096;down_thread=false;up_thread=false):pbcast.G
   MS(join_timeout=5000;
   join_retry_timeout=2000;shun=false;print_local_addr=true);discard_incompatible_
   packets=true</MultiCastConfiguration>
   ```

5. Restart Oracle Identity Analytics.

Solution 2:

In the rare case that Solution 1 does not solve the problem do the following:

1. Open the $RBACX\WEB-INF\lib folder and get the file jgroups-all.jar.
2. Unjar the file.
3. Recompile the TP.java file with the variable drop_incompatible_packets = TRUE (the default is FALSE).
4. Recompile the jgroups-all.jar file and put it back in the $RBACX\WEB-INF\lib folder.

You can also contact Support and request a copy of the jgroups-all.jar file that has the drop_incompatible_packets variable set to TRUE.

1.9 User Attribute Mappings Between OIM and OIA

The following table shows how OIM user attributes are mapped to OIA global user attributes during an OIM user import. The OIA columns are located in the oia_staging_users table.

Table 1–2 User Attribute Mappings Between OIM and OIA

OIA Column Name	Type	OIM 9.1 Column	OIM 11g Column	Comments
id	number(19)	-	-	Primary key.
userName	varchar2(256)	usr_login	usr_login	
firstName	varchar2(256)	usr_first_name	usr_first_name	
lastName	varchar2(256)	usr_last_name	usr_last_name	
middleName	varchar2(256)	usr_middle_name	usr_middle_name	
street	varchar2(120)	-	usr_street	
city	varchar2(100)	-	-	
stateOrProvince	varchar2(120)	-	usr_state	
zipOrPostalCode	varchar2(30)	-	USR_POSTAL_CODE	
countryOrRegion	varchar2(100)	-	usr_country	
fax	varchar2(50)	-	usr_fax	
phone	varchar2(50)	-	usr_telephone_number	
extension	varchar2(50)	-	-	
mobile	varchar2(50)	-	usr_mobile	
pager	varchar2(50)	-	usr_pager	
title	varchar2(120)	-	usr_title	
primaryEmail	varchar2(256)	usr_email	usr_email	
secondaryEmail	varchar2(256)	-	-	
officeName	varchar2(100)	-	-	
description	varchar2(512)	-	-	
comments	varchar2(512)	-	-	
status	varchar2(25)	usr_status	usr_status	
suspendedDate	date	-	-	
userData	varchar2(512)	-	-	
employeeId	varchar2(100)	-	-	
customproperty1 *through* customproperty20	varchar2(100)	-	-	
createUser	varchar2(256)	usr_createby	usr_createby	
updateUser	varchar2(256)	usr_updateby	usr_updateby	
created_on	date	usr_create	usr_create	
updated_on	date	usr_update	usr_update	
employeeType	varchar2(255)	usr_emp_type	usr_emp_type	
serviceDeskTicketNumber	varchar2(200)	-	-	
startDate	date	usr_start_date	usr_start_date	

Table 1–2 (Cont.) User Attribute Mappings Between OIM and OIA

OIA Column Name	Type	OIM 9.1 Column	OIM 11g Column	Comments
endDate	date	usr_end_date	usr_end_date	
manager	varchar2(256)	usr_manager	usr_manager	
businessApprover	varchar2(100)	-	-	
technicalApprover	varchar2(100)	-	-	
delegate	varchar2(100)	-	-	
location	varchar2(100)	-	USR_LOCATION	
jobCodes	varchar2(512)	-	-	

The following table shows the database columns that map extended properties in OIM to custom properties in OIA.

Table 1–3 Extended User Property Mappings Between OIM and OIA

Column Name	Type	Comments
user_id	number(19)	Foreign key from staging_users_table
property_name	varchar2(30)	The user defined field name.
property_value	varchar2(2000)	The value of the user defined field in the Users table.

2

Integrating With Oracle Identity Manager, Deprecated Method

This chapter contains the following sections:

- Section 2.1, "Introduction"
- Section 2.2, "Overview"
- Section 2.3, "Understanding Terminology in Oracle Identity Analytics and Oracle Identity Manager"
- Section 2.4, "To Configure Oracle Identity Analytics and Oracle Identity Manager to Work Together (Deprecated Integration Method)"
- Section 2.5, "Populating Oracle Identity Analytics With User Information From Oracle Identity Manager"
- Section 2.6, "Populating Oracle Identity Manager With Roles Information From Oracle Identity Analytics"
- Section 2.7, "Understanding Closed Loop Compliance"

2.1 Introduction

This chapter describes the original approach to configuring Oracle Identity Analytics and Oracle Identity Manager so that the two products can be used together. This older integration method does not support incremental user and account imports. To use this integration method you must have at least Oracle Identity Manager version 9.1.0.2 BP5, and Oracle Identity Analytics 11gR1. A newer, preferred integration method is available that does support incremental user and account imports. For details, see Chapter 1, "Integrating With Oracle Identity Manager, Preferred Method."

2.2 Overview

Oracle Identity Analytics software and Oracle Identity Manager (OIM) software work together seamlessly when integrated using the Thor-API connection mechanism. When integrated, Oracle Identity Manager serves as the automated provisioning and identity synchronization solution, while Oracle Identity Analytics defines the Role-based Access Control (RBAC) framework, the attestation process, and the approach to Segregation of Duties (SoD) policy enforcement. Rather than assigning individual access entitlements, the RBAC framework allows organizations to assign and unassign roles as a means of controlling user access on various applications.

In a fully-integrated scenario, provisioning and role management works in the following manner:

- OIM is the authoritative source for users, accounts, and entitlements. Any update made to the users or their corresponding accounts is done in OIM.
- Oracle Identity Analytics is the authoritative source for role management and role membership. Oracle Identity Analytics is also the authoritative source for policy entitlement definitions. (Roles in Oracle Identity Analytics correspond to "groups" in OIM, and policies in Oracle Identity Analytics correspond to "access policies" in OIM.)
- All roles are defined and created in Oracle Identity Analytics. All entitlements for policies and role-to-user relationships are managed from Oracle Identity Analytics.
- Roles managed by Oracle Identity Analytics become read-only in OIM.

Note - Provisioning attribute definitions for Access Policies, which are required to create accounts, is managed in much the same way as the previous Oracle Role Manager (ORM) - OIM integration (by OIM or external process).

2.3 Understanding Terminology in Oracle Identity Analytics and Oracle Identity Manager

The following table maps Oracle Identity Analytics terminology to Oracle Identity Manager terminology.

Table 2–1 Comparing Oracle Identity Analytics Terminology and Oracle Identity Manager Version 9.x Terminology

Oracle Identity Analytics Terminology	Oracle Identity Manager Terminology
Resource Type	Resource Type
Resource Type Attributes (NameSpace Attributes)	Provisioning Attributes and Entitlements
Resource	IT Resource
Global Users	Xellerate End Users
Roles	Groups
Policies	Access Policies

2.4 To Configure Oracle Identity Analytics and Oracle Identity Manager to Work Together (Deprecated Integration Method)

Before You Begin -

- **At least version 9.1.0.2 BP5 of Oracle Identity Manager and at least version 11gR1 of Oracle Identity Analytics are required.**
- Oracle Identity Manager should be installed and configured.

1. In Oracle Identity Analytics add Oracle Identity Manager as a provisioning server option. ("Sun Identity Manager" and "File" are the default options.)

   See Section 2.4.1, "Step 1: Enable Oracle Identity Manager as a Provisioning Server Option."

2. Copy the required Oracle Identity Manager API JAR files to Oracle Identity Analytics.

   See Section 2.4.2, "Step 2: Copy the Required .jar Files."

3. In Oracle Identity Analytics, designate Oracle Identity Manager as the provisioning server. Establish a connection by entering authentication details.

   See Section 2.4.3, "Step 3: Designate Oracle Identity Manager as the Provisioning Server."

4. To send real time changes from Oracle Identity Analytics to Oracle Identity Manager, change the Oracle Identity Analytics configuration files related to workflows.

2.4.1 Step 1: Enable Oracle Identity Manager as a Provisioning Server Option

In the Oracle Identity Analytics user interface, the **Administration > Configuration > Provisioning Servers** tab displays **file** and **sun** as the available options. To display Oracle Identity Manager as a supported provisioning server, edit `iam-context.xml` in the *RBACX_Home*`/WEB-INF` folder as follows.

Uncomment the `oracle` key entry in the `iamSolutions` property map lines in `iam-context.xml`:

```
<bean id="rbacxIAMService" parent="baseTransactionProxy">
<property name="target">
<bean class="com.vaau.rbacx.iam.service.impl.RbacxIAMServiceImpl"
parent="baseServiceSupport">
<property name="iamSolutions">
<map>
<entry key="sun">
<ref local="waveset"/>
</entry>
<!--entry key="ca">
<ref local="eTrust"/>
</entry-->
<!--entry key="ibm">
<ref local="tim"/>
</entry-->
<entry key="oracle">
<ref local="oim"/>
</entry>
<entry key="file">
<ref local="file"/>
</entry>
</map>
</property>
```

and the second change to this file is to uncomment the bean definition:

```
<bean id="oim" class="com.vaau.rbacx.iam.oracle.OIMIAMSolution"
parent="abstractIAMSolution">

<property name="metadataManager" ref="metadataManager"/>

<property name = "namespaceMap">
<map>
<!-- This mapping fetches the attributes from
the appropriate object form ( AD User). This
mapping clarifies that, for the "AD Server"
resource type, attributes are imported from
the "AD User" Object form in OIM -->
<entry key = "AD Server">
<value>AD User</value>
</entry>
```

```
</map>
</property>
<property name="resourceFieldMap">
<map>
<!-- This mapping identifies the field that is the
ITResourceLookupField for each resource type.
(Oracle Identity Manager "IT resources" map to
resources in Oracle Identity Analytics.) From the mapping
for the "AD Server" resource type field, we
define that the "UD_ADUSER_AD" column field
corresponds to the ITResource Entry. -->
<entry key="AD Server">
<value>UD_ADUSER_AD</value>
</entry>
</map>
</property>

<property name="accountIdentifierMap">
<map>
<entry key="AD Server">
<value>UD_ADUSER_UID</value>
</entry>
</map>
</property>
<property name = "secPolicyMap">
<map>
<entry key = "RACF Account">
<value>Server,Group</value>
</entry>
</map>
</property>
<property name="maxStaleDays">
<value>${com.vaau.rbacx.iam.oracle.maxStaleDays}</value>
</property>
<property name = "excludeFlag" >
<value>${com.vaau.rbacx.iam.oracle.excludeFlag}</value>
</property>

<property name = 'roleDao'>
<ref bean="roleDao"/>
</property>
<property name = "policyManager">
<ref bean = "policyManager"/>
</property>
<property name="userProperties">
<map>
<entry key = "userName">
<value>Users.User ID</value>
</entry>
<entry key = "firstName">
<value>Users.First Name</value>
</entry>
<entry key = "lastName">
<value>Users.Last Name</value>
</entry>
<entry key = "middleName">
<value>Users.Middle Name</value>
</entry>
<entry key = "manager">
<value>Users.Manager Login</value>
```

```
</entry>
<entry key = "primaryEmail">
<value>Users.Email</value>
</entry>
<entry key = "employeeType">
<value>Users.Role</value>
</entry>
<entry key = "startDate">
<value>Users.Start Date</value>
</entry>
<entry key = "endDate">
<value>Users.End Date</value>
</entry>
<entry key = "createDate">
<value>Users.Provisioned Date</value>
</entry>
</map>
</property>
<property name = "customProperties">
<list>
<value>Users.Email</value>
<value>Organizations.Organization Name</value>
<value>USR_UDF_LOCATION</value>
<value>Users.Deprovisioning Date</value>
<value>Users.Xellerate Type</value>
<value>Users.Identity</value>
<value>Users.Lock User</value>
<value>Users.Disable User</value>
<value>Users.Role</value>
</list>
</property>
</bean>
```

2.4.2 Step 2: Copy the Required .jar Files

1. Copy the following Oracle Identity Manager Java API JAR files (located here: *$OIM_HOME*/xellerate/lib/.jar) to the Oracle Identity Analytics *$RBACX_HOME*/WEB-INF/lib folder:
   - wlXLSecurityProviders.jar
   - xlAPI.jar
   - xlAuthentication.jar
   - xlCache.jar
   - xlCrypto.jar
   - xlDataObjectBeans.jar
   - xlDataObjects.jar
   - xlLogger.jar
   - xlScheduler.jar
   - xlUtils.xls
   - xLVO.jar

2. Copy the following Oracle Identity Manager Java API JAR file (located in the `client/ext` folder) to the Oracle Identity Analytics *$RBACX_HOME*`/WEB-INF/lib` folder:
   - `iam-platform-utils.jar`
3. Copy the following JAR files if you are deploying to a JBoss or WebLogic application server:
   - If deploying to a JBoss application server, copy `jbossall-client.jar`
   - If deploying to a WebLogic application server, copy `oim_design_console\xlclient\ext\wlfullclient.jar`

     Note - The `wlfullclient.jar` is only required if Oracle Identity Analytics and Oracle Identity Manager are on different WebLogic domains. This JAR file allows client applications, such as Oracle Identity Analytics, to communicate with the WebLogic Server over the T3 protocol. If you deploy OIA and OIM to the same WebLogic domain, skip this step, otherwise you may receive an error similar to the following:

     ```
     Caused By: java.lang.LinkageError: loader constraint violation: loader
     (instance of weblogic/utils/classloaders/ChangeAwareClassLoader) previously
     initiated loading for a different type with name
     "javax/xml/namespace/QName"
     ```

     If `wlfullclient.jar` is not present in Oracle Identity Manager, follow these steps to generate it:

   a. Type `cd <WLS-HOME>/server/lib`, where `<WLS-HOME>` is the base WebLogic installation directory
   b. Type `java -jar wljarbuilder.jar`
   c. Copy the `wlfullclient.jar` file to the *$RBACX_HOME*`/WEB-INF/lib` folder
4. Copy the following 11g Oracle Identity Manager Java API JAR files to Oracle Identity Analytics:
   a. Copy *$OIM_HOME*`/server/client/oimclient.jar` to *$RBACX_HOME*`/WEB-INF/lib`.

      Note - If this JAR file is not present, you will receive the following exception during integrated operations:

      ```
      java.lang.NoClassDefFoundError:oracle/iam/platform/OIMClient at
      Thor.API.tcUtilityFactory.<init>(tcUtilityFactory.java:154) at
      com.vaau.rbacx.iam.oracle.OIMIAMSolution.getUtilityFactory(OIMIAMSolution.
      java:2595) at
      com.vaau.rbacx.iam.oracle.OIMIAMSolution.readUsers(OIMIAMSolution.java)
      ```

   b. Copy the OIM 11g logger JAR file, `xlLogger10g.jar`, to *$RBACX_HOME*`/WEB-INF/lib`.

      Note - If this JAR file is not present, you will receive the following error during integrated operations:

      ```
      Caused by: java.lang.NoClassDefFoundError: com/thortech/util/logging/Logger
      at Thor.API.tcUtilityFactory.<clinit>(tcUtilityFactory.java:80) at
      com.vaau.rbacx.iam.oracle.OIMIAMSolution.getUtilityFactory(OIMIAMSolution.
      java:2595) at
      com.vaau.rbacx.iam.oracle.OIMIAMSolution.readUsers(OIMIAMSolution.java:770)
      at com.vaau.rbacx.iam.service.impl.RbacxIAMServiceImpl.importUsers(Rbacx
      IAMServiceImpl.java:119)
      ```

2.4.3 Step 3: Designate Oracle Identity Manager as the Provisioning Server

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Provisioning Servers**.
4. Click **New Provisioning Server Connection**.

   The New Provisioning Server Connection wizard asks you to choose the type of provisioning server connection that you want to create.
5. From the **Type of Provisioning Server Connection** drop-down menu, select **Oracle** and click **Next**.
6. Complete the form:
   - **Server Name -** Type the connection object name.
   - **Xellerate Home -** Type the path to the config file in OIM. (For example, `C:\oracle\xellerate`)
   - **Login Config -** Type the path to the authentication configuration (`auth.config`) file. (For example, `C:\oracle\xellerate\config\auth.conf`)
   - **Provider URL -** Type the provider URL. The format for this field is as follows:
     - **WebLogic -** `t3://host:7001`
     - **JBoss -** `jnp://host:1099` (The default port number in a clustered environment is 1100.)
     - **WebSphere -** `corbaloc:iiop:host:2809`
   - **Initial Context Factory -** Enter the name of the environment property for specifying the initial context factory. The default values are as follows:
     - **WebLogic -** `weblogic.jndi.WLInitialContextFactory`
     - **JBoss -** `org.jnp.interfaces.NamingContextFactory`
     - **WebSphere -** `com.ibm.websphere.naming.WsnInitialContextFactory`
   - **User Name -** Enter the OIM user name. (example: `xelsysadm`)
   - **Password -** Enter the OIM password.

2.4.4 Step 4: Enable Real-Time Updates from Oracle Identity Analytics to Oracle Identity Manager

To send real-time changes from Oracle Identity Analytics to Oracle Identity Manager, change the configuration files related to workflows.

For example, the following code snippet has to be enabled in `role-creation-workflow.xml` during the "Finish" step (step 6):

```
<!--<function name="exportIAMRoleFunction" type="spring">
<arg name="bean.name">exportIAMRoleFunction</arg>
<arg name="iamConnectionName"/>
</function>-->
```

This becomes the following:

```
<function name="exportIAMRoleFunction" type="spring">
```

```
<arg name="bean.name">exportIAMRoleFunction</arg>
<arg name="iamConnectionName">OIMConnectionObjectName</arg>
</function>
```

Note - `OIMConnectionObjectName` is the name of the connection object you define in Step 2. Similar changes have to be made for all role related workflows: `role-modification-workflow.xml`, `role-user-membership-workflow.xml`, `role-user-membership-activation-workflow.xml`

2.5 Populating Oracle Identity Analytics With User Information From Oracle Identity Manager

Refer to the use cases in this section if you have user entitlements in Oracle Identity Manager that you want to use to populate the Oracle Identity Analytics Identity Warehouse. Importing users and roles from Identity Manager into Oracle Identity Analytics should be a one-time event that takes place when first configuring the systems.

2.5.1 Use Case 1: Importing Global Users From Oracle Identity Manager Into Oracle Identity Analytics

The users existing in Oracle Identity Manager (Xellerate End Users) are imported as global users in Oracle Identity Analytics on a scheduled basis. The attributes of the users in OIM are mapped to global user properties in Oracle Identity Analytics by way of a map. Extended attributes in OIM can be imported as custom properties in Oracle Identity Analytics.

The following table contains the default mapping of user attributes between Oracle Identity Analytics and Oracle Identity Manager.

Table 2–2 User Attribute Mappings Between Oracle Identity Analytics and Oracle Identity Manager

Oracle Identity Analytics User Attribute Name	Oracle Identity Manager (OIM) User Attribute Name
username	Users.UserID
firstname	Users.First Name
lastname	Users.Last Name
middlename	Users.Middle Name
manager	Users.Manager Login
primaryemail	Users.Email
startdate	Users.Start Date
enddate	Users.End Date
createdate	Users.Provisioned Date

2.5.1.1 To Import Users From Oracle Identity Manager Into Oracle Identity Analytics

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Configuration**.
3. Click **Import/Export**.

4. To start a new import job, choose **Schedule Job > Import > Import Users**.
5. Under **Data Selection Source**, select the appropriate **Connection Name** and click **Next**.
6. Complete the form by entering the **Name** and **Description** of the Job.
7. Choose one of the following tasks:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
8. Click **Finish**.

   The import users job runs on the scheduled date and time.
9. Verify that the users are imported into Oracle Identity Analytics from Identity Manager by accessing the Users View in Oracle Identity Analytics (choose **Identity Warehouse > User**).

2.5.2 Use Case 2: Importing Resource Metadata From Oracle Identity Manager Into Oracle Identity Analytics

In the Oracle Identity Analytics integration with Identity Manager, information on resource metadata can be imported from Identity Manager to Oracle Identity Analytics. This eliminates the need to manually recreate resource metadata in Oracle Identity Analytics.

2.5.2.1 To Import Resource Metadata From Identity Manager Into Oracle Identity Analytics

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Import/Export**.
4. To start a new import job, choose **Schedule Job > Import > Import Resource Metadata**.

   The next page will prompt you to choose the resource from the list of available resources for which metadata on attributes needs to be imported.
5. Select the specific resource type.
6. Under **Data Selection Source**, select the appropriate Connection Name and click **Next**.
7. Complete the form by entering the **Name** and **Description** of the Job.
8. Choose one of the following:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
9. Click **Finish** to generate the Import Job.

   The import resource metadata job runs on the scheduled date and time.
10. Verify that the resource metadata was properly imported into Oracle Identity Analytics by accessing the Oracle Identity Analytics Resources Types tab (choose **Configuration > Resources Types**).

2.5.3 Use Case 3: Importing Resources From Identity Manager Into Oracle Identity Analytics

With out-of-the-box integration capabilities, Oracle Identity Analytics can import resources from Oracle Identity Manager to Oracle Identity Analytics. This eliminates the need to manually create the resources in Oracle Identity Analytics. ITResource in OIM corresponds to a resource in Oracle Identity Analytics.

2.5.3.1 To Import Resources From Identity Manager Into Oracle Identity Analytics

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Import/Export**.
4. To start a new import job, choose **Schedule Job > Import > Import Resources**.
5. Under **Data Selection Source**, select the appropriate Connection Name and click **Next**.
6. Complete the form by typing a name and description for the job.
7. Choose one of the following tasks:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
8. Click **Finish** to generate the import job.

   The import resources job runs on the scheduled date and time.
9. Verify that the resources are imported into Oracle Identity Analytics from Identity Manager by accessing the Oracle Identity Analytics Resources tab (choose **Identity Warehouse > Resources**).

2.5.4 Use Case 4: Importing Roles From Identity Manager Into Oracle Identity Analytics

Groups defined in OIM are imported as Roles within Oracle Identity Analytics. This import also pulls in the relationship between the Group to Access Policy within OIM as Roles-Policy relationship within Oracle Identity Analytics. This requires a successful policy import.

In addition, this step also imports the group-user relationship from OIM and recreates it as a role-user relationship in Oracle Identity Analytics. To establish role-user relationship, ensure that users are imported.

2.5.4.1 To Import Role From Identity Manager Into Oracle Identity Analytics

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Import/Export**.
4. To start a new import job, choose **Schedule Job > Import > Import Roles**.
5. Under **Data Selection Source**, select the appropriate Connection Name and click **Next**.
6. Complete the form by typing a name and description for the job.
7. Choose one of the following tasks:

- To run the job immediately, select the **Run the Job Now** option.
- To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.

8. Click **Finish** to generate the import job.

   The import resources job runs on the scheduled date and time.

9. Verify that the roles are imported into Oracle Identity Analytics from Identity Manager by accessing the Oracle Identity Analytics Roles tab (choose **Identity Warehouse > Resources**).

2.6 Populating Oracle Identity Manager With Roles Information From Oracle Identity Analytics

See the use cases in this section if you have user accounts in Oracle Identity Analytics that you want to use to populate the Identity Manager repository.

Roles defined in Oracle Identity Analytics can be exported to OIM on a scheduled basis, once role definition/management is completed. This use case will perform the following exports into OIM:

1. Export Oracle Identity Analytics roles to OIM groups.
2. Export the Oracle Identity Analytics policy definition and its entitlements from Oracle Identity Analytics into OIM Access Policies. If the policy does not exist it would create the new policy as Access Policies within OIM.
3. Export the Oracle Identity Analytics Policy-Resource relationship as OIM Access Policy- ITResource relationship.
4. Export the Oracle Identity Analytics Role-Policy relationship as OIM Group-Access Policy relationship.
5. Export the Oracle Identity Analytics Role-User relationship to OIM Group-User relationship.

Note: During initial integration this is done on a scheduled basis. A recommended long-term solution is to update OIM as definitions are changed in Oracle Identity Analytics on a real-time basis.

2.6.1 Use Case 1: Exporting Roles From Oracle Identity Analytics to Identity Manager

---

Note:

- Roles in Oracle Identity Analytics correspond to Groups in Identity Manager.
- Policies (roles content) are exported as part of roles export. Therefore when the Export Roles scheduled job is run, the associated policies will also get exported from OIA to OIM.

2.6.1.1 To Export Roles to Identity Manager

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.

3. Click **Import/Export**.
4. To start a new export job, choose **Schedule Job > Export> Export Roles**.
5. Under **Data Selection Source**, select the appropriate Connection Name and click **Next**.
6. Complete the form by entering the **Name** and **Description** of the Job.
7. Choose one of the following:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
8. Click **Finish** to create the Import Job.

   The job runs on the scheduled date and time.
9. Verify that the roles were properly exported to Identity Manager by opening Identity Manager and clicking the **User Group > Manage** link on the left pane.

2.7 Understanding Closed Loop Compliance

With the integration of Oracle Identity Analytics and Oracle Identity Manager, it is possible to directly revoke roles and entitlements from Oracle Identity Manager if the results of the certification process require it. This integration eliminates the need for manual de-provisioning of access for managed resources. In addition, the manual process of revoking roles and entitlements by leveraging the information stored in the remediation configuration module is also retained. This takes into account non-managed applications.

If certification remediation is enabled, changes are propagated to Oracle Identity Manager either when the certification is complete, or when the certification end-date is reached (depending on configuration). OIM revokes or re-provisions target system accounts based on the revocations and certifications that occurred during the certification process.

2.7.1 To Configure Resources in Oracle Identity Analytics for Remediation

Every resource type in Oracle Identity Analytics can be separately configured for automatic or manual remediation.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse> Resources**.
3. Click the resource for which remediation action needs to be configured, and go to the **Remediation** tab.
4. Select the **Select Provisioning Mode** check box.
5. Choose the mode of provisioning desired for the particular resource.
   - **Auto -** Automatically send role/entitlement updates linked with this resource to Oracle Identity Manager. Select the appropriate connection name of the provisioning server and save the changes.
   - **Manual -** Use the manual steps for revocation of roles and entitlements using a text editor. List the steps to be followed for non-managed system remediation and save the changes.

2.7.2 To Configure Certifications in Oracle Identity Analytics for Remediation

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Identity Certification**.
4. Expand the Revoke and Remediation section, and, under the Remediation section, choose one of the following options:
   - **Display Remediation Instructions -** Select to display instructions about how to perform manual remediation of nonmanaged resources.
   - **Perform Closed Loop Remediation on -** Select to specify that the remediation be completed by either the Certification End Date or the Certification Completion Date.

3

Integrating With Oracle Waveset (Sun Identity Manager)

This chapter contains the following sections:

- Section 3.1, "Overview"
- Section 3.2, "Integration Architecture"
- Section 3.3, "Integrating Oracle Identity Analytics With Oracle Waveset"
- Section 3.4, "Populating Oracle Identity Analytics With User Information From Oracle Waveset"
- Section 3.5, "Populating Oracle Waveset With Roles Information From Oracle Identity Analytics"
- Section 3.6, "Understanding Closed Loop Compliance"
- Section 3.7, "Oracle Waveset Sample Workflows"
- Section 3.8, "Oracle Identity Analytics Web Services"
- Section 3.9, "Troubleshooting"

3.1 Overview

Oracle Identity Analytics software and Oracle Waveset software (formerly named Sun Identity Manager) work together seamlessly when integrated using the Service Provisioning Mark-Up Language (SPML). When integrated, Oracle Waveset serves as the automated provisioning and identity synchronization solution, while Oracle Identity Analytics defines the Role-based Access Control (RBAC) framework, the attestation process, and the approach to Segregation Of Duties (SoD) policy enforcement. Rather than assigning individual access entitlements, the RBAC framework allows organizations to assign and unassign roles as a means of controlling user access on various applications.

The Oracle Identity Analytics Identity Warehouse makes it possible for Oracle Identity Analytics to manage users and their identities across various target systems. Before Oracle Identity Analytics features can be utilized, however, the Identity Warehouse of users and their entitlements must be built. If Oracle Waveset is already in use, building the Identity Warehouse is as easy as connecting to Oracle Waveset and importing the user entitlement information that is stored in the Oracle Waveset repository. Roles are then assigned to users, either based on their actual entitlements or business-level attributes. These roles can be exported to Oracle Waveset for user management and provisioning purposes. Additionally, revocations made during the

certification campaigns can also be sent from Oracle Identity Analytics to Oracle Waveset so that remediation can take place.

Figure 3–1 OIA and Oracle Waveset Integration Overview

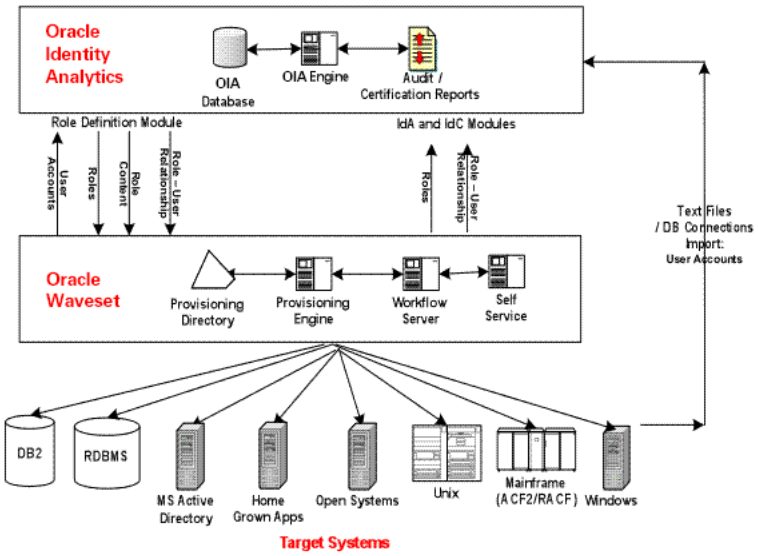
Refer to the *User's Guide for Oracle Identity Analytics* for explanations of attributes, attribute categories, resource types, and other concepts.

Oracle Identity Analytics and Oracle Waveset share the following integration points:

- Oracle Waveset *users* are imported into Oracle Identity Analytics
- Oracle Waveset *resources* are imported into Oracle Identity Analytics
- Oracle Waveset *resource metadata* is imported into Oracle Identity Analytics
- Oracle Waveset *user accounts* are imported into Oracle Identity Analytics
- Oracle Identity Analytics *roles* and *role content* are exported to Oracle Waveset
- Closed Loop Compliance

> **Note:** See the "Oracle Identity Analytics Importing" chapter in the *Administrator's Guide for Oracle Identity Analytics* for more information about the import process.

Figure 3–2 OIA and Oracle Waveset Integration Diagram 1

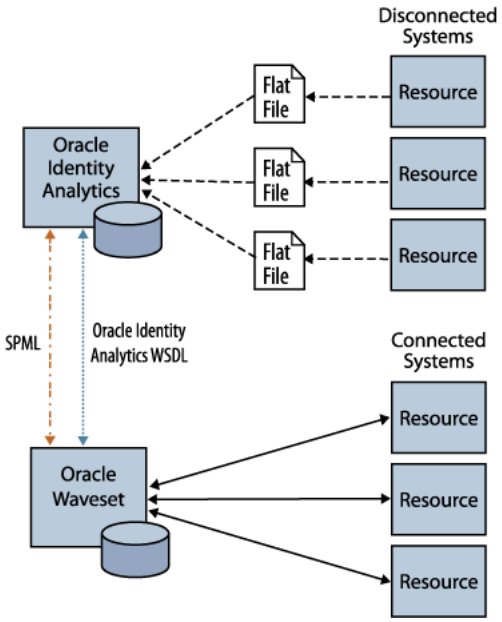


3.2 Integration Architecture

As illustrated in the following figure, Oracle Waveset and Oracle Identity Analytics use SPML and Web Services (WSDL) to communicate. SPML calls are used when Oracle Identity Analytics initiates requests, and Web Services are used when Oracle Waveset initiates the requests.

User and entitlement data can be imported into Oracle Identity Analytics using flat files. In an environment where Oracle Waveset is already deployed, however, (or is in the process of being deployed) Oracle Identity Analytics can connect to Oracle Waveset using SPML to import the user and entitlement data of managed resources. Oracle Identity Analytics can also be used to export roles and user-role membership, and send revocations back to Oracle Waveset.

Figure 3–3 OIA and Oracle Waveset Integration Diagram 2



3.3 Integrating Oracle Identity Analytics With Oracle Waveset

This section describes how to configure Oracle Identity Analytics and Oracle Waveset so that the two products can be used together.

3.3.1 To Configure Oracle Identity Analytics and Oracle Waveset to Work Together

Before You Begin -

- **At least version 8.1.1 of Oracle Waveset and at least version 11gR1 of Oracle Identity Analytics are required.**
- Install and configure Oracle Waveset with the Oracle Waveset Gateway.
- In a production environment, deploy Oracle Waveset and Oracle Identity Analytics on separate application servers.
- If you are running Oracle Waveset on the WebLogic application server, install the Metro libraries in the Waveset `WEB-INF/lib` directory. For details, see *Oracle Waveset Installation 8.1.1*, "Installing Waveset on WebLogic," "Step 5: Install the Metro Libraries."

1. In Oracle Waveset, import the SPML Exchange File so that Oracle Waveset can receive (and respond to) SPML requests sent from Oracle Identity Analytics. The SPML Exchange File (`rm_idm_init.xml`) is supplied with Oracle Identity Analytics.

   See Section 3.3.1.1, "Step 1: To Import the Oracle Waveset SPML Exchange File" for details.

2. In Oracle Identity Analytics, create an Oracle Identity Analytics user that Oracle Waveset will use to connect to Oracle Identity Analytics using Web Services.

   See Section 3.3.1.2, "Step 2: To Create a Oracle Identity Analytics User That Oracle Waveset Will use to Connect" for details.

3. In Oracle Waveset, create an Oracle Waveset user that Oracle Identity Analytics will use to invoke SPML calls to Oracle Waveset.

   See Section 3.3.1.3, "Step 3: To Create an Oracle Waveset User That Oracle Identity Analytics Will use to Connect" for details.

4. In Oracle Identity Analytics, designate Oracle Waveset as the provisioning server.

   See Section 3.3.1.4, "Step 4: To Designate Oracle Waveset as the Provisioning Server" for details.

5. In Oracle Waveset, add Oracle Identity Analytics Web Services so that Oracle Waveset can send requests to (and receive responses from) Oracle Identity Analytics.

   See Section 3.3.1.5, "Step 5: To Configure Oracle Waveset to use Oracle Identity Analytics Web Services" for details.

6. In Oracle Waveset, configure the User Deferred Task Scanner. This step is required so that real-time Segregation of Duties (SoD) processing will work properly.

   See Section 3.3.1.6, "Step 6: To Configure the User Deferred Task Scanner" for details.

7. In Oracle Waveset, configure the User Form so that Oracle Identity Analytics can authenticate over SPML.

   See Section 3.3.1.7, "Step 7: To Configure the User Form so That Oracle Identity Analytics can Authenticate Over SPML" for details.

8. Configure Oracle Identity Analytics for closed loop remediation.

   For details, see Section 3.6, "Understanding Closed Loop Compliance."

3.3.1.1 Step 1: To Import the Oracle Waveset SPML Exchange File

1. Copy the `rm_idm_init.xml` file, which is located in the Oracle Identity Analytics `conf/spml` directory, to the Oracle Waveset server.
2. Log in to Oracle Waveset.
3. Choose **Configure > Import Exchange File**.
4. Click **Browse** and navigate to the `rm_idm_init.xml` file.
5. Click **Import**.

   The exchange file import status is displayed on the Admin Console.

6. Restart the Oracle Waveset application server.

3.3.1.2 Step 2: To Create a Oracle Identity Analytics User That Oracle Waveset Will use to Connect

1. Log in to Oracle Identity Analytics.
2. Create a user that Oracle Waveset can use to connect to Oracle Identity Analytics using Oracle Identity Analytics Web Services.

   For help creating an Oracle Identity Analytics user, see the *Administrator's Guide for Oracle Identity Analytics*, "Oracle Identity Analytics Access Control" chapter, To Create, Update, and Delete an Oracle Identity Analytics User task.

   a. Assign the user the **SRMAdmin** system role.

   b. Save the user.

3.3.1.3 Step 3: To Create an Oracle Waveset User That Oracle Identity Analytics Will use to Connect

1. Log in to Oracle Waveset.
2. Create a user that Oracle Identity Analytics can use to invoke SPML calls to Oracle Waveset. For help creating an Oracle Waveset user, see the *Oracle Waveset Business Administrator's Guide*, "Administration" chapter, To Create an Administrator task.
    1. If you are using Oracle Waveset 8.1.1, assign the user the "Identity Analytics Admin" admin role, and skip to step c. Otherwise, in at least version 8.1.1 of Oracle Waveset, assign the user the following capabilities:
        - Create User
        - Deprovision User
        - Update User
        - Unlink User
        - Unassign User
        - Rename User
        - Enable User
        - Disable User
        - View User
        - Role Administrator
    2. Assign the user control of the `Top` organization.
    3. Assign the user the Empty Form as its User Form.
    4. Save the user.

3.3.1.4 Step 4: To Designate Oracle Waveset as the Provisioning Server

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Provisioning Servers**.
4. Click **New Provisioning Server Connection**.

    The New Provisioning Server Connection wizard asks you to choose the type of provisioning server connection to create.
5. From the **Type of Provisioning Server Connection** drop-down menu, select **Sun** and click **Next**.
6. Complete the form:
    - **Connection Name -** Type a new connection name for Oracle Waveset. This connection name is used during the import process instead of the host name and port.
    - **SPML URL -** Format the SPML URL as follows: `http://`*IdentityManagerApplicationServerName*`:`*PortNumber*`/idm/servlet/rpcrouter2`

      For example: `http://localhost:8080/idm/servlet/rpcrouter2`

- **Username -** Type a user name that Oracle Identity Analytics will use to connect to Oracle Waveset. You should have created a special Oracle Waveset user account for this purpose in step 3. Do not use the configurator account.
- **Password -** Type the password that Oracle Identity Analytics will use to connect to Oracle Waveset.
- **Test Connection -** Click to test whether the connection was successfully established between Oracle Waveset and Oracle Identity Analytics. This will help you in troubleshooting connection issues.
- **Role Consumer -** Select this box to export roles and role content from Oracle Identity Analytics to Oracle Waveset on a real-time basis. Oracle recommends that you select this option.
- **Role Update Schedule -** Choose to schedule when to send updates back to Oracle Waveset.
  - **Now** - Updates roles in Oracle Waveset as soon as they are updated in Oracle Identity Analytics.
  - **Later**- Schedules the update of roles to take place on a daily, weekly, or monthly basis, or just one time, and schedules the time and date for the update task to start.

3.3.1.5 Step 5: To Configure Oracle Waveset to use Oracle Identity Analytics Web Services

Oracle Waveset needs to be configured to use Oracle Identity Analytics Web Services. Oracle Waveset uses Oracle Identity Analytics web service calls to both send requests to Oracle Identity Analytics, and receive responses. To configure Oracle Identity Analytics Web Services, use the Oracle Waveset resource wizard.

1. Log in to Oracle Waveset.
2. Choose the **Resources** tab and verify that the **List Resources** subtab is selected.
3. Locate the **Resource Type Actions** drop-down list and select **New Resource**.

   The New Resource page opens.
4. Select the **Oracle Identity Analytics (Sun Role Manager) Web Services** resource type from the drop-down list, and click **New**. (If this resource type is not listed, you need to enable it. See "Managing the Resources List" in the "Roles and Resources" chapter in the *Oracle Waveset Business Administrator's Guide* for details.)

   The Resource Wizard Welcome Page opens.
5. Click **Next** to begin configuring the Oracle Identity Analytics (Role Manager) Web Services resource.

   The Create Oracle Identity Analytics (Sun Role Manager) Web Services Resource Wizard / Resource Parameters page opens.
6. Complete the form:
   - **Web Service Base URI -** Type the Uniform Resource Identifier (URI) for your Oracle Identity Analytics installation as follows:

     `http://`*server-name*`:`*port-number*`/rbacx`

     where *server-name* is the IP address or alias of the server on which Oracle Identity Analytics is running, and *port-number* is the port number of the application server that is listening to Oracle Identity Analytics calls.

- **User -** Type the user name that Oracle Waveset will use to connect to Oracle Identity Analytics. You should have created a special Oracle Identity Analytics user account for this purpose in step 2. Do not use the rbacxadmin account.
- **Password -** Type the password that Oracle Waveset will use to connect to Oracle Identity Analytics.
- **Oracle Identity Analytics Version -** Type the version number of Oracle Identity Analytics that Oracle Waveset is connecting to.
- **Is SRM Configured -** Type `true` to enable Oracle Waveset to use Oracle Identity Analytics Web Services.
- **Test Configuration -** Click to test the connection to Oracle Identity Analytics Web Services.

Note - Upon completing the wizard, additional form fields are unlocked. These fields include the following:

- **Process Check Policy Results Rule -** Value should be *Sun Role Manager:Process Policy Result*
- **Check Policy Compliance Violation Form -** Value should be *Sun Role Manager Compliance Violation Form*
- **Check Policy Status Rule -** Value should be *Sun Role Manager:Risk Analysis Status*
- **Compliance Violation Owners Rule -** Value should be *Sun Role Manager:Compliance Violation Owners*

---

7. Click **Next**.

   The Create Oracle Identity Analytics (Sun Role Manager) Web Services Resource Wizard / Account Attributes page opens.

8. Verify that the account attribute mappings on this page are correct and click **Next**.

   The Create Oracle Identity Analytics (Sun Role Manager) Web Services Resource Wizard / Identity Template page opens.

9. Verify that the attribute value in the Identity Template box is correct and click Save.

3.3.1.6 Step 6: To Configure the User Deferred Task Scanner

The User Deferred Task Scanner in Oracle Waveset needs to be configured for a delay of one minute so that SoD processing will work properly. The scanner picks up SoD information after it has been retrieved from Oracle Identity Analytics using Oracle Identity Analytics (Sun Role Manager) web services.

1. Log in to Oracle Waveset.
2. Choose **Server Tasks > Manage Schedule**.
3. Click **User Deferred Task Scanner** to edit the task.

   The Edit Task Schedule page opens.

4. Change the value in the **Repeat Every** box to a value of `1 Minutes`.
5. Click Save.

3.3.1.7 Step 7: To Configure the User Form so That Oracle Identity Analytics can Authenticate Over SPML

Within Identity Manger, the User Form of the user that Oracle Identity Analytics authenticates as over SPML needs to be set to "Empty Form."

1. Log in to Oracle Waveset.
2. Choose the **Accounts** tab and verify that the **List Accounts** subtab is selected.
3. Click the user that you created in Section 3.3.1.3, "Step 3: To Create an Oracle Waveset User That Oracle Identity Analytics Will use to Connect."

   The Edit User page opens.
4. Click the **Security** tab.
5. From the User Form drop-down box, select **Empty Form**.
6. Click Save.

Oracle Identity Analytics and Oracle Waveset are now configured to work together. To configure closed loop remediation, see Section 3.6, "Understanding Closed Loop Compliance."

3.4 Populating Oracle Identity Analytics With User Information From Oracle Waveset

Refer to the use cases in this section if you have user entitlements in Oracle Waveset that you want to use to populate the Oracle Identity Analytics Identity Warehouse. Importing users and roles from Oracle Waveset into Oracle Identity Analytics should be a one-time event that takes place when first configuring the systems.

3.4.1 Use Case 1: Importing Global Users From Oracle Waveset Into Oracle Identity Analytics

Oracle Waveset saves information about users who are auto-provisioned. These users are imported into Oracle Identity Analytics as global users before their accounts are pulled in.

3.4.1.1 To Import Users From Oracle Waveset Into Oracle Identity Analytics

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Import/Export**.
4. To start a new import job, choose **Schedule Job > Import > Import Users**.
5. Under **Data Selection Source**, select the appropriate **Connection Name** and click **Next**.
6. Complete the form by entering the **Name** and **Description** of the Job.
7. Choose one of the following tasks:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
8. Click **Finish**.

The import users job runs on the scheduled date and time.

9. Verify that the users are imported into Oracle Identity Analytics from Oracle Waveset by accessing the Users View in Oracle Identity Analytics (choose **Identity Warehouse > User**).

3.4.2 Use Case 2: Importing Resource Metadata From Oracle Waveset Into Oracle Identity Analytics

A *resource type* in Oracle Waveset is a type of target system, whereas a *resource* is an instance of a resource type. For example, consider the case of four different Windows NT systems hosting four different sets of users. In this scenario, "Windows NT" is the resource type, whereas the four individual system names are resources of type "Windows NT."

In the Oracle Identity Analytics integration with Oracle Waveset, information on resource metadata can be imported from Oracle Waveset to Oracle Identity Analytics. This eliminates the need to manually recreate resource metadata in Oracle Identity Analytics.

3.4.2.1 To Import Resource Metadata From Oracle Waveset Into Oracle Identity Analytics

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Import/Export**.
4. To start a new import job, choose **Schedule Job > Import > Import Resource Metadata**.

   The next page will prompt you to choose the resource from the list of available resources for which metadata on attributes needs to be imported.
5. Select the specific resource type.
6. Under **Data Selection Source**, select the appropriate Connection Name and click **Next**.
7. Complete the form by entering the **Name** and **Description** of the Job.
8. Choose one of the following:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
9. Click **Finish** to generate the Import Job.

   The import resource metadata job runs on the scheduled date and time.
10. Verify that the resource metadata was properly imported into Oracle Identity Analytics by accessing the Oracle Identity Analytics Resources Types tab (choose **Configuration > Resources Types**).

Note: Seven resource types in Oracle Waveset are treated differently by Oracle Identity Analytics. They are the following:

- Simulated
- Scripted JDBC
- Database Table
- External
- Scripted Gateway
- Scripted Host
- Shell Script

Each resource within the above resource type is created as a resource_type within Oracle Identity Analytics. The naming convention is "ResourceName__ResourceTypeName". This is because each resource is likely to have its own resource type metadata rather than a common metadata format.

3.4.3 Use Case 3: Importing Resources From Oracle Waveset Into Oracle Identity Analytics

With out-of-the-box integration capabilities, Oracle Identity Analytics can import resources from Oracle Waveset to Oracle Identity Analytics. This eliminates the need to manually create the resources in Oracle Identity Analytics.

3.4.3.1 To Import Resources From Oracle Waveset Into Oracle Identity Analytics

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Import/Export**.
4. To start a new import job, choose **Schedule Job > Import > Import Resources**.
5. Under **Data Selection Source**, select the appropriate Connection Name and click **Next**.
6. Complete the form by typing a name and description for the job.
7. Choose one of the following tasks:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
8. Click **Finish** to generate the import job. The import resources job runs on the scheduled date and time.
9. Verify that the resources are imported into Oracle Identity Analytics from Oracle Waveset by accessing the Oracle Identity Analytics Resources tab (choose **Identity Warehouse > Resources**).

3.4.4 Use Case 4: Importing User Accounts From Oracle Waveset Into Oracle Identity Analytics

After global users are imported, you can import accounts into Oracle Identity Analytics for different resource types. Before importing user accounts, make sure that the resource types and attributes are correctly configured in Oracle Identity Analytics. For more information, see "Resource Types Configuration" in the *Administrator's Guide for Oracle Identity Analytics*, "Oracle Identity Analytics Configuration" chapter.

3.4.4.1 To Import Accounts From Oracle Waveset Into Oracle Identity Analytics

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Import/Export**.
4. To start a new import job, choose **Schedule Job > Import > Import Accounts**, and then click **Next**.
5. From the list of available resources for which user accounts can be imported, select the resource and the specific resource type.
6. Under **Data Selection Source**, select the appropriate Connection Name and click **Next**.
7. Complete the form by entering the **Name** and **Description** of the Job.
8. Choose one of the following:
   - To run the job immediately, select the **Run the Job Now** option.
   - To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.
9. Click **Finish** to create the Import Job.

   The job runs on the scheduled date and time.
10. Verify that the accounts imported into Oracle Identity Analytics match the corresponding resource type accounts in Oracle Waveset.

3.4.5 Use Case 5: Importing Roles From Oracle Waveset Into Oracle Identity Analytics

Note - This should be done only as a one time effort for initial Roles population. It is recommended that SRM kept as the Authoritative Source for roles and the toles would be overwritten if they are imported from IDM on an ongoing basis.

3.4.5.1 To Import Role From Oracle Waveset Into Oracle Identity Analytics

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Import/Export**.
4. To start a new import job, choose **Schedule Job > Import > Import Roles**.
5. Under **Data Selection Source**, select the appropriate Connection Name and click **Next**.
6. Complete the form by typing a name and description for the job.
7. Choose one of the following tasks:
   - To run the job immediately, select the **Run the Job Now** option.

- To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.

8. Click **Finish** to generate the import job.

   The import resources job runs on the scheduled date and time.

9. Verify that the roles are imported into Oracle Identity Analytics from Oracle Waveset by accessing the Oracle Identity Analytics Roles tab (choose **Identity Warehouse > Resources**).

3.5 Populating Oracle Waveset With Roles Information From Oracle Identity Analytics

See the use cases in this section if you have user accounts in Oracle Identity Analytics that you want to use to populate the Oracle Waveset repository.

Note - Exporting roles from Oracle Identity Analytics to Oracle Waveset should be a one-time event that takes place during configuration. To export roles to Oracle Waveset, be sure that the Role Consumer box is selected in the Sun (Oracle Waveset) Provisioning Server settings.

Oracle Identity Analytics can create roles based on either existing entitlements or business attributes (client requirements). Policy formation and role-policy association can be performed during role creation. In addition, the role-user association can also be established.

Oracle Waveset does not have the concept of policies. The roles in Oracle Identity Analytics are mapped to Business Roles in Oracle Waveset, whereas the policies in Oracle Identity Analytics are mapped to IT Roles in Oracle Waveset. As policies are directly assigned to resources in Oracle Identity Analytics, similarly, IT Roles are directly assigned to resources in Oracle Waveset. Thus, the one-to-many relationship between role and policies is carried forward from Oracle Identity Analytics to Oracle Waveset by way of the one-to-many relationship between Business Roles and IT Roles. This allows for more efficient grouping of entitlements and easier management of user access. Thus, along with roles, policies also need to be exported from Oracle Identity Analytics to Oracle Waveset.

3.5.1 Use Case 1: Exporting Roles From Oracle Identity Analytics to Oracle Waveset

Note - Roles in Oracle Identity Analytics correspond to Business Roles in Oracle Waveset.

3.5.1.1 To Export Roles to Oracle Waveset

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Import/Export**.
4. To start a new export job, choose **Schedule Job > Export> Export Roles**.
5. Under **Data Selection Source**, select the appropriate Connection Name and click **Next**.
6. Complete the form by entering the **Name** and **Description** of the Job.
7. Choose one of the following:
   - To run the job immediately, select the **Run the Job Now** option.

- To schedule the job for later, clear the **Run the Job Now** option and enter the details of the scheduled job.

8. Click **Finish** to create the Import Job.

   The job runs on the scheduled date and time.

9. Verify that the roles were properly exported to Oracle Waveset by opening Oracle Waveset and clicking the **Business Role** Roles tab.

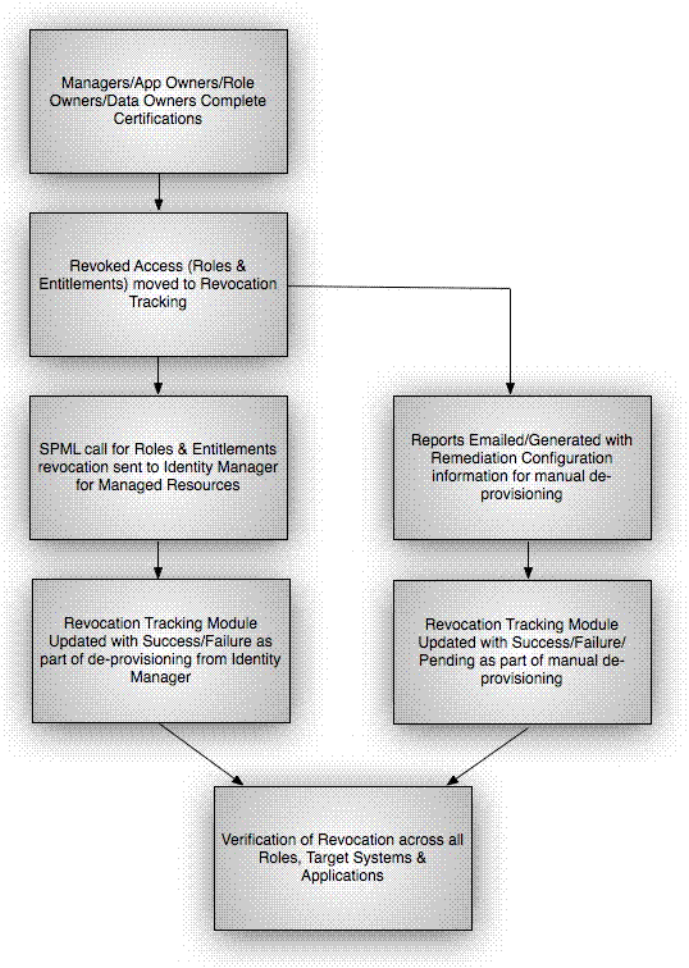
Note: Policies (roles content) are exported as part of roles export.

3.6 Understanding Closed Loop Compliance

With the integration of Oracle Identity Analytics and Oracle Waveset, it is possible to directly revoke roles and entitlements from Oracle Waveset if the results of the certification process require it. This integration eliminates the need for manual de-provisioning of access for managed resources. In addition, the manual process of revoking roles and entitlements by leveraging the information stored in the remediation configuration module is also retained. This takes into account nonmanaged applications.

The following closed loop remediation diagram illustrates this process.

Figure 3–4 OIA and Oracle Waveset Closed-Loop Remediation Diagram



3.6.1 To Configure Resources in Oracle Identity Analytics for Remediation

Every resource type in Oracle Identity Analytics can be separately configured for automatic or manual remediation.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse> Resources**.
3. Click the resource for which remediation action needs to be configured, and go to the **Remediation** tab.
4. Select the **Select Provisioning Mode** check box.
5. Choose the mode of provisioning desired for the particular resource.
   - **Auto -** Automatically send role/entitlement updates linked with this resource to Oracle Waveset.

     Select the appropriate connection name of the provisioning server and save the changes.
   - **Manual -** Use the manual steps for revocation of roles and entitlements using a text editor.

List the steps to be followed for non-managed system remediation and save the changes.

3.6.2 To Configure Certifications in Oracle Identity Analytics for Remediation

1. Log in to Oracle Identity Analytics.
2. Choose **Administration > Configuration**.
3. Click **Identity Certification**.
4. Expand the **Revoke and Remediation** section and, under the **Remediation** section, choose one of the following options:
   - **Display Remediation Instructions -** Select to display instructions about how to perform manual remediation of nonmanaged resources.
   - **Perform Closed Loop Remediation on -** Select to specify that the remediation be completed by either the Certification End Date or the Certification Completion Date.

3.7 Oracle Waveset Sample Workflows

Sample Oracle Waveset workflows are available to facilitate the integration of Oracle Waveset with Oracle Identity Analytics. Use the sample workflows included with Oracle Waveset 8.1.1-Patch 1 (located in the `sample/wfrolemanager.xml` file).

Note - Do not use the sample workflows included with Oracle Waveset 8.1.1 because they are no longer current.

The following Oracle Waveset sample workflows are available.

Table 3–1 Oracle Waveset Sample Workflows

Workflow Name	Description
Check SRM Integration	Invokes workflow services to determine if Oracle Identity Analytics (Sun Role Manager) integration has been configured. Returns a Boolean value in the `isSRMIntegrated` variable.
Merge SRM Role Assignments	If Oracle Identity Analytics is integrated and the `UserView` option `getRuleDrivenRoleManagerRoles` is set to `true`, this process will retrieve the list of roles to be automatically assigned by OIA configured rules. This list of roles will be merged with the Waveset-assigned roles into the `UserView`.
Create SRM User	If Oracle Identity Analytics is integrated, this process invokes the create OIA user action based on `UserView` attributes.
Update SRM User	If Oracle Identity Analytics is integrated, this process invokes the update OIA user action based on `UserView` attributes.
Rename SRM User	If Oracle Identity Analytics is integrated, this process invokes the rename OIA user action.
Delete SRM User	If Oracle Identity Analytics is integrated, this process invokes the delete OIA user action.
Disable SRM User	If Oracle Identity Analytics is integrated, this process invokes a disable OIA user action.
Enable SRM User	If Oracle Identity Analytics is integrated, this process invokes an enable OIA user action.

Table 3–1 (Cont.) Oracle Waveset Sample Workflows

Workflow Name	Description
Create SRM User Reconcile Response Workflow	If Oracle Identity Analytics is integrated, this per-account workflow invokes the creation of OIA users while processing unmatched accounts during reconciliation.

3.8 Oracle Identity Analytics Web Services

With an out-of-the-box integration, web services from both Oracle Waveset and Oracle Identity Analytics can be used as needed. For information about Oracle Identity Analytics web services, see the *API Guide for Oracle Identity Analytics*.

3.9 Troubleshooting

The information in this section briefly describes how to approach troubleshooting a Oracle Identity Analytics and Oracle Waveset integration.

3.9.1 System Logs

Application logs are generated and stored in the application deployment folder in `rbacx.log`. The log captures various details such as import/export information, ETL processing, and any exceptions that can arise while running the application. There are different levels of logging in the `rbacx.log` file, and these can be adjusted and modified as needed. The properties file that is used to alter the logging level is found under the *$RBACX_HOME*`/WEB-INF` folder, and the file name is `log4j.properties`.

There are three levels of logging that are commonly used by the system integrators: `WARN`, `INFO`, and `DEBUG`.

To change logging levels, open `log4j.properties` in a text editor and modify the line under the `#Role Manager IAM logging` section as follows:

```
log4j.logger.com.vaau.Role Manager.iam=DEBUG
```

Other parameters to be aware of are Security logging and IAM logging. These logs report Security and entitlement data exceptions.

For more information about logging, see the *Administrator's Guide for Oracle Identity Analytics*.

4

Configuring Oracle Identity Analytics for Web Access Control

This chapter describes how to authenticate with Oracle Identity Analytics using Web Access Components. It contains the following sections:

- Section 4.1, "Overview"
- Section 4.2, "Configuring Oracle Identity Analytics For Web Access Control"
- Section 4.3, "To Access Oracle Identity Analytics When Using Web Access Control"

4.1 Overview

Oracle Identity Analytics can be integrated with Web Access Control solutions such as Sun Access Manager, CA's eTrust SiteMinder, Novell's ICHAIN, and so on. This enables Oracle Identity Analytics to follow enterprise standards for web application security.

4.2 Configuring Oracle Identity Analytics For Web Access Control

The following two configuration changes need to be made in Oracle Identity Analytics:

1. Setting up the correct HTTP header variable name in `security-context.xml`
2. Setting up the logout URL

4.2.1 To Set Up the http Reader

Web Access Control Solutions send user information as part of the `http` header variable. This header variable, which is the user name, holds a unique identity for the user being authenticated. This user name should be the same as the Oracle Identity Analytics user.

As shown in the following snippet from the `security-context.xml` configuration file (under the `WEB-INF` folder in Oracle Identity Analytics), Oracle Identity Analytics is configured to use the value of the **`sm-user`** `http` header variable to authorize a user.

Change the property of *"preAuthEnabled"* to *"true"* and also change "**sm-user**" for "**preAuthUsernameHeaderKey**" and "**preAuthPasswordHeaderKey**" to the header variable sent by the Web Access Control Solution.

```
<bean id="preAuthAwareAuthenticationProcessingFilter"
```

```
class="com.vaau.commons.springframework.security.filter.PreAuthAwareAuthentication
ProcessingFilter">
        <property name="authenticationManager">
            <ref bean="authenticationManager"/>
        </property>
        <property name="authenticationFailureUrl"
value="/welcome.action?login_error=true"/>
        <property name="defaultTargetUrl"
value="/secure/checkExpiredCredentials.action"/>
        <property name="filterProcessesUrl" value="/j_acegi_security_check"/>
        <property name="formUsernameParameterKey" value="j_username"/>
        <property name="formPasswordParameterKey" value="j_password"/>
        <property name="preAuthEnabled" value="true"/>
        <property name="preAuthUsernameHeaderKey" value="sm-user"/>
        <property name="preAuthPasswordHeaderKey" value="sm-user"/>
        <!--SM_USER -->
        <property name="exceptionMappings">
            <props>
                <prop
key="org.springframework.security.BadCredentialsException">/welcome.action?login_e
rror=true</prop>
                <prop
key="org.springframework.security.CredentialsExpiredException">/passwordExpired.ac
tion</prop>
            </props>
        </property>
    </bean>
```

4.2.2 To Set Up the Logout URL

For a user to completely log out from the session, the Oracle Identity Analytics default logout URL needs to be modified with the logout URL for the Web Access Control Solution.

To configure the logout URL in Oracle Identity Analytics, change the following entry in the `header.jspf` file under the `WEB-INF/jspf` folder.

Current information in line 111-122 in the `header.jspf` file:

```
<tr>
   <td height="22">
       <div align="center" style="font-size:10px;">
              <a href="<%=ctx%>/secure/home/home.action" class="hoverUnderline"
        style="color:#000000">Home</a>
              <a href="<%=ctx%>/logout.action" class="hoverUnderline"
        style="color:#000000">Logout</a>
              <a href="<%=ctx%>/docs/userguide/index.html" target="_blank"
 class="hoverUnderline" style="color:#000000">Help</a>
      </div>
   </td>
</tr>
```

Line 111-122 in the `header.jspf` file after the modification:

```
<tr>
   <td height="22">
       <div align="center" style="font-size:10px;">
<a href="<%=ctx%>/secure/home/home.action" class="hoverUnderline"
                  style="color:#000000">Home</a> |
              <a href="www.vaau.com/logout.jsp" class="hoverUnderline"
```

```
                    style="color:#000000">Logout</a> |
                <a href="<%=ctx%>/docs/userguide/index.html" target="_blank"
class="hoverUnderline" style="color:#000000">Help</a>
        </div>
    </td>
</tr>
```

4.3 To Access Oracle Identity Analytics When Using Web Access Control

End-users should use the following URL to access Oracle Identity Analytics:

`http://`*OiaHost*`:`*Port*`/rbacx/j_acegi_security_check`

> **Note:** If the SSO solution allows for setting up a specific redirect URL for each application, then the SSO solution should be configured to redirect to the URL provided above.

Because this URL is protected by the SSO solution, the end-user is redirected to the SSO login screen, and, once successfully authenticated, re-directed to the URL provided. At this point, Oracle Identity Analytics can verify the HTTP header and allow the end-user to access the application.

5

Customizing the Oracle Identity Analytics User Interface

This chapter describes how to customize the Oracle Identity Analytics user interface (UI). It contains the following sections:

- Section 5.1, "Overview"
- Section 5.2, "Before You Begin"
- Section 5.3, "Configuring Logos"
- Section 5.4, "Configuring Labels"
- Section 5.5, "Configuring Error Messages"
- Section 5.6, "Configuring the Maximum Number of Identity Certification Records That Should Display in the UI"
- Section 5.7, "Enabling Hidden Pages in the UI"

5.1 Overview

Oracle Identity Analytics features a rich AJAX Web 2.0 user interface for an enhanced, user-friendly experience. Menu items and logos can be customized so that your organization can adhere to its internal style guidelines.

5.2 Before You Begin

To customize the user interface, you need the following access privileges:

- Access to the Oracle Identity Analytics application server with rights to modify and add files to the Oracle Identity Analytics deployed `war` folder
- Administrative credentials to log in to the Oracle Identity Analytics application

5.3 Configuring Logos

The Oracle Identity Analytics home screen displays the default logo.

If Oracle Identity Analytics is hosted on the Apache Tomcat application server, the directory where the `.war` file is expanded is usually set to the following location:

On UNIX `/usr/local/Vaau/rbacx-4.0/tomcat55/webapps/rbacx/`
On Windows `C:\Program Files\Vaau\RBACx2008\tomcat55\webapps\rbacx`

This path is referred to as *$RBACX_WAR* in this chapter.

Note: If you are using an application server other than Tomcat, contact a system administrator to determine the location of the deployed Oracle Identity Analytics WAR file.

5.3.1 To Configure a Custom Logo

1. Open the *$RBACX_WAR*/images directory and replace the logo.gif file with your company logo. Ensure that the company logo follows the same naming convention, which is logo.gif.
2. Open Oracle Identity Analytics to view the new logo.

   The new logo is displayed throughout the application.
3. If the new logo is not displayed immediately, restart the application server.

5.4 Configuring Labels

All labels in Oracle Identity Analytics can be modified or renamed as desired.

To make changes to labels, it is important to understand the structure of two files: rbacxmessages.properties and rbacxaudit-messages.properties. These two files contain the dynamic links to configure labels for the Oracle Identity Analytics user interface.

These files are located in *$RBACX_WAR*/WEB-INF/classes.

- The rbacxmessages.properties file contains labels that are separated by modules such as Identity Warehouse, Role Management, Identity Certification, and so on.
- The rbacxaudit-messages.properties file allows modifications to labels only within the Identity Audit module.

The following procedures describe how to modify the labels of various modules and menu items.

5.4.1 To Modify Menu Labels

1. Open the rbacxmessages.properties file located in *$RBACX_WAR*/WEB-INF/classes.
2. Scroll down to the # Menu section of the file.
3. As needed, modify the existing menu definitions, which are located to the right of the '=' sign, and save the file.
4. Restart the Oracle Identity Analytics application in a new browser window to view your changes.

An excerpt from the rbacxmessages.properties file follows:

```
# Menus
menu.welcome=<span>Welcome</span>
menu.register=Register
menu.info=My info
menu.administration=<span Title='Administration'>Administration
  <img src="/rbacx/images/arrow.gif"/></span>
menu.monitoring=Monitoring
menu.logout=Log out
menu.tools=Tools
menu.reports=Reports
```

```
menu.dashboard=<span Title='My Reports'> My Reports</span>
menu.security=Security
menu.help=Help
menu.certifications=<span Title='Identity Certification'>Identity
  Certification</span>
menu.provisioning=Access Control
menu.audit=<span Title='Identity Audit'>Identity Audit</span> menu.home=Home
menu.configuration=Configuration
menu.settings=<span Title='My Settings'>My Settings</span>
menu.requests=<span Title='My Requests'>My Requests</span>
menu.system=System
menu.identityWarehouse=<span Title='Identity Warehouse'>Identity Warehouse</span>
menu.users= Users
menu.roles= Roles
menu.businessUnit=Business Unit
menu.reporting=<span Title='Reports'>Reports</span>
menu.roleManagement=<span Title='Role Management'>Role Management</span>
menu.roleEngineering=<span Title='Role Engineering'>Role Engineering</span>
menu.roleEntitlementDiscovery=Role Entitlement Discovery
menu.roleConsolidation=Role Consolidation
menu.myRequest=<span Title='My Request'>My Request</span>
menu.rme=<span Title='Role Engineering'>Role Engineering</span>
```

5.4.2 To Modify User Labels

1. Open the `rbacxmessages.properties` file located in *$RBACX_WAR*`/WEB-INF/classes`.
2. Scroll down to the `# Identity Warehouse` section of the file.
3. As needed, modify any of the existing user labels, which are located to the right of the "=" sign, and save the file.
4. Restart the Oracle Identity Analytics application in a new browser window to view your changes.

An excerpt from the `rbacxmessages.properties` file follows:

```
##################Identity Warehouse ############################

user.username= User Name
user.employeeid= Employee Id
user.employeetype= Employee Type
user.firstname= First Name
user.middlename= Middle Name
user.lastname= Last Name
user.allNameRequired=All name's required. user.fullname= Full Name
user.title= Title
user.officename= Office Name
user.street= Street
user.city= City
user.state= State/Province
user.zip= Zip/Postal Code
user.country= Country/Region
user.phone= Phone
user.extension= Extension
user.mobile= Mobile
user.fax= Fax
user.filter.pagesize=Page Size user.pager= Pager
user.pemail= Primary Email
user.semail= Secondary Email
user.comments= Comments
```

```
user.suspension= Suspension
user.gustatus= Global User Status user.startdate= Start Date
user.enddate= End Date
user.servicedesk= Service Desk user.status= Status
user.servicedeskticket= Service Desk Ticket
user.serverDeskTicket=Server Desk Ticket
user.customProperty1=Custom Property 1
user.customProperty2=Custom Property 2
user.customProperty3=Custom Property 3
user.customProperty4=Custom Property 4
user.customProperty5=Custom Property 5
user.customProperty6=Custom Property 6
user.customProperty7=Custom Property 7
user.customProperty8=Custom Property 8
user.customProperty9=Custom Property 9
user.customProperty10=Custom Property 10
user.customProperty11=Custom Property 11
user.customProperty12=Custom Property 12
user.customProperty13=Custom Property 13
user.customProperty14=Custom Property 14
user.customProperty15=Custom Property 15
user.customProperty16=Custom Property 16
user.customProperty17=Custom Property 17
user.customProperty18=Custom Property 18
user.customProperty19=Custom Property 19
user.customProperty20=Custom Property 20
user.addBusinessUnit=Add Business Unit
user.address=Address
```

5.5 Configuring Error Messages

Configuring error messages in Oracle Identity Analytics is similar to configuring labels.

The `rbacxmessages.properties` and `rbacxaudit-messages.properties` files contain the dynamic links to configure error messages for the Oracle Identity Analytics user interface.

- The `rbacxmessages.properties` file contains error messages that are separated by modules (such as Identity Warehouse, Role Management, Identity Certification, and so on).
- The `rbacxaudit-messages.properties` file allows modifications to error messages only within the Oracle Identity Analytics Identity Audit Module.

These files are located at *$RBACX_WAR*`/WEB-INF/classes`.

The following procedures describe how to modify the error messages generated from various Oracle Identity Analytics modules.

5.5.1 To Modify My Requests Error Messages

1. Open the `rbacxmessages.properties` file located in *$RBACX_WAR*`/WEB-INF/classes`.
2. Scroll down to the `#My Requests` section of the file.
3. As needed, modify the existing error message labels, which are located to the right side of the '=' sign, and save the file.

4. Restart the Oracle Identity Analytics application in a new browser window to view your changes.

An excerpt from the `rbacxmessages.properties` file follows:

```
################################################
#       My Requests
################################################
request.error.selectRequest=Please choose a request first!
request.error.approveFailed=Unable to approve the request!
request.error.rejectFailed=Unable to reject the request!
```

5.5.2 To Modify Identity Certification Error Messages

1. Open the `rbacxmessages.properties` file located in *$RBACX_WAR*`/WEB-INF/classes`.
2. Scroll to the `#Identity Certification` section of the file.
3. As needed, modify the existing error message labels, which are located to the right of the '=' sign, and save the file.
4. Restart the Oracle Identity Analytics application in a new browser window to view your changes.

An excerpt from the `rbacxmessages.properties` file follows:

```
################################################
#       Identity Certification
################################################

idc.error.errorUsersRequired = No Users found in this certification...
idc.error.errorRolesRequired = No Roles found in this certification...
idc.error.updateCommentsFailed = Unable to update the comments!
idc.error.noEndPointsFound = No EndPoints found in this certification!
idc.error.selectCertification = Please select at least one certification
first!
idc.error.selectReport = Please select a report first!
idc.error.reportError = This report has no pages!
idc.error.selectDate = Please select date values!
idc.error.selectMonths = Please select months values!
idc.error.selectYear = Please select year values!
idc.error.selectSeconds = Please select seconds values!
idc.error.selectMinutes = Please select minute values!
idc.error.selectHours = Please select hour values!
idc.error.errorAlphanumericCharactersRequired = Certification name must contain
alphanumeric characters!
idc.error.deleteFailed = Unable to delete certification job!
idc.error.unableToAdd = Unalbe to add certification job!
idc.error.checkHighlightedFields = Please check the highlighted fields!
idc.error.selectBusinessUnit = Please select a business unit!
```

5.6 Configuring the Maximum Number of Identity Certification Records That Should Display in the UI

You can configure the maximum number of records that users see onscreen when viewing certifications on the My Certifications screen by defining batch sizes. Batch sizes for data owner certifications, user entitlement certifications, and resource entitlement certifications can be configured, but role entitlement certifications cannot.

If UI batch sizes are set too high, long load times can result. If set too low, end-users will need to request pages more often, which can also result in delays.

Note: To improve identity certification performance, server-side batching can be configured. See "Configuring Identity Certification Settings on the Server" in the "Tuning Server Configuration Properties" chapter of the *Administrator's Guide for Oracle Identity Analytics* for information.

5.6.1 To Modify Identity Certification Batch Sizes in the UI

1. Open the `idc.properties` file located in *$RBACX_WAR*`/conf` to configure batch sizes for user entitlement certifications and resource entitlement certifications. (To configure batch sizes for data owner certifications, open the `idc-context.xml` file located in *$RBACX_WAR*`/conf`.)
2. Scroll to the section that says `IDC UI` batch sizes.
3. Find the correct configuration key, then change the value. See the following examples:
   - For user entitlement certifications, find the `com.vaau.rbacx.idc.ui.usersBatchSize` key and change the numeric value up or down.
   - For resource entitlement certifications, find the `com.vaau.rbacx.idc.ui.resourcesBatchSize` key and change the numeric value up or down.
4. Save the file.
5. Restart the Oracle Identity Analytics application in a new browser window to view your changes.

5.7 Enabling Hidden Pages in the UI

This section includes steps for enabling hidden pages in the user interface.

5.7.1 To Enable the Workflow Tab on the Identity Warehouse Pages

The Workflow page displays three approver fields that are populated with data if OIA has been integrated with the CA Identity Manager provisioning server.

1. Open `userDetailDialog.js` for editing.
2. Change the variable `SHOW_WORKFLOW_INFO` from `false` to `true` and save the file.
3. Clear your browser's cache.

   The Workflow tab is now enabled.

Note: For more information about the Workflows page, see the *User's Guide for Oracle Identity Analytics*, "Identity Warehouse" chapter, "Tabs on the Identity Warehouse - Users - User Detail Page" section.

5.7.2 To Enable the Exclusion Roles Tab on the Identity Warehouse Pages

The Exclusion Roles page lists roles that are in conflict with one another from a segregation of duties standpoint. This page is hidden in the user interface. To enable the page, follow these steps.

1. In a text editor, open `header.jspf` located in *$RBACX_WAR*`/WEB-INF/jspf`.
2. Locate the following lines:

```
// hide the Exclusion Roles tab by default.
// set to true to enable this feature
request.setAttribute("exclusionRolesEnabled", false);
```

3. Change the `false` parameter to `true`.

   The modified line should look like this:

```
request.setAttribute("exclusionRolesEnabled", true);
```

4. Save your changes.

   You do not need to restart Oracle Identity Analytics for the change to take effect.

Note: For more information about the Exclusion Roles page, see the *User's Guide for Oracle Identity Analytics*, "Identity Warehouse" chapter, "Setting the Segregation of Duties at the Role and Policy Levels" section.

A

Preparing to Integrate Oracle Identity Manager and Oracle Identity Analytics on WebSphere

This appendix includes instructions that describe how to configure WebSphere so that Oracle Identity Manager (OIM) and Oracle Identity Analytics (OIA) can be installed on separate servers.

A.1 To Integrate OIM and OIA on WebSphere

Before You Begin -

- The following steps describe how to install Oracle Identity Manager (OIM) 9.1.0.2 BP17 and Oracle Identity Analytics (OIA) 11.1.1.5.0 on WebSphere.
- When installing OIM and OIA on different machines, OIM needs to be installed using the cluster install instructions (even if you need only one server of OIM), and the cell needs to be spread across the other machine as described in these steps.

1. Install the WebSphere Network Deployment binaries on the machine where you will run OIM and on the machine where you will run OIA.
2. Using the Upgrade Utility, upgrade the WebSphere Network Deployment Server software to the required version.
3. Install OIM 9.1.0.2 as documented in the *Installation Guide for Oracle Identity Manager*, "Deploying Oracle Identity Manager in a Clustered WebSphere Configuration" chapter.

   Note: Install OIM on the WebSphere cell before installing OIA or configuring the OIA server.

4. Zip up the entire contents of the `OIM_HOME` directory and copy it to the OIA machine and extract in the same location.
5. Create a new managed server profile on the OIA machine:
   - **UNIX:**

```
WAS_NDS_HOME/AppServer/bin/manageprofiles.sh -create
-templatePath WAS_NDS_HOME/AppServer/profileTemplates/managed
-profileName oia-managed01 -profilePath WAS_NDS_HOME/profiles/oia-managed01
-nodeName oia-managed01-node01 -hostname hostname
```

- **Windows:**

```
%WAS_NDS_HOME %\AppServer\bin\manageprofiles.bat -create
-templatePath %WAS_NDS_HOME %\AppServer\profileTemplates\managed
-profileName oia-managed01 -profilePath %WAS_NDS_HOME
%\profiles\oia-managed01 -nodeName oia-managed01-node01 -hostname hostname
```

6. Integrate the OIA node to the OIM Cell by typing the following command on the OIA Machine:

   - **UNIX:**

```
cd OIM_HOME/xellerate/setup; ./xlAddNode.sh oia-managed01
oia-managed01-node01 192.168.21.9 8883 xelsysadm password1
```

   - **Windows:**

```
cd %OIM_HOME%\xellerate\setup
xlAddNode.bat oia-managed01 oia-managed01-node01 192.168.21.9 8883
xelsysadm password1
```

7. Login to the WebSphere Deployment Manager server and create a new server:
   a. Choose **Servers >Application Servers >New**.
   b. Type a name (for example, `oia-managed01-server`).

      Select your OIA managed node from the drop-down menu (for example, `oia-managed01-node01`) and click next.
   c. Choose the default server and click next.
   d. Verify that **Generate Unique Ports** is selected and click next.
   e. Click **Finish**.
   f. Click **Review**, check the synchronize nodes, and click **Save**.
8. Configure the default Java properties for the newly created server:
   a. Choose **Servers >Application Servers** and click the newly created server.
   b. Choose **Java and ProcessManagement >Process Definition**.
   c. Click **Java Virtual Machine**.
   d. Click **Custom Properties**.
   e. Click **New** and enter the following info:
      – **UNIX:**

        `XL.HomeDir` (For example: `/opt/oim9102/xellerate`)
      – **Windows:**

        `OIM_HOME` (For example: `c:\oim9102\xellerate`)
   f. Click **New** and enter the following info:
      – `java.awt.headless`
      – `true`
   g. Click **Apply** and **Save**.

Note: The JVM properties needs to be set for all the servers created in the WebSphere cell for all the OIA servers.

9. Configure the OIA node(s) by setting the "CSIv2 outbound authentication" as follows:
   a. Choose **Servers >Application Servers > *yourOiaApplicationServerName* > Server Security**.
   b. Click **CSIv2 outbound authentication**.

      A new page opens.
   c. Select the **Identity assertion** option and verify that the sub-option **User server trusted identity** is selected.
   d. Click **Apply** and **Save**.
10. Configure the OIM node(s) by setting the "CSIv2 outbound authentication" as follows:
   a. Choose **Servers >Application Servers > XL_SERVER1_ON_NODE1 > Server Security**.
   b. Click **CSIv2 outbound authentication**.

      A new page opens.
   c. Select the **Identity assertion** option and type the OIA node name(s) in the **Trusted identities** box. (For example, *oia-managed01-server*.)

      Multiple nodes can be entered using a "|" as a separator.
   d. Click **Apply** and **Save**.
11. Restart both the OIA and the OIM servers.
12. Create the `rbacx.war` file by following the instructions in the *Installation and Upgrade Guide for Oracle Identity Analytics*, "Configuring Your Oracle Identity Analytics Installation Prior to Deployment" chapter.
13. Deploy the `rbacx.war` file by following the instructions in the *Installation and Upgrade Guide for Oracle Identity Analytics*, "Deploying Oracle Identity Analytics" chapter.

Note: When deploying, make sure to assign only the OIA managed server to the `rbacx` application.

14. Complete the steps in Chapter 1, "Integrating With Oracle Identity Manager, Preferred Method."