Oracle® Fusion Middleware

Administrator's Guide for Oracle Identity Analytics

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

E23369-03

March 2014

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

E23369-03

Primary Author: Deena Purushothaman

Contributing Authors: Kevin Kessler, Sridhar Machani

Contents

Part I Business Administrator's Guide

1 Oracle Identity Analytics Identity Warehouse

2 Oracle Identity Analytics Importing

3 Oracle Identity Analytics ETL Process

4 Oracle Identity Analytics Data Correlation

5 Role Engineering and Management

6 Oracle Identity Analytics Workflows

7 Oracle Identity Analytics Identity Certifications

8 Oracle Identity Analytics Identity Audit

9 Oracle Identity Analytics Reports

10 Oracle Identity Analytics Scheduling

11 Oracle Identity Analytics Configuration and Settings

13 Audit Event Log and Import-Export Log

Part II System Administrator's Guide

14 Securing Oracle Identity Analytics

15 Understanding and Configuring the System Log

16 Using System Logs

17 Oracle Identity Analytics Troubleshooting

18 Tuning Server Configuration Properties

Preface

This guide consists of two parts: Part I is the Business Administrator's Guide, which provides detailed information about configuring and administering the role management and compliance functionality available in Oracle® Identity Analytics 11gR1 software. Part II is the System Administrator's Guide, which describes how to configure and administer the Oracle® Identity Analytics 11gR1 PS1 software at a systems level.

Audience

Part I, the Business Administrator's Guide, is written for administrators, compliance officers, and IT specialists.

Part II, the System Administrator's Guide, is written for system administrators, deployment engineers, and service providers who are responsible for administering the Oracle Identity Analytics 11gR1 software at a systems level.

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 User's Guide*
- *Oracle Identity Analytics System Integrator'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.

Business Administrator's Guide

Part I of the Administrator's Guide is the Business Administrator's Guide, which provides detailed information about configuring and administering the role management and compliance functionality available in Oracle® Identity Analytics software.

1

Oracle Identity Analytics Identity Warehouse

This chapter contains the following sections:

1.1 Overview

This chapter documents Identity Warehouse functionality that is available to business administrators, but not to general business users. Identity Warehouse information for general business users is documented in the *User's Guide for Oracle Identity Analytics* "Identity Warehouse" chapter.

See the *User's Guide for Oracle Identity Analytics* to learn more about the following Identity Warehouse topics:

- What is the Identity Warehouse?
- Understanding the Identity Warehouse user interface
- Working with users
- Searching for a user
- Viewing user details
- Working with Business Structures
- Associating users with roles and business structures
- Setting user status
- Working with resources
- Working with policies
- Working with roles
- Setting the segregation of duties at the role and policy levels

1.2 Working With Resources

Resources are the applications and enterprise information assets that users need to do their jobs. In Oracle Identity Analytics, a resource is an instance of a *resource type*, which is a grouping of like resources. A resource type defines meta-data common to all resources of that type. For example, a resource type of "Oracle DBMS" might define entitlements (that is, attribute-values of Oracle database accounts) that are common to all database instances. Each resource of that type represents a specific database instance to which a user might have access

Common resource types include platforms (Windows 2000, UNIX®, Mainframe) or business applications (such as, billing and accounts payable applications). Each resource has an owner who handles the various operations on the resource, such as reviewing user entitlements. The user entitlements are collected from different resources and stored in a central repository.

Note: For information about configuring resource types, including creating or modifying resource types, see Section 11.1.3, "Resource Types Configuration."

1.2.1 To Create or Modify Resources

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Resources**.
3. To add a new resource, click the **New Resource** button.

   The New Resource dialog box opens.
4. Complete the form:
   - **Resource Type** - Select the resource type that the new resource/directory should belong to.
   - **Resource Name** - Type a name for the resource.
   - **Host Name** - Type the host name.
   - **Host IP** - Type the host's IP address.
   - **Description** - Type a short description for the resource.
   - **Comments** - Additional comments can be entered here.
5. Click Save.

1.2.2 To Delete Resources

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Resources**.

   All the resources and resource types are listed.
3. Go to the resource you want to delete, then click **Delete** in the **Actions** column.

   A window opens asking you to confirm the delete action.

1.3 Working With Applications

An application is a collection of multiple resource types and resources. You can select the resource type and resources to be included in the application and enter metadata around applications.

1.3.1 To Create Applications

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Applications**.
3. Click the **New Application** button.

   The Create Application page opens.
4. Complete the form.
   - **Name** - Enter the name of the application.
   - **Version** - Enter version details.
   - **Description** - Enter a description for the application.
   - **Environment** - Enter environment details.
   - **Comments** - Enter comments, if applicable.
   - **Status** - Set the status as active or inactive. You can schedule a user assignment for the application only if the application is in the active state.
5. Click **Next**.

   The Add Owners page opens.
6. Click the **Add Owner** button.

   The Search dialog box opens.
7. Search for the user to add as the application owner.

   For help using Search, see the "Searching for a User" topic in the "Identity Warehouse" chapter of the *User's Guide for Oracle Identity Analytics*.
8. Click **Next**.

   The **Add Conditions** page opens.
9. Click the **Add Conditions** button.

   The **Add Conditions** window opens.
10. From the table select the resource types, resources, attribute names, and attribute values. You do not have to select from all four columns

    Click **OK**.
11. Click **Next**.

    The summary page opens.
12. Click **Create**.

1.3.2 To Schedule a Job for Assigning Users to Applications

In Oracle Identity Analytics, you cannot use the user interface to manually add users to (or remove users from) applications. Instead, after you create an application, you need to schedule a job using configuration files. The job scans all users and assigns the users who have an account in the selected resource type to the application.

1. To enable a scheduling job, edit the `scheduling-context.xml` file located in the *$RBACX_HOME*`/WEB-INF` folder.
2. To schedule a job, edit the `jobs.xml` file located in the *$RBACX_HOME*`/WEB-INF` folder.

For detailed instructions, see Section 10.2, "Scheduling a Job by Editing the Configuration Files."

Remember to restart the application server after editing the configuration files.

Note - If you select two or more attribute values from the same resource, users who are associated with any one of the selected attribute values are assigned to the application. However, if you select one or more attribute values from multiple resources, users who have an account in all the multiple resources will be assigned to the application.

1.4 Understanding How Risk Summaries are Calculated

You can directly assign high, medium, and low risk levels to roles, resources, and resource-attribute values (entitlements), as well as to certain predefined risk factors. A risk-aggregation job calculates Risk Summaries for the remaining higher-order data objects that are needed to support the OIA Identity Certification feature. These objects include every User, User-Role assignment, Account, and Account-Attribute value in the Identity Warehouse. During identity certification, OIA certifiers use Risk Summaries to separate high-risk certification items from medium-risk and low-risk items.

This section describes how the system processes risk levels to arrive at Risk Summaries. It also describes the risk-aggregation job, which you can run manually or on a scheduled basis.

Note: In OIA, Roles, Resources, and Entitlements (Resource-Attribute Values) are *metadata* objects, whereas Users, Accounts, and Account-Attribute Values are *instance-data* objects.

Think of metadata objects as "structural" objects that represent and describe your information systems within OIA, whereas instance-data objects are the individual instances of application data that populate the systems described. For example, consider a customer service application (a Resource) that has a predefined role that enables users to create trouble tickets (an entitlement). In this example, a single Resource object represents the application and a single entitlement object represents a specific privilege within that application.

Now consider there might be thousands of user accounts on this resource, some subset of which has the entitlement-assignment that allows the user to create a trouble ticket. In the Identity Warehouse, each user account is represented by an Account object, and each instance of the entitlement assignment is represented by an Account-Attribute-Value object. This illustrates the one-to-many relationship that exists between metadata objects and instance data objects. A single resource (metadata object) can have multiple accounts (instance-data objects), and a single entitlement (metadata object) can have multiple assignment instances (instance-data objects). OIA calculates the risk levels for instance-data objects because it would not be feasible for a human to process risk levels for every User, Account, and Account-Attribute Value in the Identity Warehouse on a recurring basis.

1.4.1 Understanding Item Risk and Risk-Factor Mappings

Item Risk and the Risk-Factor Mappings are settings that are under your direct control. Item Risk is discussed first.

1.4.1.1 Understanding Item Risk

Item Risk refers to the risk levels that you and other administrators can assign to specific roles, resources, and entitlements in the Identity Warehouse. (There are other ways that Item Risk can be assigned to metadata objects, but direct assignment is the most common method.)

Note: In OIA, three bars signifies high risk, two bars signifies medium risk, one bar signifies low risk.

Assigning an Item-Risk level to a metadata object in the UI is straightforward. To do so, you open the object in the Identity Warehouse and select a *High*, *Medium*, or *Low* risk setting from the menu.

If you do not directly assign an Item-Risk level to a metadata object in the Identity Warehouse, the system assigns a default Item-Risk level for you. Roles, Resources, and Entitlements can each have a default value. You can configure a default Item-Risk level using the Risk Mapping page (from the menu, choose **Administration > Configuration > Risk Level**).

Generally speaking, you should reserve high Item-Risk levels for metadata objects that confer highly-restricted privileges to users. Note that setting a high Item-Risk level on an object will cause its parent object to also have a high Risk-Summary value. Similarly, setting a medium Item-Risk level on an object will cause its parent object to have at least a medium Risk-Summary value. In order for a higher-order object to have a low Risk-Summary value, all of the objects under it in the system hierarchy would have to have low risk settings.

Following are the other ways that Item Risk can be assigned to objects in OIA:

- An external system such as Oracle Identity Manager can set an object's risk level. When OIA imports a role or glossary entry from the external system, if that object has an assigned value for Item Risk, the value is also imported. (OIA does not import Item Risk values for any other type of imported object. Instead, the system assigns the object a default Item-Risk level as described earlier.)
- OIA can set Item-Risk values when customers upgrade from a previous version of the software. Prior to version 11gR1 PS1, OIA had an attribute named "High-Privileged." Upon upgrade, instances of the "High-Privileged" attribute are converted to a value of high Item Risk if the High-Privileged attribute is set. If it is not set, the Item Risk will default to a value of medium risk.

For steps that describe how to assign an Item-Risk level to a specific role, resource, or entitlement, see the following sections.

- To assign an Item-Risk level to a specific role, see "To Rename, Modify, or Decommission (Delete) a Role" in the "Identity Warehouse" chapter of the *User's Guide for Oracle Identity Analytics*.
- To assign an Item-Risk level to a specific resource or a specific entitlement, see "To Create a Policy" in the "Identity Warehouse" chapter of the *User's Guide for Oracle Identity Analytics*.

> **Note:** The policy Risk-Level attribute is a deprecated attribute that has no current use.

1.4.1.2 Understanding Risk-Level Mappings (Risk Factors)

Risk-Factor Mappings are settings that map risk levels to certain predefined conditions within OIA. For example, you might configure "items with open audit violations" as high risk, whereas "items that are closed as risk-accepted" you might configure as medium risk.

Generally speaking, you should reserve high Risk-Factor levels for conditions in which privileges are being extended to users that may be irregular or dangerous.

There are three Risk-Factor categories in OIA, and each category contains multiple settings. Risk-Factor categories are described in the following table.

Table 1–1 Risk Factors

Risk Factor	Description
Provisioning Scenarios / Assignment Scenarios	*Provisioning Scenarios* define the risk levels that should be associated with the method or mechanism that a system external to OIA used to assign a role, account, or account-attribute value to a user. (Oracle Identity Manager is one example of an external system.) For example, you might configure a risk level of *High* for objects that are provisioned directly by an administrator, and a risk level of *Low* for objects that are provisioned based on Policies that are tied to Roles. For a description of each of the Provisioning Scenarios risk-level mapping settings, see Section 11.1.2.1, "External Provisioning (Provisioning Scenarios)." *Assignment Scenarios* define the risk levels that should be associated with assignment actions applied from within OIA. For example, you might configure a risk level of *High* for role memberships that are assigned directly by an administrator, and a risk level of *Low* for objects that are assigned by role-membership rules. For a description of each of the Assignment Scenarios risk-level mapping settings, see Section 11.1.2.2, "System Defaults," "Assignment Scenarios."
Audit Violations (Open SoD Violation)	Defines the risk level associated with having a Segregation-Of-Duties (SoD) violation. For example, you might configure a risk level of *High* for an unresolved SoD violation, and a risk level of *Medium* for an SoD violation that was closed as risk-accepted. For a description of each of the Audit Violations risk-level mapping settings, see Section 11.1.2.2, "System Defaults," "Audit Violations."
Last Certification Action	Defines risk level based on the status of the last certification for the account, account-attribute value, or user-role assignment under consideration. For example, configure a risk level of *Low* for any item for which the previous certification decision was to approve, and configure a risk level of *Medium* for any item for which the previous certification decision was to *Certify Conditionally*. Finally, you might configure a value of *High* for any item for which the previous certification decision was *Abstain* or *Revoke*. For a description of each of the Last Certification Action risk-level mapping settings, see Section 11.1.2.2, "System Defaults," "Last Certification Action."

In the UI, you configure Risk-Factor mappings using the Risk Mapping page (from the menu, choose **Administration > Configuration > Risk Level**).

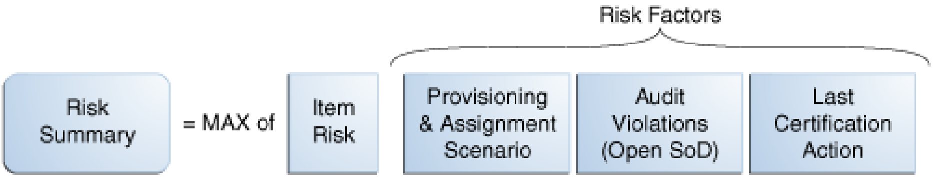
Note: Changing Risk-Level mappings on the Configuration page in the UI can cause major ripple effects that impact Risk Summaries throughout the Identity Warehouse. During your initial setup you should configure mappings on the Risk Level configuration page, and then avoid making additional unnecessary changes.

For more information, see Section 1.4.3, "Understanding How Changing Risk Configuration Values Impacts the System."

1.4.2 Understanding Risk Aggregation and Risk Summaries

The Risk-Aggregation job processes Item-Risk levels and Risk-Factor levels, and calculates Risk Summaries for each higher-order object that supports Identity Certification.

In the first phase of risk aggregation, the Risk-Aggregation job evaluates each individual object's Item-Risk level and its three Risk-Factor levels and assigns the highest of the four levels to the object's Risk Summary property. A Risk Summary value is calculated for each individual User object, User-Role Assignment object, Account object, and Account-Attribute-Value (AAV) object. The following diagram illustrates this process.

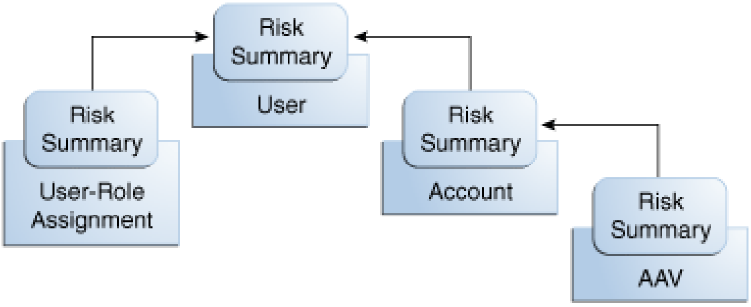

Risk Factors
Risk Summary
= MAX of
Item Risk
Provisioning & Assignment Scenario
Audit Violations (Open SoD)
Last Certification Action

Once Risk Summaries are calculated for every object in the Identity Warehouse, the next phase of aggregation begins, in which the Risk Summary of each individual object rolls up to the Risk Summary of the parent object that contains it.

Above the AAV level, each data object's Risk Summary value contributes to the Risk Summary of the parent-object that contains it. For example, Account objects are one hierarchy level up from AAV objects, and User objects are one hierarchy level up from there. So, the Risk Summary of every AAV object within an Account object contributes to the Risk Summary for that Account, and, similarly, the Risk Summary for every Account object within the User object contributes to the Risk Summary for that User.

User objects are also one level above User-Role Assignment objects, so the Risk Summary for every User-Role Assignment object contributes to the Risk Summary for that User.

The following diagram illustrates this process.



In the diagram, the Risk-Summary value of the Account-Attribute Value rolls up to the Account object. The Risk-Summary values of Accounts and the Risk-Summary values of User-Role Assignments roll up to the Risk Summary of any associated User.

1.4.3 Understanding How Changing Risk Configuration Values Impacts the System

There are three main actions or system events that can impact Risk Summary values in the Identity Warehouse. Depending on the action/system event, the impact can be minor, moderate, or major. Each action or event and its consequences is described in the following table.

Table 1–2 Actions or System Events That can Impact Risk Summary Values in the Identity Warehouse

Action or Event	Impact	Description
OIA Users and/or the system make changes to individual data objects	Minor	Applies to changes to individual data objects (such as Accounts, Account Attributes, and User-Role assignments). These values may change frequently. For example, the following types of changes are included in this category: ■ An Attribute Value is added to or removed from an Account. ■ An Account is added to or removed from a User. ■ A Role Assignment is added to or removed from a User. ■ A Risk Factor on an individual data object changes. The impact within the Identity Warehouse is relatively minor because the changes happen at the level of each individual data object.
An administrator or external system makes Item-Risk changes to Roles, Resources, and Resource-Attribute Values	Moderate	Applies to situations where you or another administrator change the risk-level of a Role, a Resource, or a Resource-Attribute Value. The ripple-effect of these changes can be large. Changing the risk level on a metadata object can change the Item-Risk level on every data-object associated with the metadata object. Changing the risk level on a data-object may affect its Risk Summary and, in turn, the Risk Summary of every other data-object that contains it. For example, changing the risk level on a Resource-Attribute Value will change the Item Risk on every Account-Attribute Value (AAV) that corresponds to it. Changing the Item Risk on an AAV may change its Risk Summary. Changing the Risk Summary of an AAV may affect the Risk Summary of the parent Account. Changing the Risk Summary of an Account may affect the Risk Summary of the User who owns the Account.
An administrator makes configuration changes to the Risk-Level Mappings	Major	Applies to situations where you or another administrator change the Risk-Level Mappings on the Configuration page in the UI. Changing the risk level associated with a specific value of a specific risk factor could affect the Risk Summary of any User-Role Assignment, Account, or Account-Attribute Value that has that risk-factor value. Changing the Risk Summary of any User-Role Assignment, Account, or Account-Attribute Value could in turn affect every User associated with an affected User-Role Assignment, Account, or Account-Attribute Value. For this reason, you should change Risk-Level Mappings only rarely.

1.4.4 Understanding the Risk-Aggregation Job

The `riskSummaryMaintenanceJob` calculates Risk Summaries in Oracle Identity Analytics. Each data object's Risk Summary score is accurate as of the last time the `riskSummaryMaintenanceJob` ran successfully.

1.4.4.1 To Enable the Risk-Aggregation Job

1. Open the `scheduling-context.xml` file for editing.
2. Locate the entry for `riskSummaryMaintenanceJob` within the `jobDetails` property of the `quartzSchedulerFactoryBean` bean definition.
3. Uncomment the reference to `riskSummaryMaintenanceJob`.
4. Uncomment the reference to the `riskSummaryMaintenanceJobTrigger` in the `triggers` property for the `quartzSchedulerFactoryBean`.
5. Restart the application server

> **Note:** If the `riskSummaryMaintenanceJob` takes a long time to complete, update statistics on your database indexes to improve performance. New OIA installations in particular may benefit from updating statistics on database indexes.
>
> For information about how to update statistics on database indexes, consult your database server documentation.

1.4.4.2 To Control How Often the Risk Aggregation Job Runs

1. Open the `jobs.xml` file for editing.
2. Locate the `riskSummaryMaintenanceJobTrigger` definition and modify the cron expression based on your needs.
3. For more information about the `jobs.xml` file and editing cron expressions, see Section 10.2, "Scheduling a Job by Editing the Configuration Files."

1.5 Working With Extended User Custom Properties

Custom properties and extended custom properties save custom user information in the Identity Warehouse. Out-of-the-box, Oracle Identity Analytics features twenty custom properties. If you need more than twenty custom properties, you can enable extended user custom properties and use them in a similar way.

> **Note:** The known limitations while using extended user custom properties are as follows:
>
> - There is no ability to search using extended properties.
> - Extended properties cannot be used in audit rules.
> - Extended properties cannot be used in role management rules.

In the user interface, custom properties are displayed by choosing **Identity Warehouse** > **Users** > *User Name*, and clicking the **Custom Properties** tab, whereas extended custom properties are displayed by clicking the **User Defined Properties** tab.

Custom properties and extended custom properties can be populated with user data either by importing the data or by using the user interface.

1.5.1 To Enable Extended User Custom Properties

1. Open the `idw-context.xml` file located in `$RBACX_WAR/WEB-INF`.
2. Scroll down to the section of the file that contains the comment *Add Extended Global User Attributes* and locate the following lines:

   ```
   <!-- <value>extendedAttribute1</value>-->
   <!-- <value>extendedAttribute2</value>-->
   ```

3. Remove the comment tags from around the extended property lines. (Remove the `<!--` and `-->` tags for each extended attribute that you want to enable.) To create additional extended user properties, copy and paste additional extended property values in the `idw-context.xml` file and increment the number as needed (for example, `extendedAttribute3`, `extendedAttribute4`, and so on).
4. Change extended attribute label names as needed by editing the `rbacxmessages.properties` file and adding a line for each extended user property. For example:

   ```
   user.extendedAttribute1=Sample Label Name 1
   user.extendedAttribute2=Sample Label Name 2
   ```

   For more information, see the "To Modify User Labels" topic in the "Customizing the Oracle Identity Analytics User Interface" chapter of the *System Integrator's Guide for Oracle Identity Analytics*.

1.6 Working With Orphan Accounts

An orphan account is an account that does not correlate to a global user. You can assign orphan accounts to users from the user interface.

1.6.1 To Assign an Orphan Account to a User

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. Click **Orphan Accounts**.

   Resource Types are listed in the panel on the left.
4. Expand each resource type to view orphan accounts.
5. Click the **Account Name** on the right to view the Account and Entitlement details.
6. Select the account and click the **Assign to User** button.
7. Search for and select the user that you want to assign the account to.

   For help using Search, see the "Searching for a User" topic in the "Identity Warehouse" chapter of the *User's Guide for Oracle Identity Analytics*.
8. Click OK.

1.7 Creating Business Structure Rules

Business structure rules correlate users to appropriate business units based on correlation rules that you define. You can define business structure rules to reduce the need for manual correlation.

If the user meets the conditions you have specified, then the system automatically assigns the user to the business structure, along with any associated roles and policies.

1.7.1 To Create Business Structure Rules

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Business Structures**.
3. Click **Rules**.
4. Click **New Rule**.
5. Complete the **Rule Name**, **Description**, and **Status** fields, and click Next.
6. Create one or more conditions for the rule.

   Specify an object, an attribute, and the condition, and enter a value.

   - To add more conditions, select **AND** or **OR**, and click **Add Condition**.
   - Use the **Group** and **Ungroup** buttons to create complex conditions.
7. Click Next.
8. Specify the business structure and click Next.
9. Search for the user to add as the rule owner and click Next.

   For help using Search, see the "Searching for a User" topic in the "Identity Warehouse" chapter of the *User's Guide for Oracle Identity Analytics*.
10. Select an unAssign action. An unAssign action is the action taken by Oracle Identity Analytics in the event of a rule change.

    - **No Action** - Means no change takes place to the existing business structure.
    - **Remove Business Structure** - Means the business structure is removed in the event of a rule change. Only users who satisfy the new rule are now part of the business structure.
    - **Notify Administrator** - Means the administrator is notified in the event of a rule change. Click Choose Template to select an email template.
11. Click Finish.

    The business structure rule is created.
12. The following actions are optional:

    - **Preview** - Means Oracle Identity Analytics runs the rule and allows you to preview the results. However, Oracle Identity Analytics does not save the results of the rule. You can either save the results or discard them. To preview the results of the rule, see Section 1.7.2, "To Preview Results Of A Business Structure Rules Job."
    - **Run** - Means Oracle Identity Analytics runs the rule and saves the results. To run and save the results of the rule, see Section 1.7.3, "To Run Business Structure Rules Job.".

- **View results** - Oracle Identity Analytics displays the results of the rule, after you have clicked preview or run.

1.7.2 To Preview Results Of A Business Structure Rules Job

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Business Structures**.
3. Click **Rules**.

   The business structure to user rules are displayed.
4. In the **Actions** column, click **Preview** for the rule that you want to preview.

   The Rule Preview wizard opens.
5. Select a strategy from the following options:
   - **All Business Structures** - All business structures in Oracle Identity Analytics are selected.
   - **Selected Business Structures** - Only the business structures you select are included.
   - **All Users** - All users in Oracle Identity Analytics are selected.
   - **Users Criteria** - All users based on the condition you create are included.
   - **Selected Users** - Only the users that you individually select are included.
6. Based on the user selection strategy in Step 5, select the desired business structures or users and click Next.

   The summary page opens.
7. Click **Preview**.

   The **Status** column displays the progress of the preview request.
8. After the preview request is 100 percent complete, click the job name.

   The results of the preview are displayed.
9. Do one of the following:
   - To save the results, click **Apply**.
   - To return to the rules page, click **Don't Apply**.

1.7.3 To Run Business Structure Rules Job

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Business Structures**.
3. Click **Rules**.

   The business structure to user rules are displayed.
4. In the **Actions** column, click **Run** for the rule that you want to run.

   The Run Rule wizard opens.
5. Select a strategy from the following options:
   - **All Business Structures** - All business structures in Oracle Identity Analytics are selected.

- **Selected Business Structures** - Only the business structures you select are included.
- **All Users** - All users in Oracle Identity Analytics are selected.
- **Users Criteria** - All users based on the condition you create are included.
- **Selected Users** - Only the users that you individually select are included.

6. Based on the user selection strategy in step 5, select the desired business structure or users and click Next.
7. Do one of the following:
   - To run the rule immediately, click **Run Now**.

     The **Status** column displays the progress of the run request.

     – After it is 100 percent complete, click the job name.

       The results of the rule are displayed.
   - To schedule a job for the rule, click **Run Later**.

     – Complete the form and click Next.

     – Review the summary and click **Schedule**.

1.7.4 To Edit Business Structure Rules

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Business Structures**.
3. Click **Rules**.

   The business structure to user rules are displayed.
4. Click the desired rule.

   The **Edit Rule** page opens. Details of the rule are displayed on the following tabs: **General**, **Conditions**, **Ownership**, and **Unassign** Actions.
5. Choose the tabs and make changes as needed.
6. Click Save.

2 Oracle Identity Analytics Importing

This chapter contains the following sections:

- Section 2.1, "Overview"
- Section 2.2, "Understanding the Import Process"
- Section 2.3, "Configuring the Import Process"
- Section 2.4, "Verifying Imports"

2.1 Overview

Importing data in Oracle Identity Analytics is a three-step process:

- Configuring the import process
- Scheduling the import process Scheduling can be done either from the user interface or by editing configuration files on the application server.
- Verifying the import process

2.2 Understanding the Import Process

Typically, it is the administrator's responsibility to create import jobs to populate the Oracle Identity Analytics Identity Warehouse. Data can be imported from a text file or you can directly import data from either Oracle Identity Manager or Oracle Waveset if OIA is integrated with either provisioning server. Oracle Identity Analytics inserts or updates data in the data warehouse, and archives all of the data feeds.

> **Note:** You can only import resource metadata and resources if Oracle Identity Analytics is integrated with either Oracle Identity Manager or Oracle Waveset (Sun Identity Manager). For more information about importing resource metadata and resources, see either of the following chapters in the *System Integrator's Guide for Oracle Identity Analytics*:
>
> - Integrating With Oracle Identity Manager, Preferred Method
> - Integrating With Oracle Waveset (Sun Identity Manager)

The following import jobs can be executed in Oracle Identity Analytics:

- User import
- Resource metadata import (Importing from a text file not supported)

- Resources import (Importing from a text file not supported)
- Account import
- Roles import
- Policies import
- Glossary import
- Business structure import

> **Note:** While running "Import Users, Accounts, User Role Memberships and Entitlements" combo job to import data from OIM, the OIA Administrator should always uncheck the "User Role Membership" box, which is checked by default, before running the job to ensure that role rules function as expected.

To import data using text files you need a *schema file* and an *input file*. The following sections describe how to create a schema file and an input file for each type of import job.

> **Note:** You can import Resource-Attribute Values 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 Section 1.4.1, "Understanding Item Risk and Risk-Factor Mappings."

2.2.1 Importing Users

Before you can import Users into Oracle Identity Analytics using text files, you need a schema file and an input file.

2.2.1.1 Understanding the Schema File for Users

The schema file for the global-user import is a standard `.rbx` file that needs to be located in the schema folder. The `username` field is mandatory, whereas the other fields are optional. A sample schema file for user import is shown here:

```
userName,firstName,lastName,middleName,street,city,state,zip,country
```

The naming convention for the schema file is `users.rbx`.

2.2.1.2 Understanding the Input File for Users

The input file for user import maps every attribute in it to the schema file. The mapping between the user's schema file and the import file needs to be one-to-one.

The naming convention for the user import files is as follows:

`users`<*file number*>

The contents of a sample mapped user import file are shown here:

```
"Cox01","Alan 01","Cox","M","Test","Test","Test","90007","USA"
```

2.2.1.3 Global-User Schema File Reference

The following table lists details about the required and optional fields that you can include in the global-user import schema file.

Table 2–1 Global-User Import Schema File Fields

Field Name	Data Type	Max Length	Description	Required?
`userName`	Text	100		Required
`firstName`	Text	100		Required
`lastName`	Text	100		Required
`middleName`	Text	100		Optional
`street`	Text	512		Optional
`city`	Text	100		Optional
`stateOrProvince`	Text	100		Optional
`zipOrPostalCode`	Text	40		Optional
`countryOrRegion`	Text	100		Optional
`fax`	Text	100		Optional
`phone`	Text	100		Optional
`extension`	Text	100		Optional
`mobile`	Text	100		Optional
`pager`	Text	100		Optional
`title`	Text	100		Optional
`primaryEmail`	Text	100		Optional
`secondaryEmail`	Text	100		Optional
`officeName`	Text	100		Optional
`description`	Text	512		Optional
`statusKey`	Number		Must be one of the following numbers: **1** - Active **2** - Inactive	Optional
`comments`	Text	512		Optional

Table 2–1 (Continued)Global-User Import Schema File Fields

Field Name	Data Type	Max Length	Description	Required?
`suspendedDate`	Date		`yyyy-MM-dd'T'HH:mm:ss`	Optional
`userData`	Text	512		Optional
`employeeId`	Text	100		Optional

`customProperty1`
through
`customProperty20`
	Text	100		Optional

`createUser`	Text	100		Optional
`updateUser`	Text	100		Optional
`createDate`	Date		`yyyy-MM-dd'T'HH:mm:ss`	Optional
`updateDate`	Date		`yyyy-MM-dd'T'HH:mm:ss` The date and time that the record was last updated by a system external to OIA, for example an integrated provisioning system or a system that exports updates to OIA using CSV files. (A separate column, `SRM_UPDATEDATE`, saves the date and time that a record was last updated internally.)	Optional
`employeeType`	Text	100		Optional
`serviceDeskTicketNumber`	Text	200		Optional
`startDate`	Date		`yyyy-MM-dd'T'HH:mm:ss`	Optional
`endDate`	Date		`yyyy-MM-dd'T'HH:mm:ss`	Optional
`manager`	Text	100		Optional
`businessApprover`	Text	100		Optional
`technicalApprover`	Text	100		Optional
`delegate`	Text	100		Optional
`location`	Text	100		Optional
`jobCodes`	Text	512		Optional
<extendedProperty>	Text	100		Optional

2.2.1.4 To Import Users

1. Add the `users01` file:
   - For Windows - `C:\Oracle\OIA_11gR1\import\in`
   - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/in`
2. Add the `users.rbx` file:
   - For Windows - `C:\Oracle\OIA_11gR1\import\schema`
   - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/schema`

3. Schedule the import.

   See Section 10.1, "Scheduling Import and Export Jobs in Oracle Identity Analytics" for more information.

4. To Verify the Import, see Section 2.4, "Verifying Imports."

2.2.2 Importing Accounts

Before you can import Accounts into Oracle Identity Analytics using text files, you need a schema file and an input file.

2.2.2.1 Understanding the Schema File for Accounts

Oracle Identity Analytics imports accounts by resource type. Each resource type has a schema file that defines the resource type's entitlements, and the order that the entitlements need to be listed in the input file. The file extension of the schema file is `.rbx`.

> **Note:** For information about creating and modifying resource types in Oracle Identity Analytics, see Section 11.1.3, "Resource Types Configuration."

The following declaration is required to map accounts to a resource type:

```
# @iam:namespace name="<resource type's Name>" shortName="<resource type's Short
Name>"
```

The `userName` field is used for correlation and the following fields are mandatory: `name`, `endPoint`, and `domain`. All other fields are optional.

The naming convention for the schema file is as follows:

<resource type's Short Name>`_accounts.rbx`

or

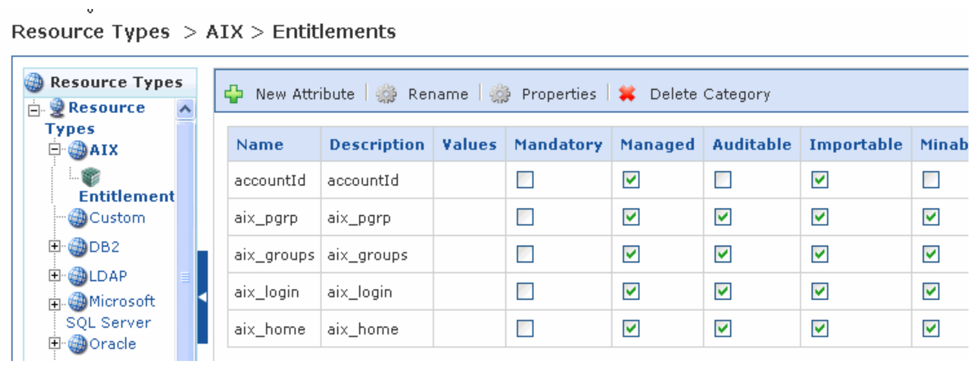
<resource type Name>`_accounts.rbx`

A sample schema file for the LDAP resource type is shown here:

```
# @iam:namespace name="LDAP" shortName="LDAP"
userName<CorrelationKey>,comments,endPoint,domain,suspended,locked,
AcidAll,AcidXAuth,FullName,GroupMemberOf,InstallationData,
ListDataResource,ListDataSource,M8All
```

The sample schema file illustrates the list of attributes or entitlements that are defined for the LDAP resource type. The `username` entry contains the name of the user account, and this is also the correlation or crossreference key between user accounts and global users. The correlation key should have `<Correlation Key>` defined next to it. Next, a list of entitlements that are common to the LDAP resource type are defined, and each entitlement is comma-separated from the other. In the sample schema file, the following fields are namespace attributes: `AcidAll`, `AcidXAuth`, `FullName`, `GroubMemberOf`, `InstallationDate`, `ListDataResource`, `ListDataSource`, and `M8All`.

To import a custom resource type entitlement, first define it in OIA (using the **Administration > Configuration > Resource Types >** ***Resource Type*** **> Entitlements** page), then add a matching entry in the schema file for each custom entitlement. The following screen capture shows custom entitlements for the AIX resource type in the OIA user interface.



Name	Description	Values	Mandatory	Managed	Auditable	Importable	Minab
accountId	accountId		☐	☑	☐	☑	☐
aix_pgrp	aix_pgrp		☐	☑	☑	☑	☑
aix_groups	aix_groups		☐	☑	☑	☑	☑
aix_login	aix_login		☐	☑	☑	☑	☑
aix_home	aix_home		☐	☑	☑	☑	☑

A sample `AIX_accounts.rbx` file with the same custom entitlements is shown here:

```
userName<CorrelationKey>,name,accountId,aix_pgrp,aix_groups,aix_login,
aix_home,domain,endPoint
```

2.2.2.2 Understanding the Input File for Accounts

An input file contains the list of user accounts and a list of user entitlements in the accounts. Each file can be differentiated from the different resource types by the naming convention used in each file.

The naming convention for the schema file is as follows:

`<resource type's Short Name>_accounts.rbx`

or

`<resource type Name>_accounts.rbx`

The following input file content matches the sample schema file for the LDAP resource:

```
"Cox01","CNBNT","VAAU","rbactest.com",5,"false",
"false","CN=DomainUsers","consultant","","",
"","DomainUsers","Consultant"
```

2.2.2.3 Accounts Schema File Reference

The following table lists details about the required and optional fields that you can include in the accounts import schema file.

In the following table, *<namespaceAttributes>* refers to the custom Resource Type attributes that you define in OIA (using the **Administration > Configuration > Resource Types >** ***Resource Type*** **> Entitlements** page) prior to importing accounts.

Table 2–2 Accounts Import Schema File Fields

Field Name	Data Type	Max Length	Description	Required?
`name`	Text	300		Required

Table 2–2 (Continued)Accounts Import Schema File Fields

Field Name	Data Type	Max Length	Description	Required?
`endPoint`	Text	256		Required **Note:** If a value for this field is not specified while creating or importing an account, then RBACx is used as the default endPoint.
`domain`	Text	512		Optional
`description`	Text	512		Optional
`comments`	Text	512		Optional
`suspended`	Number		Must be one of the following numbers: **1** - True **0** - False	Optional
`createUser`	Text	100		Optional
`updateUser`	Text	100		Optional
`itemRisk`	Number		The value must be **1, 2**, or **3**, where: **1** = high risk **2** = medium risk **3** = low risk	Optional
<*namespaceAttributes*>	Text	2000		Optional

2.2.2.4 To Import Accounts

1. Add the `LDAP_01_accounts` file:
   - For Windows - `C:\Oracle\OIA_11gR1\import\in`
   - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/in`
2. Add the `LDAP_accounts.rbx` file:
   - For Windows - `C:\Oracle\OIA_11gR1\import\schema`
   - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/schema`
3. Schedule the import.
   - See Section 10.1, "Scheduling Import and Export Jobs in Oracle Identity Analytics" for more information.
4. To Verify the Import, see Section 2.4, "Verifying Imports."

2.2.3 Importing Roles

Before you can import Roles into Oracle Identity Analytics using text files, you need a schema file and an input file.

2.2.3.1 Understanding the Schema File for Roles

The schema file for the role import is a standard `.rbx` file that needs to be specified under the schema folder. The `rolename` field is mandatory, whereas the other fields are optional.

A sample schema file for role import is shown here:

```
roleName<use=mandatory>,
roleDescription<use=required defaultValue="No Role Description">,
itemRisk, customproperty2<use=required defaultValue="No Role Owner">
```

The naming convention for the schema file is `roles.rbx`.

2.2.3.2 Understanding the Input File for Roles

The input file for roles maps every attribute in it to the schema file. The mapping between the role's schema file and import file needs to be one-to-one. The naming convention for the role import input file needs to be as follows:

`roles`<*file number*>

The contents of a sample mapped role import file are shown here:

```
"Auditor","EERS MODEL ID SG-RPAC","Auditor"
```

2.2.3.3 Roles Schema File Reference

The following table lists details about the required and optional fields that you can include in the roles import schema file.

Table 2–3 Roles Import Schema File Fields

Field Name	Data Type	Max Length	Description	Required?
`roleName`	Text	512		Required
`parentRoleName`	Text	512		Optional
`roleDescription`	Text	2048		Optional
`roleComments`	Text	2048		Optional
`department`	Text	100		Optional

`customproperty1`
through
`customproperty 10`
	Text	100		Optional

`statusKey`	Number	100		Optional
`itemRisk`	Number		Assigns an Item-Risk setting to the Role. The value must be **1, 2**, or **3**, where: **1** = high risk **2** = medium risk **3** = low risk	Optional
`jobCode`	Text			Optional
`serviceDeskTicketNumber`	Text	512		Optional

Table 2–3 (Continued)Roles Import Schema File Fields

Field Name	Data Type	Max Length	Description	Required?
`roleOwners`	CSV text	100 each	Max length is 100 per role owner.	Optional
`businessUnits`	CSV text	512 each	Max length is 512 per business unit.	Optional
`users`	CSV text	100 each	`globalusers` is also accepted. Max length is 100 per user.	Optional
`policies`	CSV text	512 each	Max length is 512 per policy.	Optional

2.2.3.4 To Import Roles

1. Add the `roles01` file:
   - For Windows - `C:\Oracle\OIA_11gR1\import\in`
   - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/in`
2. Add the `roles.rbx` file:
   - For Windows - `C:\Oracle\OIA_11gR1\import\schema`
   - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/schema`
3. Schedule the import.

   See Section 10.1, "Scheduling Import and Export Jobs in Oracle Identity Analytics" for more information.

2.2.4 Importing Policies

Before you can import Policies into Oracle Identity Analytics using text files, you need a schema file and an input file.

2.2.4.1 Understanding the Schema File for Policies

The schema file for the policy import is a standard `.rbx` file that needs to be located in the schema folder. The following declaration is required to map policies to a resource type:

```
# @iam:namespace name="<resource type's Name>" shortName="<resource type's Short Name>"
```

The `endPoints` and `policyName` fields are mandatory, whereas the other fields are optional.

The naming convention for the schema file is as follows:

<resource type's Short Name>`_policies.rbx`

A sample schema file for role import is shown here:

```
# @iam:namespace name="LDAP" shortName="LDAP" endPoints<use=mandatory>,policyName,
policyComments,ldapGroups
```

2.2.4.2 Understanding the Input File for Policies

The mapping between the policy's schema file and the import file needs to be one-to-one. Each file can be differentiated from the different resource types by the naming convention used in each file.

The naming convention for the files is as follows:

<resource type's Short Name>_<file number>`_policies`

The contents of a sample policy import file mapped are shown here:

```
"LDAP","Investment Management Attorney_LDAP","Manual Policy
import","CN=DEPT_LEGL,ou=Groups,dc=identric,dc=com"
```

2.2.4.3 Policies Schema File Reference

The following table lists details about the required and optional fields that you can include in the policies import schema file.

Table 2–4 Policies Import Schema File Fields

Field Name	Data Type	Max Length	Description	Required?
`policyName`	Text	512		Required
`endPoints`	Text	256 each	Max length is 256 per end point.	Required
`policyComments`	Text	2048		Optional
`serviceDeskTicketNumber`	Text	200		Optional
`riskLevel`	Number		The policy Risk-Level attribute is a deprecated attribute with no present usage.	Deprecated
`statusId`	Number		The value must be **1**, **2**, or **5**, where: **1** - Active **2** - Inactive **5** - Decommissioned	Optional
<namespaceAttributes>	CSV text			Optional

2.2.4.4 To Import Policies

1. Add the `LDAP_01_policies` file:
   - For Windows - `C:\Oracle\OIA_11gR1\import\in`
   - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/in`
2. Add the `LDAP_policies.rbx` file:
   - For Windows - `C:\Oracle\OIA_11gR1\import\schema`
   - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/schema`
3. Schedule the import.

   See Section 10.1, "Scheduling Import and Export Jobs in Oracle Identity Analytics" for more information.

2.2.5 Importing Business Structures

Before you can import Business Structures into Oracle Identity Analytics using text files, you need a schema file and an input file.

2.2.5.1 Understanding the Schema File for Business Structures

The schema file for the business structure import is a standard `.rbx` file that needs to be located in the schema folder. The `businessUnitName` field is mandatory, whereas the other fields are optional.

The naming convention for the schema file is `businessstructure.rbx`.

A sample schema file for business structure import is shown here:

```
businessUnitName,parentBusinessUnitName,statusKey,division,mainPhone,otherPhone,
fax,email,website,street1,street2,street3,city,stateOrProvince,zipOrPostalCode,
countryOrRegion,businessUnitType,businessUnitOwner,businessUnitAdministrator,
mailCode,businessUnitDescription,businessUnitCode,serviceDeskTicketNumber,
businessUnitManagers
```

2.2.5.2 Understanding the Input File for Business Structures

The mapping between the business structure's schema file and the import file needs to be one-to-one. The naming convention for the files is as follows:

`businessstructure_`<*file number*>

2.2.5.3 Business Structures Schema File Reference

The following table lists details about the required and optional fields that you can include in the Business Structures import schema file.

Table 2–5 Business Structures Import Schema File Fields

Field Name	Data Type	Max Length	Description	Required?
`businessUnitName`	Text	512		Required
`parentBusinessUnitName`	Text	512		Optional
`statusKey`	Number		Must be **1** or **2** where: **1** - Active **2** - Inactive If this field is not set, the default is **2** (Inactive).	Optional
`mainPhone`	Text	100		Optional
`otherPhone`	Text	100		Optional
`fax`	Text	100		Optional
`email`	Text	100		Optional
`website`	Text	100		Optional
`street1`	Text	100		Optional
`street2`	Text	100		Optional
`street3`	Text	100		Optional
`city`	Text	100		Optional

Table 2–5 (Continued)Business Structures Import Schema File Fields

Field Name	Data Type	Max Length	Description	Required?
stateOrProvince	Text	100		Optional
zipOrPostalCode	Text	100		Optional
countryOrRegion	Text	100		Optional
division	Text	100		Optional
businessUnitType	Text	100		Optional
businessUnitOwner	Text	100		Optional
businessUnitAdministrator	Text	100		Optional
businessUnitCode	Text	100		Optional
businessUnitDescription	Text	2048		Optional
mailCode	Text	100		Optional
serviceDeskTicketNumber	Text	100		Optional
businessUnitManagers	Text	2048		Optional

2.2.5.4 To Import Business Structures

1. Add the businessstructure_01 file:
   - For Windows - C:\Oracle\OIA_11gR1\import\in
   - For UNIX - /opt/Oracle/OIA_11gR1/rbacx/import/in
2. Add the businessstructure.rbx file:
   - For Windows - C:\Oracle\OIA_11gR1\import\schema
   - For UNIX - /opt/Oracle/OIA_11gR1/rbacx/import/schema
3. Schedule the import.

   See Section 10.1, "Scheduling Import and Export Jobs in Oracle Identity Analytics" for more information.

2.2.6 Importing Glossary Names

Before you can import glossary names into Oracle Identity Analytics using text files, you need a schema file and an input file.

2.2.6.1 Understanding the Schema File for Glossary Names

The schema file for the glossary import is a standard .rbx file that needs to be located in the schema folder.

The following declaration is required to map glossary to a resource type:

```
# @iam:namespace name="<resource type's Name>" shortName="<resource type's Short
Name>"
```

The endPointName, attributeName, and attributeValueValue fields are mandatory, whereas the other fields are optional. The naming convention for the schema file is<*resource type's Short Name*>_glossary.rbx.

A sample schema file for glossary import is shown below:

```
# @iam:namespace name="LDAP"
shortName="LDAP"endPointName,attributeName,attributeValueValue,owner,itemRisk,clas
sification,definition,comments
```

2.2.6.2 Understanding the Input File for Glossary Names

The mapping between the glossary's schema file and the import file needs to be one-to-one. Each file can be differentiated from the different resource types by the naming convention used in each file.

The naming convention for the files is as follows:

<*resource type's Short Name*>`_glossary`<*file number*>

2.2.6.3 Glossary Schema File Reference

The following table lists details about the required and optional fields that you can include in the glossary import schema file.

Table 2–6 Glossary Import Schema File Fields

Field Name	Data Type	Max Length	Description	Required?
`endPointName`	Text	256		Required
`attributeName`	Text	512		Required
`attributeValueValue`	Text	2000		Required
`owner`	Text	100		Optional
`itemRisk`	Number		Assigns an Item-Risk setting to the Attribute Value. The value must be **1, 2**, or **3**, where: **1** = high risk **2** = medium risk **3** = low risk If you do not include the `itemRisk` field, the default OIA "Entitlements" Risk-Mapping level will be used instead.	Optional
`classification`	Text	512		Optional
`definition`	Text	4Gb		Optional
`comments`	Text	4Gb		Optional

2.2.6.4 To Import Glossary Definitions

1. Add the `LDAP_glossary01` file:
   - For Windows - `C:\Oracle\OIA_11gR1\import\in`
   - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/in`
2. Add the `LDAP_glossary.rbx` file:
   - For Windows - `C:\Oracle\OIA_11gR1\import\schema`
   - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/schema`

3. Schedule the import.

   See Section 10.1, "Scheduling Import and Export Jobs in Oracle Identity Analytics" for more information.

2.2.7 Scheduling Import and Export Jobs

For information about scheduling import and export jobs, see Section 10.1, "Scheduling Import and Export Jobs in Oracle Identity Analytics."

2.3 Configuring the Import Process

Oracle Identity Analytics can import multiple files at the same time and can insert or update its database using different batch sizes. File import properties are configured in *$RBACX_HOME*`/conf/iam.properties`. These properties are set at their default value, and can be changed by the administrator depending on the needs of the organization.

Table 2–7 File Import Configuration Properties

Property Name	Variable	Description	Default Value
Maximum Concurrent Imports	`com.vaau.rbacx.iam.file.import.maxConcurrentImports=2`	Specifies the number of files to import concurrently.	`2`
Maximum Errors Limit	`com.vaau.rbacx.iam.file.import.rowErrorsLimit=3`	Specifies the maximum number of errors per file before aborting the process.	`3`
Batch Size	`com.vaau.rbacx.iam.file.import.batchSize=100`	Specifies the number of records to read and process in a batch during an import. **Note** - If this value is set too high, the import process will fail. A maximum value of 1000 or less is recommended.	`100`
Correlation Parameters	`com.vaau.rbacx.iam.correlation.dropOrphanAccounts=true`	Specifies whether orphan accounts (accounts that are not correlated to a global user) are dropped (True) or saved (False) as orphan accounts during the import process.	`true`
Correlation Options	`com.vaau.rbacx.iam.correlation.correlate=orphan`	Allows further control over correlation of accounts to users during the import process. Options available are Always (all accounts are correlated on every import), Orphan (only orphan accounts are correlated; established user-account associations are not updated), and Never (accounts are not correlated).	`orphan`
Drop Location	`com.vaau.rbacx.iam.file.import.dropLocation=$RBACX_HOME/import/in`	Specifies the location where the feeds to be imported are placed.	`$RBACX_HOME/import/in`

Table 2–7 (Continued)File Import Configuration Properties

Property Name	Variable	Description	Default Value
Complete Location	`com.vaau.rbacx.iam.file.import.completeLocation=$RBACX_HOME/import/complete`	Specifies the location where the input files are moved after processing.	`$RBACX_HOME/import/complete`
Schema Location	`com.vaau.rbacx.iam.file.import.schemaLocation=$RBACX_HOME/import/schema`	Specifies the location where the schema files are placed.	`$RBACX_HOME/import/schema`

2.4 Verifying Imports

You can verify if imports have been successful in the following two ways:

- Verifying from the front end
- Verifying from the back end

2.4.1 To Verify Success of Imports From the Front-End

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Auditing and Events**.
3. Select **Import/Export Logs**.

   All import jobs are listed.
4. Check the **Result** column to see if the import was successful or if it failed.

2.4.2 To Verify Success of Import From the Back-End

1. Verify success or failure of the import:

- If the import has been successful, then the input file placed in *$RBACX_Home*`/import/in` is shifted to *$RBACX_Home*`/import/complete/success`.
- If the import has failed, then the input file placed in *$RBACX_Home*`/import/in` is shifted to *$RBACX_Home*`/import/complete/error`.

For information about how to view the import-export log, see Chapter 13, "Audit Event Log and Import-Export Log."

3 Oracle Identity Analytics ETL Process

This chapter contains the following sections:

3.1 Overview

ETL stands for Extract, Transform, and Load. Oracle Identity Analytics uses CloverETL, which is a Java™-based data integration framework, to extract, transform, and load data to applications, databases, or warehouses.

3.2 Introduction

Oracle Identity Analytics provides the ability to import users, accounts, roles, and policies through CSV and XML files. It also supports a wide range of data transformations during the import process. Oracle Identity Analytics processes the CSV and XML files that are placed in a drop location and creates or updates objects in the Oracle Identity Analytics database. Oracle Identity Analytics uses different schema files (templates) to parse different data feeds (for example, users, accounts, roles, and policies). After Oracle Identity Analytics successfully processes a data feed, it moves the feed to a Completed location.

In addition to the Oracle Identity Analytics import functionality, Oracle Identity Analytics also provides the functionality to transform data feeds before they are put into the drop location. For example, Oracle Identity Analytics can read Excel and raw data files using the transformation graphs. Transformation graphs are XML files that contain machine-style processing instructions. For details, see Section 3.2.2, "Transformation Graphs."

3.2.1 Transformation Process

Oracle Identity Analytics transforms data files dropped into the ETL drop location using the transformation graphs. Oracle Identity Analytics uses CloverETL to perform all the transformation processing. At the end of transformation, ETL Manager writes the files to a specified drop location, which is usually configured as input for Oracle Identity Analytics.

3.2.2 Transformation Graphs

Transformation graphs are XML files that contain a machine-style processing instructions. The basic elements in graphs are as follows:

- Parameters
- Nodes
- Edges
- Metadata
- Phases

For example:

```
<Graph name="testing" rbacxRegxLookupFiles="tss_\w*_accounts[\.\w]*">

<Global>

<Metadata id="InMetadata" fileURL="${graphsLocation}/metadata/TSSAccount.fmt"/>

</Global>

<Phase number="0">

<Node id="INPUT" type="com... ...DelimitedDataReader" fileURL="${inputFile}"/>

<Node id="TRANSFORM" type="REFORMAT" transformClass="com... ...ReformatAccount"/>

<Node id="OUTPUT" type="com... ...DelimitedDataWriter" fileURL="${outputFile}"/>

<Edge id="INEDGE" fromNode="INPUT1:0" toNode="COPY:0" metadata="InMetadata"/>

<Edge id="OUTEDGE" fromNode="COPY:0" toNode="OUTPUT:0" metadata="InMetadata"/>

</Phase>

</Graph>
```

In the previous example, the Oracle Identity Analytics ETL processor will transform all the files dropped in the ETL location that match the `tss_\w*_accounts[\.\w]*` format to the following:

```
tss_endpoint01_accounts.csv

tss_endpoint02_accounts.csv
```

Thus, a different transformation can be applied to each Resource type and to each resource within a Resource type.

3.2.2.1 Metadata Element

Metadata defines records node for node. In the previous example, the metadata is defined in a file called `TSSAccount.fmt`.

A record must be defined as `delimited` or `fixed`. When the record is defined as `delimited`, then the attribute delimiter is required. When the record is defined as `fixed`, a `size` attribute is required.

The following example shows the contents of the `TSSAccount.fmt` file:

```
<?xml version="1.0" encoding="UTF-8"?>

<Record name="TestInput" type="delimited">

<Field name="name" type="string" delimiter=","/>

<Field name="comments" type="string" delimiter=","/>

<Field name="endPoint" type="string" delimiter=","/>

<Field name="domain" type="string" delimiter=","/>

<Field name="suspended" type="string" delimiter=","/>

<Field name="locked" type="string" delimiter=","/>

<Field name="AcidAll" type="string" delimiter=","/>

<Field name="AcidXAuth" type="string" delimiter=","/>

<Field name="FullName" type="string" delimiter=","/>

<Field name="GroupMemberOf" type="string" delimiter=","/>

<Field name="InstallationData" type="string" delimiter=","/>

<Field name="ListDataResource" type="string" delimiter=","/>

<Field name="ListDataSource" type="string" delimiter=","/>

<Field name="M8All" type="string" delimiter="\r\n"/>

</Record>
```

3.2.2.2 Node

A node is an element that performs a specific task. In the following example, the Node `INPUT` reads from a `CSV` file, the node `TRANSFORM` transforms the data, and the last Node, `OUTPUT`, writes the resulting records to a CSV file.

```
<Node id="INPUT" type="com... ...DelimitedDataReader" fileURL="${inputFile}"/>

<Node id="TRANSFORM" type="REFORMAT" transformClass="com... ...ReformatAccount"/>

<Node id="OUTPUT" type="com... ...DelimitedDataWriter" fileURL="${outputFile}"/>
```

The element's `type` attribute refers to a CloverETL or Oracle Identity Analytics class. You can specify a complete class name or a short class name.

Oracle Identity Analytics provides the following nodes to read and write CSV files:

- `com.vaau.rbacx.etl.clover.components.DelimitedDataReader`
- `com.vaau.rbacx.etl.clover.domain.DelimitedDataWriter`

Oracle Identity Analytics also provides the `com.vaau.rbacx.etl.clover.components.ExcelDataReader` node to read Excel files.

3.2.2.3 Edge

The Edge element connects nodes. Nodes can have more than one input or output. To indicate a port to connect to, add a semicolon and the port number to the Node.

```
<Edge id="INEDGE" fromNode="INPUT1:0" toNode="COPY:0"
metadata="InMetadata"/>
```

In this example, the output port 0 of the node `INPUT1` connects to the input port 0 of the node `COPY`, and the records are described in the XML element `InMetadata`.

3.2.2.4 Phase

Transformation tasks are performed in phases. When the first phase is finished, the second starts, and so on.

3.2.3 Oracle Identity Analytics CloverETL Extensions

The attributes `rbacxRegxLookupFiles` and `rbacxExecuteAlways` are not part of the CloverETL graph definition. They are processed by the Oracle Identity Analytics ETL Manager.

The attribute `rbacxRegxLookupFiles` is a regular expression for file names.

ETL Manager scans the drop location with this regular expression. When ETL Manager finds a file that matches this pattern, ETL Manager runs the graph with the following parameters:

```
inputFile : Absolute path of the file found in the Drop Location

graphsLocation : Graph Location

outputLocation : Output Location

dropLocation : Drop Location

outputFile : Absolute path for the output File
```

If the attribute `rbacxRegxLookupFiles` equals true, but no file is found (for example, if reading from a database), ETL Manager runs the graph without defining the parameters `inputFile` and `outputFile`.

3.2.3.1 Transformation Configuration

ETL properties are configured in `RBACX_HOME/conf/iam.properties`.

Table 3–1 ETL Configuration Properties

Property Name	Variable	Description
ETL Graphs Location	`eTLManager.graphsLocation=$RBACX_HOME/imports/etl/graphs`	Directory in which to place the CloverETL graph files.
ETL Drop Location	`eTLManager.dropLocation=$RBACX_HOME/imports/etl/drop`	Directory in which to place data files that need transformation.

Table 3–1 (Continued)ETL Configuration Properties

Property Name	Variable	Description
ETL Complete Location	`eTLManager.completeLocation=$RBACX_HOME/imports/etl/complete`	All processed files are moved to this directory after the ETL Manager completes the processing of the file.
ETL Output Location	`eTLManager.outputLocation=$RBACX_HOME/imports/drop`	This property specifies the directory in which to place the output of the transformation. To allow Oracle Identity Analytics to import the ETL output, this location should point to the Oracle Identity Analytics File Imports Drop Location.

3.3 Oracle Identity Analytics ETL Reference

This section includes reference information on the `DelimitedDataReader`, the `DelimitedDataWriter`, and the `ExcelDataReader`.

3.3.1 DelimitedDataReader and DelimitedDataWriter

CloverETL already has a `.csv` reader, but using the Oracle Identity Analytics version is recommended. If different delimiters are in use, however, use the CloverETL version.

Provide the file URL for the `DelimitedDataReader`.

```
<Node id="INPUT" type="com.vaau.rbacx.etl.clover.components.DelimitedDataReader"
fileURL="${inputFile}"/>
```

Provide the file URL for the `DelimitedDataWriter`.

```
<Node id="OUTPUT" type=" com.vaau.rbacx.etl.clover.domain.DelimitedDataWriter"
fileURL="${outputFile}"/>
```

3.3.2 ExcelDataReader

This Oracle Identity Analytics node reads Excel files.

Attributes:

`fileURL` - This attribute is Mandatory.

`Row_From` - Number of the initial Row. (Optional, Default value = `1`)

`Row_To` - Number of the final Row. (Optional, Default value= `-1` (All))

`Col_From` - Number of the initial Column. (Optional, Default value = `1`)

There is no `Col_To` because the reader uses the metadata to know how many columns it has to read.

```
<Node id="INPUT1" type="com.vaau.rbacx.etl.clover.components.ExcelDataReader"
fileURL="${inputFile}" Row_From="1" />
```

3.4 Transformation Examples

3.4.1 Merge

When a file with the pattern `tss_\w*_accounts[\.\w]*` is found in the drop location by the ETL Manager, the following graph is executed. The ETL Manager will read the `file_01.dat`, `file_02.dat`, and `file_03.dat` CSV files using the `com.vaau.rbacx.etl.clover.components.DelimitedDataReader` node and then merge the data with the `MERGE` node. The output file will keep the sort order stated in `mergeKey="ShipName;ShipVia"`.

The file with the pattern `tss_\w*_accounts[\.\w]*` is moved to the completed location. The files `file_01.dat`, `file_02.dat`, and `file_03.dat` stay in the `c:\tss` folder. The output file will have the same name as the input file.

```
<Graph name="TestingMerge" rbacxRegxLookupFiles="tss_\w*_accounts[\.\w]*">

<!--
This graph illustrates usage of MERGE component. It merges data based on the
specified key.
-->

<Global>

<Metadata id="InMetadata" fileURL="${graphsLocation}/metadata/tss_accunts.fmt"/>

</Global>

<Phase number="0">

<Node id="INPUT1" type="com.vaau.rbacx.etl.clover.components.DelimitedDataReader"
fileURL="c:\tss\file_01.dat"/>

<Node id="INPUT2" type="com.vaau.rbacx.etl.clover.components.DelimitedDataReader"
fileURL="c:\tss\file_02.dat"/>

<Node id="INPUT3" type="com.vaau.rbacx.etl.clover.components.DelimitedDataReader"
fileURL="c:\tss\file_03.dat"/>

<Node id="MERGE" type="MERGE" mergeKey="ShipName;ShipVia"/>

<Node id="OUTPUT" type="com.vaau.rbacx.etl.clover.domain.DelimitedDataWriter"
fileURL="${outputFile}"/>

<Edge id="INEDGE1" fromNode="INPUT1:0" toNode="MERGE:0" metadata="InMetadata"/>

<Edge id="INEDGE2" fromNode="INPUT2:0" toNode="MERGE:1" metadata="InMetadata"/>

<Edge id="INEDGE3" fromNode="INPUT3:0" toNode="MERGE:2" metadata="InMetadata"/>

<Edge id="OUTEDGE" fromNode="MERGE:0" toNode="OUTPUT:0" metadata="InMetadata"/>

</Phase>

</Graph>
```

3.4.2 Filter

The following graph demonstrates the functionality of the Extended Filter component.

It can filter on text, date, integer, and numeric fields with comparison operators: (>, <, ==, <=, >=, !=).

Text fields can also be compared to a Java regular expression using the ~= operator.

A filter can be made of different parts separated by a logical operator `AND` or `OR`. Parentheses for grouping individual comparisons are also supported. For example, `$Age>10` and `($Age <20 or $HireDate<"2003-01-01").`

A filter works on a single input record, where individual fields of the record are referenced using a dollar sign and the field's name. For example, `$Age,$Name`.

The date format for date constants is `yyyy-MM-dd` or `yyyy-MM-dd hh:mm:ss`.

The following graph produces one output file where all employees have the pattern "`DELTSO[0-9]*0`" in the comments field.

```
<Graph name="Testing Filter" rbacxRegxLookupFiles="tss_\w*_accounts[\.\w]*">

<Global>

<Metadata id="InMetadata" fileURL="${graphsLocation}/metadata/InAccounts.fmt"/>

</Global>

<Phase number="0">

<Node id="INPUT1" type="com.vaau.rbacx.etl.clover.components.DelimitedDataReader"
fileURL="\$\{inputFile\}"/>

<Node id="FILTEREMPL2" type="EXT_FILTER">

$comments~="DELTSO[0-9]*0"

</Node>

<Node id="OUTPUT1"
type="com.vaau.rbacx.etl.clover.components.DelimitedDataWriter"
fileURL="\$\{outputFile\}"/>

<Edge id="INEDGE1" fromNode="INPUT1\:0" toNode="FILTEREMPL2:0"
metadata="InMetadata"/>

<Edge id="INNEREDGE3" fromNode="FILTEREMPL2\:0" toNode="OUTPUT1:0"
metadata="InMetadata"/>

</Phase>

</Graph>
```

3.4.3 Fixed Length Data Reader

The following graph transforms a Fixed Length Data file into a CSV file.

```
<Graph name="Testing Filter" rbacxRegxLookupFiles="tss_\w*_accounts[\.\w]*">
```

```
<Global>

<Metadata id="OutMetadata" fileURL="${graphsLocation}/metadata/InAccounts.fmt"/>

<Metadata id="InMetadata"
fileURL="${graphsLocation}/metadata/InAccountsFixedWith.fmt"/>

</Global>

<Phase number="0">

<Node id="INPUT1" type="FIXLEN_DATA_READER_NIO" OneRecordPerLine="true"
SkipLeadingBlanks="true" LineSeparatorSize="2" fileURL=" $ { inputFile } "/>

<Node id="COPY" type="SIMPLE_COPY"/>

<Node id="OUTPUT1"
type="com.vaau.rbacx.etl.clover.components.DelimitedDataWriter"
fileURL="${outputFile}"/>

<Edge id="INEDGE1" fromNode="INPUT1:0" toNode="COPY:0" metadata="InMetadata"/>

<Edge id="OUTEDGE1" fromNode="COPY:0" toNode="OUTPUT1:0" metadata="OutMetadata"/>

</Phase>

</Graph>
```

Following is the contents of the file `InAccountsFixedWith.fmt`.

```
<?xml version="1.0" encoding="UTF-8"?>

<Record name="TestInput" type="fixed">

<Field name="name" type="string" size="16"/>

<Field name="comments" type="string" size="16"/>

<Field name="endPoint" type="string" size="16"/>

<Field name="domain" type="string" size="5"/>

<Field name="suspended" type="string" size="10"/>

<Field name="locked" type="string" size="10"/>

<Field name="AcidAll" type="string" size="10"/>

<Field name="AcidXAuth" type="string" size="10"/>

<Field name="FullName" type="string" size="40"/>

<Field name="GroupMemberOf" type="string" size="60"/>

<Field name="InstallationData" type="string" size="60"/>

<Field name="ListDataResource" type="string" size="10"/>
```

```
<Field name="ListDataSource" type="string" size="10"/>

<Field name="M8All" type="string" size="10"/>

</Record>
```

3.4.4 Database Input

This node imports data from databases. In the following example, the ETL Manager executes the graph for each file that matches the pattern in `rbacxRegxLookupFiles`.

```
<Graph name="Testing Filter" rbacxRegxLookupFiles="tss_\w*_accounts[\.\w]*">

<Global>

<Metadata id="InMetadata"
fileURL="${graphsLocation}/metadata/InAccountsFromDB.fmt"/>

<Metadata id="OutMetadata"
fileURL="${graphsLocation}/metadata/OutAccounts.fmt"/>

<DBConnection id="InterbaseDB" dbConfig="${graphsLocation}/dbConfig/Rbacx.cfg"/>

</Global>

<Phase number="0">

<Node id="INPUT1" type="DB_INPUT_TABLE"

dbConnection="InterbaseDB">


<SQLCode>

select * from tss_01_accounts

</SQLCode>

</Node>

<Node id="COPY" type="REFORMAT" >

import org.jetel.component.DataRecordTransform;

import org.jetel.data.DataRecord;

import org.jetel.data.SetVal;

import org.jetel.data.GetVal;


public class reformatAccount extends DataRecordTransform{

int counter=0;

DataRecord source;

DataRecord target;
```

```
public boolean transform(DataRecord _source[], DataRecord[] _target) {

StringBuffer strBuf = new StringBuffer(80);

source=_source[0];

target=_target[0];

try {

SetVal.setString(target,"name",GetVal.getString(source,"name"));

SetVal.setString(target,"comments",GetVal.getString(source,"comments"));

SetVal.setString(target,"endPoint",GetVal.getString(source,"endPoint"));

SetVal.setString(target,"domain",GetVal.getString(source,"domain"));

SetVal.setString(target,"suspended",
getBooleanString(GetVal.getInt(source,"suspended")));

SetVal.setString(target,"locked",
getBooleanString(GetVal.getString(source,"locked")));

SetVal.setString(target,"AcidAll",GetVal.getString(source,"AcidAll"));

SetVal.setString(target,"AcidXAuth",GetVal.getString(source,"AcidXAuth"));

SetVal.setString(target,"FullName",GetVal.getString(source,"FullName"));

SetVal.setString(target,"GroupMemberOf",
GetVal.getString(source,"GroupMemberOf"));

SetVal.setString(target,"InstallationData",
GetVal.getString(source,"InstallationData"));

SetVal.setString(target,"ListDataResource",
GetVal.getString(source,"ListDataResource"));

SetVal.setString(target,"ListDataSource",
GetVal.getString(source,"ListDataSource"));

SetVal.setString(target,"M8All",GetVal.getString(source,"M8All"));

}

catch (Exception ex) {

errorMessage = ex.getMessage() + " ->occured with record :" + counter;

return false;

}

counter++;

return true;

}
```

```
private String getBooleanString(int value){

if(value==0)

return "FALSE";

else

return "TRUE";

}

}

</Node>

<Node id="OUTPUT1"
type="com.vaau.rbacx.etl.clover.components.DelimitedDataWriter"
fileURL="${outputFile}/>



<Edge id="INEDGE1" fromNode="INPUT1:0" toNode="COPY:0"
metadata="InMetadata"/>

<Edge id="OUTEDGE1" fromNode="COPY:0" toNode="OUTPUT1:0"
metadata="OutMetadata"/>

</Phase>

</Graph>
```

If you don't want to execute this graph by putting a file in the drop location, add the attribute `rbacxExecuteAlways=true`.

```
<Graph name="Testing Filter" rbacxExecuteAlways="true" >

<Global>

<Metadata id="InMetadata"
fileURL="${graphsLocation}/metadata/InAccountsFromDB.fmt"/>

<Metadata id="OutMetadata"
fileURL="${graphsLocation}/metadata/OutAccounts.fmt"/>

<DBConnection id="InterbaseDB" dbConfig="${graphsLocation}/dbConfig/Rbacx.cfg"/>

</Global>

<Phase number="0">

<Node id="INPUT1" type="DB_INPUT_TABLE"

dbConnection="InterbaseDB">
```

```
<SQLCode>

select * from tss_01_accounts

</SQLCode>

</Node>

<Node id="COPY" type="REFORMAT" >

import org.jetel.component.DataRecordTransform;

import org.jetel.data.DataRecord;

import org.jetel.data.SetVal;

import org.jetel.data.GetVal;


public class reformatAccount extends DataRecordTransform{

int counter=0;

DataRecord source;

DataRecord target;

public boolean transform(DataRecord _source[], DataRecord[] _target) {

StringBuffer strBuf = new StringBuffer(80);

source=_source[0];

target=_target[0];

try {

SetVal.setString(target,"name",GetVal.getString(source,"name"));

SetVal.setString(target,"comments",GetVal.getString(source,"comments"));

SetVal.setString(target,"endPoint",GetVal.getString(source,"endPoint"));

SetVal.setString(target,"domain",GetVal.getString(source,"domain"));

SetVal.setString(target,"suspended",
getBooleanString(GetVal.getInt(source,"suspended")));

SetVal.setString(target,"locked",
getBooleanString(GetVal.getString(source,"locked")));

SetVal.setString(target,"AcidAll",GetVal.getString(source,"AcidAll"));

SetVal.setString(target,"AcidXAuth",GetVal.getString(source,"AcidXAuth"));

SetVal.setString(target,"FullName",GetVal.getString(source,"FullName"));

SetVal.setString(target,
"GroupMemberOf",GetVal.getString(source,"GroupMemberOf"));
SetVal.setString(target,
"InstallationData",GetVal.getString(source,"InstallationData"));

SetVal.setString(target,
"ListDataResource",GetVal.getString(source,"ListDataResource"));

SetVal.setString(target,
"ListDataSource",GetVal.getString(source,"ListDataSource"));

SetVal.setString(target,"M8All",GetVal.getString(source,"M8All"));

}

catch (Exception ex) {

errorMessage = ex.getMessage() + " ->occured with record :" + counter;

return false;

}

counter++;

return true;

}



private String getBooleanString(int value){

if(value==0)

return "FALSE";

else

return "TRUE";

}

}

</Node>

<Node id="OUTPUT1"
type="com.vaau.rbacx.etl.clover.components.DelimitedDataWriter"
fileURL="${outputLocation}/tss_01_accounts.dat"/>


<Edge id="INEDGE1" fromNode="INPUT1:0" toNode="COPY:0"
metadata="InMetadata"/>

<Edge id="OUTEDGE1" fromNode="COPY:0" toNode="OUTPUT1:0"
metadata="OutMetadata"/>

</Phase>

</Graph>
```

3.5 Load and Unload Data From the Database

This section discusses how to move data to and from the database using CloverETL.

3.5.1 How CloverETL Works With Databases

CloverETL uses the JDBC™ API to communicate with databases. If your database has a driver supporting the JDBC API, CloverETL can be used to unload data stored within database table, or it can populate a database table with internal data.

3.5.2 DBConnection

Before you can connect to a database, you must define the DBConnection. This property is defined within a graph.

```
<DBConnection id="InterbaseDB" dbConfig="Interbase.cfg"/>
```

This specifies that CloverETL should set up a database connection called InterbaseDB. All required parameters (JDBC driver name, DB connect string, user name, and password) can be found in the configuration file `Interbase.cfg`.

The `dbConfig` file is a standard Java properties file. It contains names of parameters along with their values. The following table lists the possible parameters.

Table 3–2 DBConnection Parameters

Parameter Name	Description of Parameter	Example of Parameter's Value
`dbDriver`	Specifies the name of the class containing the JDBC driver for your database. This class must be visible to Java (be part of `CLASSPATH`).	`org.postgresql.Driver`
`dbURL`	URL for connecting to the database, including the name of JDBC driver to use, the IP address where the server listens, the name of the database instance, and the port.	`jdbc:postgresql://192.168.1.100/mydb`
`user`	The user name under which to connect to the database.	`Admin`
`password`	The password to be used.	`free`
`driverLibrary`	Optional. The location of the JDBC driver class.	`c:\Oracle\product\10.1.0\Client_1\jdbc\lib\ojdbc14.jar`
JDBC driver-specific parameters	Optional. Specify as needed.	Oracle example: `defaultRowPrefetch=10`

The following example lists the possible contents of a `Postgres.cfg` file that defines the connection to a PostgreSQL database:

Postgres.cfg

```
dbDriver=org.postgresql.Driver

dbURL=jdbc:postgresql://192.168.1.100/mydb
```

```
user=david

password=unknown
```

All parameters can also be directly specified when defining the connection:

Defining Connection

```
<DBConnection id="InterbaseDB" dbDriver="org.postgresql.Driver"
dbURL="jdbc:postgresql://192.168.1.100/mydb" user="david" password="unknown"/>
```

The values specified with the `dbConfig` parameter takes precedence over parameters specified in a properties file.

3.5.2.1 Mapping JDBC Data Types to Clover Types

When working with the database through JDBC drivers, CloverETL needs to map its internal data types onto JDBC data types. The variety of DB (JDBC) field types is large, but most of them (with the exception of BLOBs) can be mapped to Clover internal types without losing any information.

3.5.2.2 JDBC to CloverETL

The following table lists JDBC data types and corresponding CloverETL data types. The conversion is done automatically by CloverETL when analyzing DB tables using the `org.jetel.database.AnalyzeDB` utility. This conversion can also be made manually.

Table 3–3 JDBC Data Types and Corresponding CloverETL Data Types

JDBC (DB) Data Type	CloverETL Data Type
INTEGER SMALLINT TINYINT	INTEGER
BIGINT	LONG
DECIMAL DOUBLE FLOAT NUMERIC REAL	NUMERIC
CHAR LONGVARCHAR VARCHAR OTHER	STRING
DATE TIME TIMESTAMP	DATE
BOOLEAN BIT	STRING (True value coded as `T`; false value coded as `F`)

The following example illustrates the conversion. First, the DDL (Oracle DB) definition of the database table is presented, and then Clover's version of the same thing using its internal data types.

DDL (Oracle DB)

```
create table MYEMPLOYEE

(

  EMP_NO      NUMBER not null,

  FIRST_NAME  VARCHAR2(15) not null,

  LAST_NAME   VARCHAR2(20) not null,

  PHONE_EXT   VARCHAR2(4),

  HIRE_DATE   DATE not null,

  DEPT_NO     CHAR(3) not null,

  JOB_CODE    VARCHAR2(5) not null,

  JOB_GRADE   NUMBER(4,2) not null,

  JOB_COUNTRY VARCHAR2(15) not null,

  SALARY      NUMBER(15,2) not null,

  FULL_NAME   VARCHAR2(35)

);
```

Clover's Version

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Automatically generated from database null -->

<Record name="EMPLOYEE" type="delimited">

    <Field name="EMP_NO" type="numeric" delimiter="," format="#"/>

    <Field name="FIRST_NAME" type="string" delimiter="," />

    <Field name="LAST_NAME" type="string" delimiter="," />

    <Field name="PHONE_EXT" type="string" nullable="yes" delimiter="," />

    <Field name="HIRE_DATE" type="date" delimiter="," format="dd/MM/yyyy" />

    <Field name="DEPT_NO" type="string" delimiter="," />

    <Field name="JOB_CODE" type="string" delimiter="," />

    <Field name="JOB_GRADE" type="numeric" delimiter="," />

    <Field name="JOB_COUNTRY" type="string" delimiter="," />
    <Field name="SALARY" type="numeric" delimiter="," />

    <Field name="FULL_NAME" type="string" nullable="yes" delimiter="\n" />

</Record>
```

3.5.2.3 CloverETL to JDBC

The reverse conversion from a CloverETL to JDBC data type (usually done when populating a target DB table) is also driven by JDBC data types. There are some exceptions that are caused by the non-existence of certain field types on the CloverETL side. These exceptions are handled automatically by CloverETL. Internally it is done by calling different than standard JDBC methods for populating database fields with values. Refer to the source code (`org.jetel.database.CopySQLData`) to get detailed information.

Table 3–4 Conversions Performed When Converting From CloverETL to JDBC

JDBC Type	CloverETL Type	Conversion Performed
Timestamp	Date	Date is converted to Timestamp, and the target is set using the `setTimestamp()` method.
Boolean Bit	String	If the string contains `T` or `t`, the target is set to be True; otherwise False using `setBoolean()`
Decimal Double Numeric Real	Integer	Conversion from Integer to Decimal is made. The target is set using the `setDouble()` method.
Other (includes `NVARCHAR` and `NCHAR`)	String	The target is set using the `setString()` method.

3.5.3 Using the AnalyzeDB Utility

The CloverETL package contains a simple utility that can analyze a source or target database table and produce Clover's metadata description file. This metadata can be used by any DB-related component.

The following table lists the parameters that can be specified with the `AnalyzeDB` command. The command must specify which database to connect to and which database table to analyze. You can use the same `DBConnection` file described previously in Section 3.5.2, "DBConnection."

To specify which table to analyze, supply an SQL query to execute against the database. The returned result set is examined for field types. As a result, you can extract and analyze a portion of table.

The following table lists the options and parameters:

Table 3–5 Parameters for use With the AnalyzeDB Utility

Parameter	Description
`-dbDriver`	JDBC driver to use
`-dbURL`	Database name (URL)

Table 3–5 (Continued)Parameters for use With the AnalyzeDB Utility

Parameter	Description
`-config`	Config or Property file containing parameters
`-user`	User name
`-password`	User's password
`-d`	Delimiter to use (a comma `,` is standard)
`-o`	Output file to use (`stdout` is standard)
`-f`	Read SQL query from file name
`-q`	SQL query on command line
`-info`	Displays list of driver's properties

The following example examines all data fields of the employees DB table:

```
java -cp cloverETL.rel-1-x.zip org.jetel.database.AnalyzeDB -config postgres.sql
-q "select * from employees where 1=0"
```

The following example extracts specific fields, as stated in the SQL query:

```
java -cp cloverETL.rel-1-x.zip org.jetel.database.AnalyzeDB -config postgres.sql
-q "select emp_no,full_name from employees where 1=0"
```

3.5.4 DBInputTable Component

To unload data from the database table, use the `DBInputTable` component. It requires that the `dbConnection` parameter be specified and an SQL command (`sqlQuery` parameter), which will be executed against the database specified by `dbConnection`.

Individual fields fetched from the database are mapped to Clover data records/fields. (See Section 3.5.2.2, "JDBC to CloverETL."). The structure of the Clover record is determined by specified Clover metadata. (Metadata is assigned to an Edge, which connects `DBInputTable` with other components connected to `DBInputTable`.)

The following example transformation graph uses the `DBInputTable` component:

Transformation Graph

```
<?xml version="1.0" encoding="UTF-8"?>

<Graph name="TestingDB">

<Global>

<Metadata id="InMetadata" fileURL="metadata/employee.fmt"/>

<DBConnection id="PosgressDB" dbConfig="Posgress.cfg"/>

</Global>

<Phase number="0">

<Node id="INPUT" type="DB_INPUT_TABLE" dbConnection="PosgressDB"

sqlQuery="select * from employee"/>

<Node id="OUTPUT" type="DELIMITED_DATA_WRITER_NIO" append="false"
```

```
fileURL="employees2.list.out"/>

<Edge id="INEDGE" fromNode="INPUT:0" toNode="OUTPUT:0"

metadata="InMetadata"/>

</Phase>

</Graph>
```

The SQL command (`sqlQuery`) can be more complicated than the previous example suggests. You can use any valid SQL construct, but make sure that the metadata corresponds to the number and types of returned data fields.

3.5.5 DBOutputTable Component

When there is a need to populate a database table with data coming from a CloverETL transformation graph, the `DBOutputTable` component can be used to fulfill it. It is complementary to `DBInputTable`. It maps CloverETL data records and individual fields to target database table fields. It can perform simple data conversions to successfully map CloverETL basic data types on to target database variants. See the previous Section 3.5.2.3, "CloverETL to JDBC."

The following example illustrates the usage of `DBOutputTable`:

```
<?xml version="1.0" encoding="UTF-8"?>

<Graph name="TestingDB2">

<Global>

<Metadata id="InMetadata" fileURL="metadata/myemployee.fmt"/>

<DBConnection id="PosgressDB" dbConfig="posgress.cfg"/>

</Global>

<Phase number="0">

<Node id="INPUT" type="DELIMITED_DATA_READER_NIO"

fileURL="employees.list.dat" />

<Node id="OUTPUT" type="DB_OUTPUT_TABLE" dbConnection="PosgressDB"

dbTable="myemployee" />

<Edge id="INEDGE" fromNode="INPUT:0" toNode="OUTPUT:0"

metadata="InMetadata"/>

</Phase>

</Graph>
```

If you need to populate only certain fields of the target DB table (when, for instance, one field is automatically populated from a DB sequence), the `dbFields` parameter of `DBOutputTable` can be used:

```
<Node id="OUTPUT2" type="DB_OUTPUT_TABLE" dbConnection="PosgressDB"
dbTable="myemployee" dbFields="FIRST_NAME;LAST_NAME" />
```

The `DBOutputTablecloverFields` parameter can be used to precisely specify mapping from CloverETL data records to database table records. It allows you to specify which source field (from Clover) is mapped to which target database table field.

Coupled with `dbFields`, it specifies a 1:1 mapping. Individual fields are mapped according to the order in which they appear in `dbFields` and `cloverFields`, respectively. The parameter that determines how many fields will be populated is always `dbFields`. When there is no `dbFields` parameter present, CloverETL assumes that all target fields should be populated in the order in which they appear in the target database table.

The following examples illustrate how to pick certain fields from the source data record (a CloverETL record), regardless of their order, and map them to target database table fields (again, regardless of their order).

```
<?xml version="1.0" encoding="UTF-8"?>

<Graph name="TestingDB3">

<Global>

<Metadata id="InMetadata" fileURL="metadata/myemployee.fmt"/>

<DBConnection id="PosgressDB" dbConfig="posgress.cfg"/>

</Global>

<Phase number="1">

<Node id="INPUT" type="DELIMITED_DATA_READER_NIO"

fileURL="employees2.list.tmp" />

<Node id="OUTPUT" type="DB_OUTPUT_TABLE" dbConnection="InterbaseDB"

dbTable="myemployee"

    dbFields="FIRST_NAME;LAST_NAME"

    cloverFields="LAST_NAME;FIRST_NAME" />

<Edge id="INEDGE" fromNode="INPUT:0" toNode="OUTPUT:0"

metadata="InMetadata"/>

</Phase>

</Graph>
```

The resulting mapping between fields specified in the previous example is:

Source Field (CloverETL)	Target Field (DB Table)
LAST_NAME	FIRST_NAME
FIRST_NAME	LAST_NAME

3.5.6 Executing SQL/DML/DDL Statements against DB

Sometimes you need to execute one or more database commands that do not require any input. Examples include creating a new table, adding a data partition, and dropping an index. For this purpose, CloverETL offers the DBExecute component.

3.5.6.1 DBExecute Component

The DBExecute component takes specified commands and executes them one by one against the database. You can define whether all commands form one transaction, or whether they should be committed to the database after each command.

The following is a simple example of DBExecute:

```
<?xml version="1.0" encoding="UTF-8"?>

<Graph name="TestingExecute">

<Global>

<DBConnection id="InterbaseDB" dbConfig="interbase.cfg"/>

</Global>

<Phase number="0">

<Node id="DBEXEC" type="DB_EXECUTE" dbConnection="InterbaseDB"

inTransaction="N">

<SQLCode>

create table EMPLOYEE

(

  EMP_NO      NUMBER not null,

  FIRST_NAME  VARCHAR2(15) not null,

  LAST_NAME   VARCHAR2(20) not null,

  PHONE_EXT   VARCHAR2(4),

  HIRE_DATE   DATE not null,

  DEPT_NO     CHAR(3) not null,

  JOB_CODE    VARCHAR2(5) not null,

  JOB_GRADE   NUMBER(4,2) not null,

  JOB_COUNTRY VARCHAR2(15) not null,

  SALARY      NUMBER(15,2) not null,
  FULL_NAME   VARCHAR2(35)

);

insert into employee values(2,'Robert','Nelson','250',28/12/1988,'600','VP',2.0,
'USA',105900.0,'Nelson, Robert');

insert into employee values(4,'Bruce','Young','233',28/12/1988,'621','Eng',2.0,
'USA',97500.0,'Young, Bruce');

insert into employee values(5,'Kim','Lambert','22',06/02/1989,'130','Eng',2.0,
'USA', 102750.0,'Lambert, Kim');

insert into employee values(8,'Leslie','Johnson','410',05/04/1989,'180','Mktg',
3.0,'USA', 64635.0,'Johnson, Leslie');

insert into employee
values(9,'Phil','Forest','229',17/04/1989,'622','Mngr',3.0,'USA',75060.0,'Forest,

Phil');

</SQLCode>

</Node>

</Phase>

</Graph>
```

3.6 CloverETL DataRecord Reference

This section provides additional information about the CloverETL DataRecord.

3.6.1 How Data is Represented Within CloverETL

CloverETL works with data in terms of data records, and data fields within records. Internally, all records are represented as variable-length data. This means that every data field consumes only as much memory as needed for storing a field's value. If you have a field of type STRING specified to be 50 characters in length and this field is populated with a string of 20 characters, only 20 characters are allocated in memory.

Moreover, CloverETL does not require that a length be specified. There is an internal maximum length for any field, but it should be enough to accommodate even very long strings. For types other than strings, there is fixed size of the field, regardless of the actual value.

There are some cases when it matters whether you specify the size of each field. This is discussed in the next section.

3.6.2 Supported Data Field Types

The following table lists all supported types of data, along with ranges of values for each type.

Table 3–6 Supported Data Types and Value Ranges in CloverETL

Data Type Name	Based on	Size	Range of Values
string	`java.lang.String`	Depends on actual data length	
date	`java.util.Date`	64bit - sizeof(long)	Starts: January 1, 1970, 00:00:00 GMT increment: 1ms
integer	`java.lang.Integer`	32bit - sizeof(int)	Min: -2^{31} Max: $2^{31}-1$
numeric	`java.lang.Double`	64bit - sizeof(double)	Min:2^{-1074} Max: $(2-2^{-52})\ 2^{1023}$
long	`java.lang.Long`	64bit - size of (long)	Min: $2^{63}-1$ Max: -2^{63}
decimal	NA	NA	Not yet implemented
byte	`java.lang.Byte`	Depends on actual data length	Min: 0 Max: 255

3.6.3 Specification of Record Format

One way of putting together a description of a record format is to create some Java code and use CloverETL classes/methods calls.

The easier way is to create an XML description of a record format that can be read by CloverETL and automatically materialized in memory.

It is customary to use the `.fmt` extension for an XML file that contains metadata describing the format of a data record. The following example shows simple metadata that describes a record containing three data fields:

```
<?xml version="1.0" encoding="UTF-8"?>

<Record name="TestInput" type="delimited">

<Field name="Name" type="string" delimiter=";"/>

<Field name="Age" type="numeric" delimiter="|"/>

<Field name="City" type="string" delimiter="\n"/>

</Record>
```

This simple example shows the definition of a data record specified as delimited. The record has three fields:

- Name (of type string)
- Age (of type numeric)
- City (of type string)

3.6.3.1 Naming

The are no strict rules for naming fields (and records). However, you use the same rules as for naming Java variables. For example, use only letters [a-zA-Z], numbers [0-9] (not in the first position), and underscores [_].

The encoding specified for the XML file is UTF-8.

> **Note:** When creating a file, you must save the file using the encoding specified in the encoding tag. Otherwise, the XML parser used by CloverETL won't be able to correctly interpret the file.

3.6.4 Delimiters

Each field in the previous example has a specified delimiter character. This information is used by the data parser when parsing data records (of this structure) from external text files. The same delimiters are used when CloverETL outputs internal data records (of this structure) to output text files.

Delimiters can be up to 32 characters long, and each field can have a different one. Basic control characters such as `\t` (tabulator), `\n` (line feed), and `\r` (carriage return) are supported.

3.6.5 Field Formats and Other Features

The following example shows additional features:

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Automatically generated from database null -->

<Record name="EMPLOYEE" type="delimited">

    <Field name="EMP_NO" type="integer" delimiter="," format="#"/>

    <Field name="FIRST_NAME" type="string" delimiter="," />

    <Field name="LAST_NAME" type="string" delimiter="," />

    <Field name="PHONE_EXT" type="string" nullable="yes" delimiter="," />

    <Field name="HIRE_DATE" type="date" delimiter="," format="dd/MM/yyyy" />

    <Field name="BIRTH_DATE" type="date" delimiter="," locale="en"/>

    <Field name="DEPT_NO" type="string" delimiter="," />

    <Field name="JOB_CODE" type="string" delimiter="," />

    <Field name="JOB_GRADE" type="numeric" delimiter="," format="#" />

    <Field name="JOB_COUNTRY" type="string" delimiter="," />

    <Field name="SALARY" type="numeric" delimiter="," />

    <Field name="FULL_NAME" type="string" nullable="yes" delimiter="\n" />

</Record>
```

3.6.5.1 Nullable

Some fields, such as PHONE_EXT, have the nullable attribute set to yes, which means that the field is allowed to contain a null value. The default is yes or true (that is, the field can contain a null value). The exact behavior is influenced by a concrete data parser or data formatter, but simply put, when a field is not specified to be nullable and an application tries to put a null value in it, this operation fails. This can stop the whole transformation process.

3.6.5.2 Format

Use the Format attribute to specify the expected format of data when parsing in, or printing out of, CloverETL. In this case, the HIRE_DATE field is of type date and it is specified that date values in external textual data will look like this: 19/12/1999

For all possible format specifiers (control characters), see the documentation for java.text.SimpleDateFormat.

Similar to HIRE_DATE is the JOB_GRADE field, which is of type numeric. Here the format specifies that data is expected to be integer numbers only (no decimal point allowed).

See the following tables for date and number format specifiers.

3.6.5.3 Date and Time Specifiers

Table 3–7 Date and Time Specifiers

Letter	Date or Time Component	Presentation	Examples
G	Era designator	Text	AD
y	Year	Year	1996; 96
M	Month in year	Month	July; Jul; 07
w	Week in year	Number	27
W	Week in month	Number	2
D	Day in year	Number	189
d	Day in month	Number	10
F	Day of week in month	Number	2
E	Day in week	Text	Tuesday; Tue
a	Am/pm marker	Text	PM
H	Hour in day (0-23)	Number	0
k	Hour in day (1-24)	Number	24
K	Hour in am/pm (0-11)	Number	0
h	Hour in am/pm (1-12)	Number	12
m	Minute in hour	Number	30
s	Second in minute	Number	55
S	Millisecond	Number	978

Table 3–7 (Continued)Date and Time Specifiers

Letter	Date or Time Component	Presentation	Examples
`z`	Time zone	General time zone	Pacific Standard Time; PST; GMT-08:00
`Z`	Time zone	RFC 822 time zone	-0800

3.6.5.4 Date and Time Format Examples

Table 3–8 Date and Time Format Examples

Date and Time Pattern	Result
`"yyyy.MM.dd G 'at' HH:mm:ss z"`	2001.07.04 AD at 12:08:56 PDT
`"EEE, MMM d, ''yy"`	Wed, Jul 4, '01
`"h:mm a"`	12:08 PM
`"hh 'o''clock' a, zzzz"`	12 o'clock PM, Pacific Daylight Time
`"K:mm a, z"`	0:08 PM, PDT
`"yyyyy.MMMMM.dd GGG hh:mm aaa"`	02001.July.04 AD 12:08 PM
`"EEE, d MMM yyyy HH:mm:ss Z"`	Wed, 4 Jul 2001 12:08:56 -0700
`"yyMMddHHmmssZ"`	010704120856-0700

3.6.5.5 Number Specifiers

Table 3–9 Number Specifiers

Symbol	Location	Localized	Meaning
`0`	Number	Localized	Digit
`#`	Number	Localized	Digit, zero shows as absent
`.`	Number	Localized	Decimal separator or monetary decimal separator
`-`	Number	Localized	Minus sign
`,`	Number	Localized	Grouping separator
`E`	Number	Localized	Separates mantissa and exponent in scientific notation. Need not be quoted in prefix or suffix.
`;`	Subpattern boundary	Localized	Separates positive and negative subpatterns
`%`	Prefix or suffix	Localized	Multiply by 100 and show as percentage
`\u2030`	Prefix or suffix	Localized	Multiply by 1000 and show as per mille
`(\u00A4)`	Prefix or suffix	Not localized	Currency sign, replaced by currency symbol. If doubled, replaced by international currency symbol. If present in a pattern, the monetary decimal separator is used instead of the decimal separator.
`'`	Prefix or suffix	Not localized	Used to quote special characters in a prefix or suffix, for example, `"'#'#"` formats 123 to "#123". To create a single quote itself, use two in a row: `"# o''clock"`.

3.6.5.6 Number Format

When specifying the format for numbers, Clover (Java) uses the default system locale setting, unless another locale is specified through the locale option.

This is important in cases when you are parsing data where decimal numbers use a , (comma) as a decimal separator, whereas the system default (global) says it is . (period).

In such a case, use the locale option together with the format option to change the expected decimal delimiter. For example:

```
<Field name="Freight" type="numeric" delimiter="|" format="#.#" locale="en.US" />
```

3.6.5.7 Locale

Instead of specifying a format parameter, you can specify a locale parameter, which states the geographical, political, or cultural region for formatting data. Thus, instead of specifying the format for the date field, you could specify the locale for Germany (`locale="de"`), for example. Clover automatically chooses the proper date format for Germany.

There are cases when both format and locale parameters make sense, for example when formatting decimal numbers. Define the format pattern with a decimal separator, and the locale specifies whether the separator is a comma or a dot.

3.6.6 Specifying Default Values for Fields

CloverETL allows you to specify a default value for each field. This value is used (in certain cases) when a field is assigned to be null, but a null value is not allowed for the field.

The following example shows fields with specified default values:

```
<?xml version="1.0" encoding="UTF-8"?>

<Record name="Orders" type="delimited">

    <Field name="OrderID" type="numeric" delimiter="|" format="#" />

    <Field name="OrderDate" type="date" delimiter="|" format="dd.MM.yyyy"

default="01.01.1900" nullable="no" />

    <Field name="Amount" type="number" delimiter="\n" default="0.0"
nullable="no" />

</Record>
```

In this example, `OrderDate` is defaulted to `1.1.1900`, in case it is not present in the text data this record is parsed from. In general, when this field is assigned a null value, the specified default value is assigned instead. The same is true for the `Amount` field, except the default is specified to be `0`.

Note - This behavior is not the default and concerns only data parsers. If your code assigns a null value into a non-nullable field, a `BadDataFormatException` error will occur.

If you use any of the Clover data parsers, you can specify a `DataPolicy`, which states what should happen if a parsed value cannot be assigned to a data field (as in the case when the value is null and the field cannot accept null values).

There are three different data policies defined:

- **Strict** - Any problem causes `BadDataFormatException`. This is the default behavior.
- **Controlled** - Similar to strict, but also logs the problematic value.
- **Lenient** - If a default value exists, CloverETL attempts to assign that default value.

4

Oracle Identity Analytics Data Correlation

This chapter contains the following sections:

4.1 Overview

4.2 Understanding Data Correlation

To construct the Identity Warehouse, global users are imported into Oracle Identity Analytics. This causes the entitlements in the various resources and target systems to be imported as well. A commonly used method to import this data is to run the automated Oracle Identity Analytics import process using flat or `.csv` files.

The process of associating global users to their respective entitlements is called *data correlation*. In Oracle Identity Analytics, multiple correlation rules can be defined to accurately associate global users to their entitlements. This chapter describes these rules and provides examples that show how to correlate global users to their entitlements using a combination of correlation rules and expressions.

Additionally, Oracle Identity Analytics provides powerful manual correlation capabilities. Manual correlation enables you to manually correlate orphan accounts (accounts that do not have any associated users) as well as change the association of existing correlated accounts.

4.3 Writing Correlation Rules

Correlation rules are defined in the schema (`.rbx`) files under the Oracle Identity Analytics schema folder.

A correlation rule checks if the global user field matches an account field. The left side of the rule (before the = sign) is associated with the global user, and the right side of the rule is associated with the account. For example, `$globalUser.userName=$account.userName`.

When creating data correlation rules, remember the following:

- Only one attribute can be set at a time for global users (on the left side of the rule), but any number of expressions can be configured on the right side of the rule for accounts.
- Correlation rules, once defined, are evaluated in the same order as they are found in the schema file.
- No patterns can be applied to the global user attribute. For example `#globaluser.userName(-10)` is not allowed.
- The default correlation rule to associate users to their entitlements on the basis of their user IDs is `$globaluser.userName=$account.userName`.
- The global user attribute and the global user table column should bear the same name for the data correlation feature to function correctly. For example, `userName` is the attribute that appears in the Oracle Identity Analytics table for global users and should be named accordingly.

  See Chapter 2.2.1.3, "Global-User Schema File Reference" for details.
- When one global user accurately meets a certain rule designed for it, the correlation is established between the user and entitlements and no further expressions are evaluated for that account.
- If more than one global user meets a correlation rule for a given account, the next correlation rule is evaluated. Subsequently, both results are intersected, and, if as a result of this intersection only one global user meets both rules, that global user is correlated to the account.

For example, suppose the following rules are configured:

```
# @IdentityCorrelationRule rule="$globalUser.FirstName=$account.FirstName"

# @IdentityCorrelationRule rule="$globalUser.LastName=$account.LastName"
```

An account has the following attributes: `FirstName="John", LastName="Cook"`. When evaluating the first rule, Oracle Identity Analytics might find many global users with "John" as `FirstName`, but when it evaluates the second rule and the intersection is made, only one global user meets both rules.

4.3.1 Example

Following is an example of a schema file with multiple correlation rules:

```
#

# @iam:namespace name="Summarization" shortName="SUM"
#

# @IdentityCorrelationRule rule="$globalUser.userName=$account.userName"

# @IdentityCorrelationRule rule="$globalUser.FirstName=$account.FirstName"

# @IdentityCorrelationRule rule="$globalUser.LastName=$account.LastName"

# @IdentityCorrelationRule
rule="$globalUser.MiddleName=$account.FirstName(-1.1)$account.LastName"

# @IdentityCorrelationRule rule="$globalUser.userName=[defaultuser]"

userName,endPoint,domain,comments,suspended,locked,name,FunctionCode,FirstName,
MiddleName, LastName
```

Note: The correlation method used in previous versions of Oracle Identity Analytics using the <correlationkey> tag also works with Oracle Identity Analytics, so you do not need to change the old schema files.

4.4 Pattern Matching Scenarios

Various pattern matching scenarios can be created in order to match the users to their entitlements.

This feature is explained using an example. Assume a user has the following attributes:

```
FirstName="John"

LastName="Cook"
```

The following pattern-matching scenarios can be created:

Rule	Result	Description
$account.FirstName$account.LastName	"JohnCook"	Consolidates FirstName and LastName without any space or special characters in between
$account.FirstName(-10)	"John "	Sets the text space to 10, leaves space after the FirstName
$account.FirstName(+10)	" John"	Sets the text space to 10, leaves space before the FirstName
$account.FirstName(/_/+10)	"______John"	Sets the text space to 10 and prints an underscore before the FirstName.
$account.FirstName(/_/-10)	"John______"	Sets the text space to 10 and prints an underscore after the FirstName.
$account.FirstName(3)	"John"	Sets the minimum number of characters to 3.
$account.FirstName(+5)	" John"	Sets the text space to 5 and prints blank space before the FirstName.
$account.FirstName(+2.3)	"ohn"	Deletes all characters after the third one from right side of the FirstName.
$account.FirstName(-2.3)	"Joh"	Deletes all characters after the third one from the left side of the FirstName.
$account.FirstName(-1.1)	"J"	Deletes all characters after the first one from the left side of the FirstName.
$account.FirstName(-1.1)$account.LastName	"JCook"	Deletes all characters after the first one from the left side of the FirstName and inserts LastName.
$account.FirstName(-1.1)_$account.LastName	"J_Cook"	Deletes all characters after the first one from the left side of the FirstName and inserts an underscore and LastName.

Note:

- The – sign signifies that the text is left justified.
- The + sign signifies that the text is right justified.
- The first number inside the parentheses indicates the minimum number of characters.
- The number after the period is used to truncate the string starting from that position.

4.5 Manual Correlation

Manual correlation refers to the ability of manually correlating accounts to users. This capability proves helpful in situations where the existing correlation rules result in accounts that are not automatically associated with any user. Such accounts are called "orphan accounts." Oracle Identity Analytics provides the ability to manually correlate such accounts to specific users. Manual correlation is also useful when the ownership of an account needs to be changed.

4.5.1 To Correlate an Orphan Account to a User

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. Click the **Orphan Accounts** tab.

   The panel on the left displays all the resource types that can be expanded to show resources. Expand the list further to view the available orphan accounts.
4. Select a resource type or resource to view all the available orphan accounts.
5. Select account(s) by selecting the corresponding check box, and then click the **Assign to User** button.
6. Search and select a user from the window that opens.
7. Select the desired user from the search result and click Ok.

4.5.2 To Change Ownership of an Account

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. Click the **Accounts** tab.
4. Select the account(s) whose ownership is to be changed by selecting the corresponding check box.
5. Click the **Change Owner** tab.
6. Search and select the user to be assigned the account(s).
7. Click Ok.

5

Role Engineering and Management

This chapter describes how role mining works in Oracle Identity Analytics. It contains the following sections:

5.1 Understanding Role Mining, Role Consolidation, and Entitlements Discovery

Role Mining, Entitlements Discovery, and Role Consolidation are modules that can be used to populate the Identity Warehouse with the right combination of users and roles. The process of populating the Identity Warehouse with roles has roughly three phases: role definition, role refinement, and role verification.

During the role definition phase you should use the role mining module to populate the Identity Warehouse with roles. To refine your roles, use the Entitlements Discovery and Role Consolidation modules. Also use the Role Consolidation module to verify that your roles are clean and complete.

5.1.1 Role Mining

The role mining process discovers relationships between users based on similar access permissions that can logically be grouped to form a role. Role engineers can specify the applications and attributes that will return the best mining results. Role mining is also called *role discovery*.

Oracle Identity Analytics supports three approaches to role mining: a top-down approach, a bottom-up approach, and a hybrid approach.

In the top-down approach, Oracle Identity Analytics creates roles by analyzing users' job functions and HR attributes. (For example, geographical location and manager are typical HR attributes.) In the bottoms-up approach, Oracle Identity Analytics creates roles by analyzing users' account permissions. In the hybrid approach, the top-down approach and the bottom-up approach are combined. The hybrid approach is recommended.

5.1.2 Role Consolidation

Role Consolidation is a feature that prevents the creation of new roles with almost the same membership and entitlements of existing roles, a syndrome known as *role explosion*.

Role Consolidation tells you how similar two roles are based on the following two criteria:

- Role membership
- Entitlements

5.1.3 Entitlements Discovery

Entitlements Discovery analyzes legacy roles in order to define, re-evaluate, and refine the content of these roles. Role Entitlements Discovery can also be used for role consolidation if you need to include more applications in the role entitlement mix.

Once roles have been defined for critical applications, you might not want to add new roles or change the makeup of a role, but instead introduce a larger domain of application entitlements in those roles. In this case, select the relevant attributes of the new application as minable only and run Role Entitlements Discovery on the existing roles.

The Role Entitlements Discovery process can also be applied to top-down roles that are already defined in the organization in order to expedite the hybrid, best-practice role definition process.

5.2 Performing Role Mining

Role mining (role discovery) uses *expectation maximization* and *cobweb clustering* algorithms to discover relationships between users based on similar access permissions that can logically be grouped to form a role.

The role mining process consists of three steps:

1. Setting role mining attributes
2. Creating and running a role mining task
3. Analyzing role mining results and configuring and saving roles

5.2.1 Setting Role Mining Attributes

Before starting a role mining job, specify the applications and attributes that will return the best data mining results. To do this, set minable attribute settings. It is important to identify attributes that define access to a particular application/target system and set them as minable. Ensure that the appropriate applications and input data are accounted for. Do not add unimportant attributes because they will affect the accuracy of the role mining effort. Running role mining without any attributes set as minable will result in an error.

> **Note:** Role mining should be performed with a small number of users who best represent the data trend. Role mining too many users can lead to out-of-memory errors.

5.2.1.1 To Set Role Mining Attributes

1. Log in to Oracle Identity Analytics.

2. Choose **Administration** > **Configuration**.
3. Click **Resource Types**.

   The Resource Types configuration screen opens.
4. Select the resource type whose attributes are to be selected for role mining by clicking on the resource type in the **Resource Types** panel on the left.
5. Select attributes for mining by selecting the check box in the **Minable** column and clear attributes that are not useful.

5.2.2 Creating a Role Mining Task

The key to a good role engineering effort is to select the best set of representative users for a given role. For best results, select a group of users whose job responsibilities are the most similar. Oracle Identity Analytics then suggests roles based on the users' collective entitlements.

A good practice before running a role mining task is to preview the input data selected for the role mining exercise. Do this to ensure that all attributes are accounted for, and also that all attributes are correct. Check for any visible inconsistencies in the data.

5.2.2.1 To Create a Role Mining Task

Follow these steps to create and run a role mining task. You can also schedule the task to run at a later time, or simply save the task without running or scheduling it.

1. Log in to Oracle Identity Analytics.
2. Choose **Role Management** > **Role Mining**.
3. Click **New Role Mining Task**.
4. In the New Role Mining Task window, complete the **Name** and **Description** fields, then select a Selection Strategy for role mining:
   - **By Business Structures** - Choose this option to perform role discovery on one or more users that you select by business unit.
   - **By Resource** - Choose this option to perform role discovery on one or more resources.
   - **By Existing Role** - Choose this option to perform role discovery using existing roles.
   - **All Users** - Choose this option to base role mining on one or more users that you select from a list of all users.
5. Click **Next**.
6. Proceed as follows.

   For help using the user interface controls during this step, see Section 5.2.2.2, "Using the Role Mining Wizard Display Controls."
   - If your selection strategy is *By Business Structures*, select the business unit from the **Business Structures** panel on the left, then select users assigned to the business unit in the **Available Users** panel on the right. Selected users will display in the panel at the bottom of the screen.
   - If your selection strategy is *By Resource*, select the resource from the **Available Resource Types** panel on the left, then select individual resources in the **Available Resources** panel on the right. Selected resources will display in the **Number of Selected Resources** panel at the bottom of the screen.

- If your selection strategy is *By Existing Role*, select the role from the A**vailable Roles** panel on the left, then select users assigned to the role in the available **Users** panel on the right. Selected users will display in the panel at the bottom of the screen.
- If your selection strategy is *All Users*, search for the users using the specific criterion. Selected users will display in the panel at the bottom of the screen.

7. Click Next.
8. Complete the Mining Criteria form by selecting parameters to refine the role mining task.

   See Section 5.2.2.3, "Using the Mining Criteria Page" for help configuring the parameters on this page.
9. Click Preview to preview and analyze role mining input data.

   The Role Engineering Data Preview window opens.

   See Section 5.2.2.4, "Using the Role Engineering Data Preview Page" later in this chapter for help using this page.
10. Use the Role Engineering Data Preview window to review the columns on the Role Engineering Data Preview page.
    a. Check the minable attributes that are accounted for in this run.
    b. Verify that minable attributes are correct with respect to your set of representative users.
    c. Verify that multi-valued attributes display correctly in separate columns. If not, specify that the attribute is multi-valued on the attributes configuration screen.
11. Click **Close** to return to the Mining Criteria page.
12. Do one of the following:
    - Click **Run Now** to start the role mining task.

      See Section 5.2.3, "Running or Scheduling a Role Mining Task" later in this chapter for more information.
    - Click **Run Later** to schedule the task.
    - Click **Save & Exit** to save the task without scheduling it.

5.2.2.2 Using the Role Mining Wizard Display Controls

This section describes how to use the display controls that are part of the role mining task creation wizard. See Section 5.2.2.1, "To Create a Role Mining Task" for more information.

- Select **Page** at the top of the panel to select all the users on the page, or select **clear Page** to deselect all the users on the page.
- Select **All** to select all users across all pages, or select **clear All** to deselect all users.
- Use the **Display** drop-down menu at the bottom of the panel to change the number of records that are displayed at once. You can choose to view 10, 20, 50, or 100 records at a time.
- Click the filter icon at the bottom of the page to filter large record sets. Type a few characters in the filter boxes, and Oracle Identity Analytics will display the matching records.

5.2.2.3 Using the Mining Criteria Page

This section describes the Mining Criteria page, which is part of the role mining task creation wizard. Role mining parameters give you more control over the role mining process. The following tables describes parameters that you can set to tune the role mining process.

Table 5–1 Mining Criteria Page—Role Mining Parameters

Parameter	Description
Find Number of Roles	The number of roles that the algorithm should find.
Let the system find the best number of roles	The maximum number of clusterer iterations.

Table 5–2 Mining Criteria Page—HR Attributes

Parameter	Description
Selected HR Attributes	A list of user attributes that can be incorporated into the search algorithm. Using these parameters, along with the logical grouping of users by job responsibility, gives the best results for a hybrid role mining effort.

Table 5–3 Mining Criteria Page—Advanced Parameters

Parameter	Description
Attribute Frequency	Instructs the role mining engine to ignore attributes that have a frequency lower than the value entered. Attributes may not be relevant if they have low frequency and they may introduce "noise." Furthermore, processing them is costly and adds processing time.
Data Resampling Percentage	The best threshold value is 300%.
Min. standard deviation	Used by the role mining algorithm to size the amount of user detail to capture. Use values between `-2`, `-1`, `0`, `1`, and `2`. Larger numbers (positive or negative) return more outliers.
Single instance per user	Keep this selected to choose a single instance per user.
Use Binary splits	The goal of splitting is to get more roles with greater differences. When role mining, the ideal subset is a group of users who do not share any attributes with users in any other group or role. Enabling Binary splits forces Oracle Identity Analytics to attempt to build a role classification model with greater differences.
Confidence factor	A method to statistically analyze the users-to-role assignment data and estimate the amount of error inherent in it.
Minimum users per role	Minimum number of users per role when building the classification rules. If the clusterer step has found a role with fewer users, the classification test can show incorrect results.
Number of folds	Reduce error pruning is another mechanism to prune the tree (the classification model).
Randomize start	Randomize the seed number used to initialize the random number generator. Role mining may return slightly different roles if you select this option.
Consider subtree raising	Another mechanism to simplify the classification model (smaller number of final roles).

Table 5–3 (Continued)Mining Criteria Page—Advanced Parameters

Parameter	Description
Unpruned	Generates a more complex decision tree (later decomposed into more rules)

5.2.2.4 Using the Role Engineering Data Preview Page

This section describes how to use the Role Engineering Data Preview page, which is part of the Role Mining task creation wizard. To open this page, follow the steps in Section 5.2.2.1, "To Create a Role Mining Task."

- To view the data associated with individual resources or resource types, make a selection in the **Resource Types** panel.
- To select the data associated with the entire user set, select **Resource Types**.
- To filter users by `GlobalUserId`, use the **Filter** feature, or click **Clear** to cancel the filtering.
- To save the role mining input data as a CSV file, click **Export to CSV**.

5.2.3 Running or Scheduling a Role Mining Task

Role mining tasks can run on demand, or you can schedule them to run at a later time. Oracle Identity Analytics provides a sophisticated scheduling mechanism that is easy to use. Tasks can be run multiple times and can be executed on demand or scheduled for a future time. Task results are timestamped and stored. This enables you to run a task and then review results later in order to configure and save roles. Unless they are explicitly deleted, all role mining tasks are permanently stored by Oracle Identity Analytics.

5.2.3.1 To Run or Schedule a Saved Role Mining Task

To run or schedule a saved task, follow these steps:

1. Log in to Oracle Identity Analytics.
2. Choose **Role Management** > **Role Mining**.

   A table of **Role Mining Tasks** is displayed.
3. In the **Action** column, click **Run** to run a given task now, or click **Schedule** to open the schedule for a task.

   To schedule the task, do the following:

   a. Select a Daily, Monthly, or One Time Only recurrence schedule.

   b. For Perform This Task, specify the Start Time, whether the task should run Every Day or only on Weekdays, and a Start Date.

   c. Click Schedule to schedule the task. The role mining task is scheduled to run at the intervals you selected.

5.2.4 Validating and Saving Role Mining Results

Role mining identifies users with nearly identical access entitlements and displays the entitlements and the resources associated with the entitlements on the role configuration screen. You can assign to the role all of the entitlements or a partial list based on a level of accepted risk.

If the need is to match users with exact entitlements only, then set a cutoff percentage of 100 percent. This value will only save entitlements where 100 percent of the users in that role have the same access entitlement. Selecting a percentage below 100 percent allows Oracle Identity Analytics to save entitlements above the set cutoff as a primary policy (or parent role), and those entitlements below the set cutoff as a secondary policy (or child role). You can decide later if you want to maintain the child role policy for a transitional period of time, or remove access altogether.

5.2.4.1 To Validate and Adjust Role Discovery Results

1. Log in to Oracle Identity Analytics.
2. Choose **Role Management** > **Role Mining**.

   A table of Role Mining Tasks is displayed.
3. Find the role mining task that you want to validate.

   To find a specific role mining task, do the following:

   - Click the **Display** drop-down menu at the bottom of the panel to change the number of records that are displayed at once. You can choose to view 10, 20, 50, or 100 records at a time.
   - Click the "filter icon" at the bottom of the page to filter large record sets.
   - Type a few characters in the filter boxes and Oracle Identity Analytics will display the matching records.
4. Click **View Results** in the Action column.

   The results display in a panel at the bottom of the page.
5. In the **View Reports** column, click **View Reports** for the task instance that you are validating.

   The Role Mining Report page opens. This page displays membership and attribute details across all resources and resource types for all the roles created in the role mining effort.

   Note - To export the report to another format, click the **Actions** button.
6. Click the **Back** button.
7. In the panel at the bottom of the page, click **View** in the **View Results** column.

   The Role Mining Results page opens.

   See Section 5.2.4.2, "Using the Role Mining Results Page," for information about this page.

5.2.4.2 Using the Role Mining Results Page

This section describes the Role Mining Results page. To open this page, see Section 5.2.4.1, "To Validate and Adjust Role Discovery Results" for instructions.

The Role Mining Results page has four tabs:

- **Roles tab** - Click to view a role mining report for one or more roles, and to save roles from the mining effort.
- **Mining Statistics tab** - Click to view the statistics used to validate the result of the role mining effort.
- **Classification Rules tab** - Click to view the classification rules that were used to create the roles during the role mining process.

- **Users In Roles tab** - Click to view a pie chart that shows the percentage of users assigned to each role type as part of the role mining process.

At the bottom of the page, click **Discard** to go back to Role Mining Option Details page.

5.2.4.3 Using the Roles Tab

Use this page to save roles created by the mining effort.

The **Roles** tab contains a **Roles Found** left panel that lists created roles, and a main panel that contains two tabs: **Role Details** and **Membership**.

Role Details Window

The following explains how you can use the Role Details Window:

- Click a resource type, resource, attribute, or attribute value for more detail.

  A new window opens and shows users with and without entitlements.

  To export the report as a PDF or CSV file, click the **Actions** button. Select a role from this list to view role details. Each role in the Roles Found panel can be expanded to view resource types, resources, and attributes associated with the role. Click on a resource type, resource, or attribute within a role to view role membership details.

- The **No. of Users** column lists the number of role users that correlate to the attribute listed in the role.

- The **% of Users** column indicates the percentage of users that have access to the selected attribute.

- Slide the cutoff ruler to the desired accepted risk percentage. All attributes above the cutoff percentage will be set to a primary or parent role policy, and all those below the cutoff percentage will be set to a secondary policy for child roles.

- Select **Create Role** to save the role in the Oracle Identity Analytics Identity Warehouse.

  The role is displayed in the Identity Warehouse with the appropriate timestamp.

  Click **Identity Warehouse** > **Roles** to view the saved role. The role can be renamed and its corresponding policy viewed and modified as required.

  Note - Before changing policies (or the associated access attributes), consult with the business owner or role owner.

- Select the role and click **View Reports** to view a role mining report for one or more roles. The role mining report details the attributes and values associated with the role across all resources and resource types.

Membership Window

The Membership Window displays the members of the selected roles.

5.2.4.4 Using the Mining Statistics Tab

Use this page to determine how well the Role Mining algorithm performed.

The **Mining Statistics** tab reports the following statistics that you can use to interpret role mining results:

Field	Description
% of users correctly / incorrectly assigned	This mining statistic tells what percentage of users has been assigned correctly and what percentage has not.
Kappa value	A statistical measure of the degree of agreement for a particular physical finding. In the case of Oracle Identity Analytics, the physical finding is the roles discovered through the role mining process. Kappa is always less than or equal to 1. A value of 1 represents perfect agreement, so the higher the Kappa value, the stronger the agreement. Depending on the application, a Kappa value of less than 0.7 indicates that your system needs improvement. Kappa values greater than 0.9 are considered excellent.
Kononenko & Bratko score and relative score	A score of the data mining algorithm. This value can be disregarded.

5.2.4.5 Using the Classification Rules Tab

Use this page to view the classification rules that were used to create the roles during the role mining process.

Field	Description
Rule #	This column lists the rules in ascending order.
Description	This column contains descriptions of the corresponding rules.
Confidence (%)	This column lists confidence scores as a percentage.
Role	This column lists roles.
Record Count	This column lists record count.

5.2.4.6 Using the Users in Roles Tab

This page displays a pie chart that shows the percentage of users assigned to each role type as part of the role mining process. Use this page to enhance your understanding of the role mining effort.

5.3 Performing Role Consolidation

Role Consolidation is a feature that prevents the creation of new roles with almost the same membership and entitlements of existing roles, a syndrome known as *role explosion*.

Role Consolidation tells you how similar two roles are based on the following two criteria:

- Role membership
- Entitlements

5.3.1 To Consolidate Roles

1. Log in to Oracle Identity Analytics.

2. Choose **Role Management** > **Role Consolidation**.

   The Role Consolidation page opens.

3. Choose one of the following:

   - **Choose consolidation based on Role Membership** - Checks for similarity of two roles based on users.
   - **Choose consolidation based on Entitlements** - Checks for similarity of two roles based on entitlements.

4. Select the two roles that you want to compare.
5. Use the "cut-off" slider at the bottom of the page to set a percentage, below which roles that have a low similarity score will not appear in the results.
6. Click **Submit**.

The Role Consolidation Results Table appears.

5.4 Performing Entitlements Discovery

This module analyzes legacy roles in order to define, re-evaluate, and refine the content of these roles. Entitlements Discovery can also be used for role consolidation if you need to include more applications in the role entitlement mix.

Once roles have been defined for critical applications, you might not want to add new roles or change the makeup of a role, but instead introduce a larger domain of application entitlements in those roles. In this case, select the relevant attributes of the new application as minable only and run Entitlements Discovery on the existing roles.

The Role Entitlements Discovery process can also be applied to top-down roles that are already defined in the organization in order to expedite the hybrid, best-practice role definition process.

5.4.1 To Perform Entitlements Discovery

1. Log in to Oracle Identity Analytics.
2. Choose **Role Management** > **Entitlements Discovery**.

   The Choose Attribute Type Strategy page opens.

3. Select **Evaluate Minable attributes** and click **Next**.
4. Select the desired role from the **Available Roles** panel on the left.

   The **Available Users** panel on the right displays the users that belong to that role.

5. Select one or more users.
6. Do one of the following:

   - Click the **Display** drop-down menu at the bottom of the panel to view more users on the page.
   - Select **Page** at the top of the panel to select all the users on the current page, or select **clear Page** to deselect the users on the current page.
   - Select **All** to select all users across all pages, or **clear All** to deselect all users.

7. Click **Next**.
8. On the left side of the screen, select a Role and click **View Details**.

9. Select a cut-off percentage for each policy and click **Save Policies**. The cut-off slider at the bottom of the page can be set to a percentage so that only the users that have an equal or higher similarity-percentage will appear in the result.

10. Choose **Identity Warehouse** > **Policies** to view the time-stamped policies.

    The access (attributes) related to these policies can be evaluated and added or removed as required. Policies, once renamed and finalized, can be re-associated to the original role.

Note - Before changing policies (or the associated access attributes), consult with the business owner or role owner.

5.5 Creating and Using Role Provisioning Rules

Organizations are in a constant state of flux. Any change in an employee's responsibility also means assigning or revoking user access. To meet this challenge, Oracle Identity Analytics enables you to create role provisioning rules.

Role provisioning rules automatically assign roles to a user, if the user meets the rule condition. The condition can include HR attributes or entitlement-related information.

5.5.1 To Create New Rules

1. Log in to Oracle Identity Analytics.

2. Choose **Role Management** > **Rules**.

3. Click **New Rule**, complete the form, and click **Next**.

4. Create the condition for the rule and click **Next**.

   a. Select the Object (four options are provided: **User**, **Role**, **Business Unit**, and **Resource Types**), an attribute, a condition, and a value.

   b. Select **AND** or **OR** from the menu in the **Operation** column to add additional conditions.

   c. Select two or more rules and use the **Group** and **Ungroup** buttons to create complex conditions.

5. Click **Select Role**, choose a role from the roles listed, and click **Next**.

   If the user meets the condition, the user is assigned the chosen role.

6. Click **Add Owners**, select the user who should own this role, and click **Next**.

   Use the quick or advanced search options, as needed.

7. Select from the following options:

   - **No Changes** - If any change occurs to the attributes or its values, this option does not make any change.
   - **Remove Role Immediately** - If any change occurs to the attributes or its values, this option removes the role immediately.
   - **Remove Role after *n* days** - If any change occurs to the attributes or its values, this option removes the role after the selected number of days.
   - **Notify Administrator** - If any change occurs to the attributes or its values, this option sends an e-mail based on the e-mail template to the concerned actor.

8. Click **Finish**.

The role provisioning rule is created and the rule state is marked as composing.

9. To send the rule for approval, select the rule and click **Send for Approval**.

   The status of the rule is changed to Pending Approval.

Note - The current status of a newly created role provisioning rule is *composing* or *pending approval* until the rule is approved by the rule owner or the administrator. Thereafter, the rule becomes active. Action can only be taken on active rules.

5.5.2 To Approve/Reject Role Provisioning Rules

1. Log in to Oracle Identity Analytics.
2. Choose **My Requests** > **Pending Requests**.

   This page displays the pending role provisioning rule request.
3. Do one of the following:
   - To approve the rule, select the rule and click the **Approve** button.
   - To reject the rule, select the rule and click the **Reject** button.

     The rule is displayed in the Completed Requests page. If approved, the rule's status (under the Role Management tab) is changed to active.

Note - Only approved roles become active.

5.5.3 To Deactivate or Decommission Rules

Before You Begin - Note the following:

- *Decommissioning* a rule makes the rule invalid permanently. It cannot be made active again, but it remains in the software to enable better rule lifecycle management.
- *De-activating* a rule makes the rule invalid temporarily. It can be made active again by changing the state of the rule.

1. Log in to Oracle Identity Analytics.
2. Choose **Role Management** > **Rules**.
3. Click a rule to edit it.

   The Edit Rule page opens.
4. Select a new status from the **New Status** drop-down menu.
5. Click Save.

After you save your changes, a new version of the rule is created. To make the changes effective, the new version needs to be approved. See Section 5.5.2, "To Approve/Reject Role Provisioning Rules" for information.

5.5.4 To Preview Role Provisioning Rules Job

You can preview the results of a role-provisioning rules job. You can preview the results of rules in the composing state, however the results cannot be saved until the rule is active.

1. Log in to Oracle Identity Analytics.
2. Choose **Role Management** > **Rules**.

3. Click **Preview** in the **Actions** column.
4. Click the **Selection Strategy** drop-down menu and choose from the following:
   - **All Business Structures** - Selects users from all business structures.
   - **Selected Business Structures** - Selects the users from the selected business structures.
   - **All Users** - Selects all users in Oracle Identity Analytics.
   - **Users criteria** - Selects users based on the condition you create. Click Preview to get an idea of the users selected.
   - **Selected Users** - Selects users which you choose individually.
5. Click **Next**. Based on the user selection strategy in Step 4, select the desired business structures or users and click **Next**.

   A summary page opens.
6. Click **Preview**.

   A Role Provisioning Jobs page opens and displays the status of the preview action.
7. Select the rule after the status is 100 percent complete. The preview results appear.
8. Select one of the following:
   - **Apply** - Saves the results of the action.
   - **Don't Apply** - Does not save the results of the action.

5.5.5 To Run Role Provisioning Rules Job

Role provisioning rules can be run only if the rule is in the active state. See Section 5.5.2, "To Approve/Reject Role Provisioning Rules" to change the rule state to active.

1. Log in to Oracle Identity Analytics.
2. Choose **Role Management** > **Rules**.
3. Select **Run** next to the rule that you want to run.
4. Click the **Selection Strategy** drop-down menu and choose from the following:
   - **All Business Structures** - Selects users from all business structures.
   - **Selected Business Structures** - Selects the users from the selected business structures.
   - **All Users** - Selects all users in Oracle Identity Analytics.
   - **Users criteria** - Selects users based on the condition you create.

     Click **Preview** to get an idea of the users selected.
   - **Selected Users** - Selects users which you choose individually.
5. Click **Next**.

   Based on the user selection strategy in Step 4, select the desired business structures or users and click **Next**.

   A summary page opens.
6. To run now, click **Run Now** and click View Results.

   To run the job later, click **Run Later** and do the following:

a. Complete the form, including name, description, and time and day for the task to start.

   A summary page opens.

b. Click Schedule.

Note - To run multiple rules simultaneously, select the desired rule and click **Run**.

5.5.6 To Manage Lifecycle of Rules

In Oracle Identity Analytics, rules play a pivotal part in role management. Therefore, every action taken on any role provisioning rule is saved in the software and can be referred to at any given point.

1. Log in to Oracle Identity Analytics
2. Choose **Role Management** > **Rules**.

   All the rules and their states are displayed.
3. Select the desired rule.

   The Edit Role Provisioning Rule page appears.

   - **General tab** - Displays information such as Rule Name, Description, Role (assigned to the rule), Current Status, New Status, Creation, and Update dates.
   - **Conditions tab** - Displays the condition associated with the rule.
   - **Ownership tab** - Displays the rule owner.
   - **Versions tab** - Displays all the previous versions of the rule. Any change, which occurs in the rule condition, rule owner, or status, is recoded in Rule Versions.
   - **History tab** - Displays the history of various changes made to the rule. All changes are recorded except rule condition, rule owner, or status changes.
   - **Action tab** - Displays the Unassign Rule Option.
4. Select the desired tab to make the required change in the rule.
5. Click Save.

6

Oracle Identity Analytics Workflows

This chapter contains the following sections:

6.1 Overview

A workflow is a specific sequence of actions or tasks that are related to a business process. In Oracle Identity Analytics, workflows enumerate each step involved in the various processes, such as role and policy creation, role and policy modification, and so on. It lists all the actors, who play a pivotal role in the management of roles and policies, and their function.

Oracle Identity Analytics has a robust and an easy-to-configure workflow engine. Workflows can be configured to any environment as they are based on the Open Source Open Symphony Workflow engine. Each workflow can be customized to support diverse requirements, such as role approval paths, policy approval paths, email integration, exposed web services to communicate with third-party applications, and so on.

6.2 Understanding Workflows

This section introduces workflows.

6.2.1 To View a Workflow

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

   Eight workflows are listed.
4. Click the desired workflow to view the steps that make up that workflow.

   To understand the Edit Workflow page, see Section 6.2.3, "Understanding the Edit Workflow Page."

6.2.2 Types of Workflows in Oracle Identity Analytics

The following table describes the eight workflows that are included with Oracle Identity Analytics.

Table 6–1 Types of Workflows in Oracle Identity Analytics

Workflow	Description
Role Creation	Runs when a role is created.
Role Modification	Runs when a role is modified. For example, when a policy is added.
Role Membership	Runs when users are added or removed from the role.
Mass Modification	Runs when many roles are created or modified.
Policy Creation	Runs when a policy is created.
Policy Modification	Runs when a policy is modified.
Role Membership Rule Creation	Runs when role provisioning rule is created.
Role Membership Rule Modification	Runs when a role provisioning rule is modified.

6.2.3 Understanding the Edit Workflow Page

The Edit Workflow page displays the name, description, and various steps involved in the completion of the task in Oracle Identity Analytics. A diagrammatic representation of the workflow is displayed on the right side of the page.

1. **Name** - Displays the name of the workflow.
2. **Description** - Displays the workflow description.
3. **Steps** - Displays a table explaining each step.

   See the following table for information.

Table 6–2 Understanding the Steps Table

Column Name	Description
Step Name	Lists all the steps involved in the workflow.
Link Status	The status displayed to the user (in the UI).
Actions	Displays all the actions that can be taken in each step and the respective consequences.
Assignee Type	Displays the type of actor that is assigned to complete this step. The assignee types are usually one of the following: ■ **Policy_owner** - The designated policy owner. ■ **Role_owner** - The designated role owner. ■ **Global_user** - Any user who is assigned to complete the step. ■ **Rule_owner** - The designated rule owner. ■ **Role** - All users who are part of the selected role.
Assignee	Displays the employee ID of the actor assigned to complete this step.
Operation	Gives you the option of adding a step, deleting a step, or adding an action.

6.3 Designing Workflows

In Oracle Identity Analytics, each workflow has pre-configured default steps to complete the tasks listed in the table.

You can customize the workflows, however, based on the requirements of your organization.

You can make the following changes to a workflow:

- Add a step.
- Delete a step.
- Edit Workflow Action Details.

6.3.1 To Add a Step in a Workflow

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Configuration**.
3. Click **Workflows**.
4. Select the desired workflow.

   The Edit Workflow page opens.
5. Click **Add Step** in the **Operations** column.
6. Select the desired template for the new step you want to add.
   - **Approval Step -** This is a template where you can choose the assignee for the step. Options available are policy owner, role owner, global user or role (any member of the role).
   - **Policy Owner Approval -** This is a pre-configured template where the policy owner is the assignee for the step.
7. Complete the form.
   - **Step Name** - Enter the name of the step that you want to add.
   - **Link Status** - Select a link status.

     The user will see this status when the workflow begins.
   - **Destination Step** - Select the next step.
   - **Assignee** - Select the assignee, or the actor, who will take action.
   - **Enable Due Date Options** - Check the box if you want to enable due date options.
   - **Stop Expires After** - Enter the number of days after which the step can expire.
   - **Enable Reminder Option** - Check the box if you want to set reminder options.
   - **Send First Reminder** - Enter the number of days for the first reminder.
   - **Reminder Frequency** - Set the reminder frequency to once, daily, or weekly.
   - **Choose Template** - Click Choose Template and select the e-mail template to use for reminders.
   - **Enable Escalation Option** - Select to enable escalation options. This will send an escalation trigger to the assignee's manager if the step has not been completed within the deadline.

- **Escalation Trigger After** - Enter the number of reminders after which the escalation trigger will be sent.
- **Choose Template** - Click **Choose Template** to select the e-mail template to use for escalation triggers.

8. Click Save.

6.3.2 To Delete a Step

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

   The Edit Workflow page opens.
5. Select the step that you want to delete by clicking **Delete Step** in the **Operations** column.

   A window opens confirming the action.
6. Click **Yes**.

   The step is deleted.

6.3.3 To Edit Workflow Action Details

You can edit the hyperlinked steps in the **Actions** column.

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Configuration**.
3. Click **Workflows**.
4. Select the desired workflow.

   The Edit Workflow page opens.
5. In the **Actions** column, click the hyperlinked step that you want to edit.
6. Complete the form.

General Tab

- **Name** - Type the name of the action involved in the workflow. For example, Approve Role, Reject Role, and so on.
- **Destination Step** - Select the next step.

Assignee Tab

- **Assignee** - Select the actor involved from the drop-down menu.
- **Selected Assignee** - If the Assignee is `global_user`, use the search feature to select the global user that you want to assign.

Pre-Functions Tab

- **Add Pre-functions** - Pre-function is an action that will be triggered when the workflow reaches this step.

  To add a pre-function, do the following:

1. Click the **Add Pre-Functions** button.
2. Select a pre-function from the list.
3. Complete the form as needed.
4. Click Save.

- **Delete Pre-functions** - Deletes the selected pre-functions.

  To delete a pre-function, do the following:

  1. Select the pre-function by selecting the check box.
  2. Click **Delete Pre-functions**.

Post-Functions Tab

- **Add Post-functions** - A post-function is an action that will be triggered when the workflow completes.

  1. Click the **Add Post-functions** button.
  2. Select a post-function from the list.
  3. Complete the form as needed.
  4. Click Save.

- **Delete Post-function** - Deletes the selected post-functions.

  To delete a post-function, do the following:

  1. Select the post-function by selecting the check box.
  2. Click **Delete Post-functions**.

7
Oracle Identity Analytics Identity Certifications

This chapter contains the following sections:

- Section 7.1, "Overview"
- Section 7.2, "Creating New Certifications"
- Section 7.3, "Scheduling Certifications"
- Section 7.4, "Understanding Closed-Loop Remediation and Remediation Tracking"

7.1 Overview

This chapter discusses identity certification tasks that need to be completed by an Oracle Identity Analytics business administrator. Identity certification information for business users, including information about how to complete identity certifications, is included in the *User's Guide for Oracle Identity Analytics* chapter.

See the *User's Guide for Oracle Identity Analytics* to learn more about the following identity certification topics:

- Identity certification overview
- Understanding the identity certification user interface
- Finding and reassigning certifications
- Completing certifications
- Getting more information about user accounts, roles, attributes, and policies
- Viewing certification reports

For information about configuring identity certifications, see the following topics:

- Section 11.2.1, "Identity Certification Configuration"
- "Configuring Identity Certification Batch Sizes in the UI" in the "Customizing the Oracle Identity Analytics User Interface" chapter in the *System Integrator's Guide for Oracle Identity Analytics*

For information about how Risk Summaries are calculated, as well as information about running the Risk Aggregation job, see the following topic:

- Section 1.4, "Understanding How Risk Summaries are Calculated"

7.2 Creating New Certifications

Four types of certifications can be created in Oracle Identity Analytics. Each type of certification addresses a particular use-case—a specific type of review that enterprises commonly perform. Each type of actor reviews a different subset of access-related data from a specific point of view.

Table 7–1 The Four Identity Certification Types in Oracle Identity Analytics

Identity Certification Type	Description
User Entitlement Certification	Allows managers to certify employee access to roles, accounts, and entitlements. This is the most common and most sweeping type of certification. Typically, each manager in an organization reviews the access-privileges of the people who report directly to that manager. Each reviewer in a certification of this type is focused on his or her direct-reports, but is expected to review all of the access-privileges for each of those people.
Role Entitlement Certification	Allows role owners to certify role content and role members. This certification is used in organizations that have implemented role-based access control (RBAC). Typically, the owner of a role is the person responsible for reviewing its definition (that is, the set of access-privileges that it conveys) as well as its membership (the set of users to whom the role has been assigned). Each reviewer in a certification of this type is focused on a particular enterprise role.
Resource Entitlement Certification	This certification allows the person who is responsible for a particular system or application to review the set of users who have accounts on that system or application. The reviewer can drill down and view the details of the access-privileges of each account. Each reviewer in a certification of this type is focused on one specific system or application.
Data Owner Certification	Allows data owners to certify user accounts that have a particular privilege. This certification is used if a specific person is responsible for a particular entitlement (that is, an Attribute Value or a group membership that confers a specific access-privilege). The data owner can review the set of user accounts that have that particular entitlement. Each reviewer in a certification of this type is focused on one specific privilege within one specific resource.

7.2.1 To Create a User Entitlement Certification

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Certifications** > **My Certifications**.
3. Click **New Certification**.

   The Create Certification window opens.
4. Complete the form as follows, then click Next:
   - **Certification Name** - Type a name for the certification.
   - **Type** - Select **User Entitlement** from the drop-down menu.

- **Incremental** - This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

  See Section 7.2.5, "Understanding the Incremental Certification Option" for more information.

5. Select a user-selection strategy from the drop-down menu, then click Next:

   - **All business structures** - Selects all business structures created in Oracle Identity Analytics.
   - **Selected business structures** - Allows you to manually select specific business structures. Click Next.

   > **Note:** When completing a certification, the Business Structure name or any other details about the Business Structure will be shown only if both the following conditions are met:
   >
   > - The user-selection strategy for the certification is by business structures.
   > - The certifier is the Business Structure Manager.

   - **All users** - Selects all the users in the system.
   - **Users criteria** - Selects all the users that meet the given search condition. For help with search, see "Searching for a User" in the "Identity Warehouse" section of the *User's Guide for Oracle Identity Analytics*. You can preview the results of this selection.
   - **Selected users** - Allows you to select specific users from a list of users in the system. Click Next.

6. Complete the Period and Certifier form as follows, then click Next:

   - **Certifier** - You can select **Business Structure Manager**, **User Manager**, or search for an authorized user to specify as the certifier.
   - **Start Date** - Enter the start date. The certification is valid as of the start date.
   - **End Date** - Enter the end date. The certification expires after the end date. Managers cannot review certifications after the expiration date.
   - **Configuration Details** - Select the check box to change the configuration of the certification you are creating. For detailed instructions on customizing configuration settings, see Section 11.2.1, "Identity Certification Configuration." After clicking Next, the summary page opens.

     Click **Back** if you want to modify any selection.

7. Select one of the following options:

   - To Run Certification immediately, select **Run**.
   - To schedule a certification job, select **Later**.

     Refer to Section 7.3, "Scheduling Certifications" for instructions.

8. Click **Create**.

7.2.2 To Create a Role Entitlement Certification

1. Log in to Oracle Identity Analytics.

2. Choose **Identity Certifications** > **My Certifications**.

3. Click **New Certification**.

   The Create Certification window opens.

4. Complete the form as follows, then click Next:

   - **Certification Name** - Type a name for the certification.
   - **Type** - Select **Role Entitlement** from the drop-down menu.
   - **Incremental** - This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the role content, which has been certified.

     See Section 7.2.5, "Understanding the Incremental Certification Option" for more information.

5. Select a role selection strategy from the drop-down menu, then click Next:

   - **All business structures** - Selects all business structures created in Oracle Identity Analytics.
   - **Selected business structures** - Allows you to manually select the business structures.

     Note: When completing a certification, the Business Structure name or any other details about the Business Structure will be shown only if both the following conditions are met:

     - The user-selection strategy for the certification is by business structures.
     - The certifier is the Business Structure Manager.

   - **All roles** - Selects all of the roles in the system.
   - **Roles criteria** - Selects all of the roles that meet the given search condition. You can preview the results of this selection.
   - **Selected roles** - Allows you to manually select the roles in the system.

6. Complete the Period and Certifier form as follows, then click Next:

   - **Certifier** - You can select **Business Structure Manager**, **Role Owner**, or search for an authorized user to specify as the certifier.
   - **Start Date** - Enter the start date. The certification is valid as of the start date.
   - **End Date** - Enter the end date. The certification expires after the end date. Managers cannot review certifications after the expiration date.
   - **Configuration Details** - Select the check box to change the configuration of the certification you are creating. For detailed instructions on customizing configuration settings, see Section 11.2.1, "Identity Certification Configuration."

     After clicking Next, the summary page opens.

     Click **Back** if you want to modify any selection.

7. Select one of the following options:
   - To Run Certification immediately, select **Run**.
   - To schedule a certification job, select **Later**.

     Refer to Section 7.3, "Scheduling Certifications" for instructions.
8. Click **Create**.

7.2.3 To Create a Resource Entitlement Certification

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Certifications** > **My Certifications**.
3. Click **New Certification**.

   The Create Certification window opens.
4. Complete the form as follows, then click Next:
   - **Certification Name** - Type a name for the certification.
   - **Type** - Select **Resource Entitlement** from the drop-down menu.
   - **Incremental** - This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

     See Section 7.2.5, "Understanding the Incremental Certification Option" for more information.
5. Select a user selection strategy from the drop-down menu, then click Next:
   - **All business structures** - Selects all business structures created in Oracle Identity Analytics.
   - **Selected business structures** - Allows you to manually select the business structures.

     > **Note:** When completing a certification, the Business Structure name or any other details about the Business Structure will be shown only if both the following conditions are met:
     >
     > - The user-selection strategy for the certification is by business structures.
     > - The certifier is the Business Structure Manager.

   - **All users** - Selects all the users in the system.
   - **Users criteria** - Selects all the users that meet the given search condition. For help with search, see "Searching for a User" in the "Identity Warehouse" section of the *User's Guide for Oracle Identity Analytics*. You can preview the results of this selection.
   - **Selected users** - Allows you to select specific users from a list of users in the system.
6. Click **Add Resource**.

   The Select Resource(s) window opens.
7. Select the desired resource and click OK.

8. Click Next.
9. Complete the Period and Certifier form as follows, then click Next:
   - **Certifier** - Select **Business Structure Manager, User Manager**, or search for an authorized user to specify as the certifier.
   - **Start Date** - Enter the start date. The certification is valid as of the start date.
   - **End Date** - Enter the end date. The certification expires after the end date. Managers cannot review certifications after the expiration date.
   - **Configuration Details** - Select the check box to change the configuration of the certification you are creating. For detailed instructions on customizing configuration settings, see Section 11.2.1, "Identity Certification Configuration." After clicking Next, the summary page opens. Click Back if you want to modify any selection.
10. Select one of the following options:
    - To Run Certification immediately, select **Run**.
    - To schedule a certification job, select **Later**.

      Refer to Section 7.3, "Scheduling Certifications" for instructions.
11. Click Create.

7.2.4 To Create a Data Owner Certification

> **Note:** 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. Log in to Oracle Identity Analytics.
2. Choose **Identity Certifications** > **My Certifications**.
3. Click **New Certification**.

   The Create Certification window opens.
4. Complete the form as follows, then click Next:
   - **Certification Name** - Type a name for the certification.
   - **Type** - Select **Data Owner** from the drop-down menu.
   - **Incremental** - This setting enables certifiers to certify or revoke only changes or inclusions made to a certification. It eliminates the need to review the access of users who have been certified.

     See Section 7.2.5, "Understanding the Incremental Certification Option" for more information.
5. Select a selection strategy from the drop-down menu, then click Next:

- **By Data Owner** - Creates a certification for the attribute values for which the selected user is designated as the data owner.

  Click **Add Data Owner**, select the user, and click OK. For help using search, see the *User's Guide for Oracle Identity Analytics*, "Identity Warehouse" chapter, "Working With Users," "Searching for a User."

- **By Attribute** - Creates a certification for data owners of the selected attribute values.

  Click the **Add Attributes** button. The Attribute Selection table appears.

  Select the resource type, resource, and attributes, and click OK.

6. Click Next.
7. Complete the Period and Certifier form as follows, then click Next:
   - **Certifier** - Select the data owner or an authorized user as the certifier.
   - **Start Date** - Enter the start date. The certification is valid as of the start date.
   - **End Date** - Enter the end date. The certification expires after the end date. Managers cannot review certifications after the expiration date.
   - **Configuration Details** - Select the check box to change the configuration of the certification you are creating. For detailed instructions on customizing configuration settings, see Section 11.2.1, "Identity Certification Configuration." After clicking Next, the summary page opens. Click **Back** if you want to modify any selection.
8. Select one of the following options:
   - To Run Certification immediately, select **Run**.
   - To schedule a certification job, select **Later**.

     Refer to Section 7.3, "Scheduling Certifications" for instructions.
9. Click Create.

7.2.5 Understanding the Incremental Certification Option

Incremental certification is a setting that allows managers to certify only those changes that are new since the last certification was created. This option is available if the certifier and certification type have not changed since the last certification. Enabling this setting saves time during the certification process.

The following options are available when the incremental certification option is selected:

- **Since Last Base -** Specifies that Oracle Identity Analytics treat the previous non-incremental certification as the base. Managers then review user access and either certify or revoke those changes that have taken place after the base. Events that are considered to be changes include the addition of new users, new accounts, or new roles. For example, a certification in Q1 has two users. In Q2 a third user is added and the certifier must certify the access of the new user as part of an incremental certification. In Q3 a fourth user is added and another account access is given to the third user. The Q3 certification displays only the fourth user and the third user's new access.
- **Since Date -** Specifies that Oracle Identity Analytics return only those certification changes made after the date provided. Access certifications that were certified before the given date have to be re-certified. For example, in January a certification

is created with two users. In March, a third user is added and a certification is completed. In August, a fourth user is added. If you create an August certification and choose February 2nd as your base, the certification will return the user added in August, as well as any users certified before February 2nd (that is, the two users in January).

- **Show Previous Values -** Specifies that Oracle Identity Analytics return the previous certified values during the certification process. A certifier can change these values, if required.

> **Note:** Incremental certification requires that the certifier and certification type remain the same. Also, incremental certification is valid only for completed certifications. Incremental certification does not apply for expired or incomplete certifications.

7.3 Scheduling Certifications

Certifications are scheduled as part of the new certification creation process. For more information, see Section 7.2, "Creating New Certifications." Certifications can be scheduled to run once, or to repeat on a daily, weekly, or monthly basis.

7.3.1 To Schedule a Certification

Before You Begin - You need to create a new certification before you can schedule it. See Section 7.2, "Creating New Certifications."

1. Complete the Certification Job form as follows:
   - **Certification Job Name** - Type the name of the job.
   - **Certification Job Description** - Type a description.
   - Select Daily, Weekly, Monthly, or One-time-only based on how often certifications should be run.
   - **Scheduled Dates** - Select the time and day for the task to start.
2. Click Create.

The certification job is displayed in the **Identity Certification** > **Certification Jobs** section.

7.3.2 To Delete a Certification Job

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Certifications** > **Certification Jobs**.

   The Certification Jobs page opens.
3. Find the certification job that you want to delete, and click **Delete** in the **Actions** column.

   A window confirming the action opens.
4. Click **Yes**.

7.4 Understanding Closed-Loop Remediation and Remediation Tracking

Closed-loop remediation is a feature that allows you to directly revoke roles and entitlements from the provisioning solution as a result of roles and entitlements revoked during the certification process. This feature is applicable only if the provisioning solution is either Oracle Identity Manager or Oracle Waveset (Sun Identity Manager).

For non-managed applications, however, you can manually revoke roles and entitlements by using the information stored in the remediation configuration module.

The remediation status can be tracked in the remediation tracking module for auditing purposes.

7.4.1 Configuring Closed-Loop Remediation

Configuring closed-loop remediation is a two-step process:

1. Selecting the provisioning mode used for the resource
2. Selecting the remediation kick-off date

7.4.1.1 To Select Provisioning Mode

To define the remediation process, first select the provisioning mode used for the resource. If auto mode is selected, choose the appropriate provisioning connection. If manual mode is selected, you must describe the steps required to de-provision an account belonging to the resource.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Resources**.
3. Select the desired resource, and click the **Remediation** subtab.
4. Check the box adjacent to **Select Provisioning Mode**.
   - **Auto -** This mode sends an SPML call to the provisioning server to revoke the account. The account is subsequently revoked in Oracle Identity Analytics after the next updated feed is imported. Select the Connection.

     > **Note:** Closed-loop remediation is supported with either Oracle Identity Manager or Oracle Waveset (Sun Identity Manager). It is not supported with other provisioning servers.

   - **Manual -** This mode prompts you to write the steps to manually de-provision the account. Example: Self-service URL, de-provisioning instructions, and so on.
5. Click Save.

7.4.1.2 To Select Remediation Start Date

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Configuration**.
3. Click **Identity Certification**.
4. Click to expand the **Revoke and Remediation** section.
5. Scroll down to the **Remediation** section.

- **Display Remediation Instructions** - Select to display remediation instructions to the user manager during the certification process.

6. **Perform Closed-loop remediation on** - Select to be able to enable one of the following two options:

   - **Certification End Date** - This will start the remediation on the date the certification ends. Even if the certifier has completed the certification before the end (expiration date), remediation will not take place until the end date is reached.
   - **Include Expired Certifications** - If **Certification End Date** is enabled, select this option to start remediation for revoked accounts of incomplete certifications.
   - **Certification Completion Date** - This will start remediation on the date that the certifier completes the certification.

7. Click Save.

7.4.2 To Track Remediation

Oracle Identity Analytics enables tracking of remediation activities for audit purposes. In the Remediation Tracking view, a revoked account can exist in two states:

- Required: Means that the remediation is not complete.
- Complete: Means that the revoked account, access within an account, or role has been successfully removed.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Certification** > **Remediation Tracking**.

   The **Status** column displays the remediation tracking information.

3. Click the certification name to see details.

   The remediation tracking details page is divided into two sections:

   a. Remediation Details

      – **Overview** - Information about the certification, number of roles, and accounts revoked and remediated.

      – **History** - Information about the creation and end of the certification, name of the creator, and so on.

      – **Export Options** - Option to export the report to a PDF or XLS file.

   b. Section for each user whose account or role has been remediated.

      – **Employee Information** - Displays the employee's name, job title, phone number, employee ID, and e-mail details.

      – **Roles or Entitlements** - Displays the details of the revoked accounts, roles, and the remediation status against each revocation.

8 Oracle Identity Analytics Identity Audit

This chapter contains the following sections:

- Section 8.1, "Overview"
- Section 8.2, "Working With Audit Rules"
- Section 8.3, "Working With Audit Policies"

8.1 Overview

This chapter documents identity audit functionality that is available to business administrators, but not to general business users. Identity audit information for general business users is documented in the "Identity Audit" chapter in the *User's Guide for Oracle Identity Analytics*.

See the *User's Guide for Oracle Identity Analytics* to learn more about the following identity audit topics:

- Identity audit overview
- Understanding the identity audit user interface
- Acting on audit policy violations

For information about configuring the identity audit module, including preventing self-remediation, see the following topic:

- Section 11.2.3, "Identity Audit Configuration"

8.2 Working With Audit Rules

An identity audit rule has a rule condition. If, during an audit policy scan, the rule condition evaluates to true, the rule is triggered.

You can define complex rules with nested conditions on the basis of user information, resource types attributes, role metadata, classification, and business structure metadata.

An audit rule can be assigned one of three states: active, inactive, and decommissioned. Only active rules associated with an identity audit policy can be scanned.

8.2.1 Impact of Rule Condition Modifications

When a rule condition is modified, all policies associated with this rule are impacted. If the modified rule is the cause of any existing open violations in the system, the cause and the associated violation will be impacted by the change in condition.

When users associated with an impacted violation are scanned against the policies associated with the modified rule, the system takes the following actions on the violation:

1. The system checks to see whether the modified condition still causes an exception.
2. If the rule condition still results in an exception, then the system sets the violation cause status to "Active." Otherwise, the system sets it to "Inactive."

8.2.2 Impact of Adding / Removing Rules in a Policy

An administrator may remove one or more rules from a policy only if all violations associated with that policy are in the "Closed" state. So if you intend to remove rules, you must change all unresolved (Open, Closed as Fixed, Closed as Risk Accepted) violations to the "Closed" state.

An administrator may add new rules to an existing policy. However, this change can impact some existing unresolved violations. The next time the modified policy is scanned, existing open violations that are impacted by this change are updated and new ones are created if the new rules have caused exceptions.

8.2.3 To Create Audit Rules

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Audit** > **Rules**.
3. Click **New Rule**.

   The New Rule form wizard opens.
4. Enter a name and description for the rule, and select whether the rule should be Active or Inactive.
5. Create one or more conditions for the rule.

   Select the Object (either User, Role, Business Unit, or Resource Types objects are provided), the corresponding attribute, the rule condition, and enter the value. You can use operators such as **AND** and **OR** to add more conditions.

   Use the **Group** and **Ungroup** buttons to create complex conditions.
6. Click Save.

   The rule is created and is displayed on the Rule page.

8.2.4 To Edit / Change the State of an Audit Rule

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Audit** > **Rules**.

   All the rules that have been created are displayed.
3. Click the rule that you want to edit or to make active/inactive.

   The Edit Rule page opens.
4. Edit the fields as required.

5. Change the state to Active, Inactive, or Decommissioned as required.

> **Note:** A decommissioned rule is made permanently inactive and cannot be activated again. All information about the rule, however, is retained in Oracle Identity Analytics.

6. Click Save.

8.3 Working With Audit Policies

An identity audit policy is a collection of audit rules that together enforce SoD business policies. Audit policies consist of metadata, such as the audit policy name, description, severity, creation date, and update data. Audit policies have designated policy owners and policy remediators.

An identity audit policy owner is responsible for the definition of the policy and approves any changes made to the policy. However, it is the remediator's responsibility to take action on an audit policy violation and fix the violation.

8.3.1 To Create Audit Policies

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Audit** > **Policies**.
3. Click **New Policy**.
4. Enter the following details:
   - **Name** - Name of the policy.
   - **Description** - A short description of the policy.
   - **Severity**- Select from High, Medium, or Low. This information is displayed in the Identity Audit dashboard.
   - **Status**- Select from Active or Inactive.
   - **Owner** - Name of the owner of the policy. Use the Search option provided to search for the owner. For help using search, see the "Searching For a User" section in the "Identity Warehouse" chapter of the *User's Guide for Oracle Identity Analytics*.
5. Complete the **Remediator** section of the form to choose the user who will act as the remediator for any policy violations:
   - **Primary** - The primary remediator, who takes precedence over the **Default** remediator.
   - **Default** - Name of a remediator. Use the search option provided to search for the remediator.
6. Click Next.
7. Click the **Add Rules** button.

   The Add Rules to Policy page opens.
8. Select the rules that you want to assign to the policy, or click the **New Rule** button in the top-left corner to create a new rule for the policy. Multiple rules can be assigned to the policy.

9. Click **OK** to close the Add Rules to Policy page.
10. Click Finish.

    The new policy is created and appears on the Policy page.

8.3.2 To Edit / Change the State of an Audit Policy

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Audit** > **Policies**.

   All the policies that have been created are displayed.
3. Click the policy that you want to edit or to make active/inactive.

   The Edit Policy page opens.
4. Edit the fields, as required.
5. Change the state to Active, Inactive, or Decommissioned, as required.

   > **Note:** A decommissioned policy is made permanently inactive. This policy cannot be activated again. However, all information about the policy is retained in Oracle Identity Analytics.
6. Click Save.

8.3.3 To Preview Audit Policy Scan Results

Previewing a policy displays the policy scan results without saving them.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Audit** > **Policies**.

   A list of policies is displayed.
3. Find the policy that you want to preview and click **Preview**.
4. When the User Selection Strategy page opens, select one of the following:
   - **All Business Structures -** Shows results only on all the business structures in Oracle Identity Analytics.
   - **Selected Business Structures -** Shows results on the business structures you select.
   - **All Users -** Shows results on all users in Oracle Identity Analytics.
   - **Users Criteria -** Shows results on the condition, which applies to users, you create.

     Click **Preview** to get an idea of the set of users selected.
   - **Selected Users -** Shows results on the users you select individually.
5. When a Summary page is displayed, click **Preview**.

   The View Results page opens showing the status.
6. Click the Policy to view the Scan Job> Policy Violation Preview.
7. Do one of the following:
   - To save the results, click **Apply**.

- To delete the results, click **Don't Apply**.

After an audit policy scan runs, the results are saved to the system. To view the results of the policy scan, click **View Results**.

Note - The identity audit preview scan results are available only for a day after the scan is complete. Therefore, it is recommended to apply the result or discard them as soon as the scan is complete.

8.3.4 To Run An Audit Policy

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Audit** > **Policies**.

   A list of policies is displayed.
3. Find the audit policy scan that you want to run and click **Run**. You can select multiple policies as well.

   The User Selection Strategy page opens.
4. Select from the following options:
   - **All Business Structures** - Shows results based on the business structures in Oracle Identity Analytics.
   - **Selected Business Structures** - Shows results based only on the business structures you select.
   - **All Users** - Shows results based on all users in Oracle Identity Analytics.
   - **Users Criteria** - Shows results based on a condition that applies to users you create. Click **Preview** to get an idea of the set of users selected.
   - **Selected Users** - Shows results based only on the users you select.
5. Click **Next**.

   The Summary Page opens.
6. Do one of the following:
   - To run a policy immediately, click **Run Now**.

     A **Policies Are Saved for Scan** message appears after Oracle Identity Analytics has finished scanning the policy against the chosen criteria.
     - To view the policy scan results, click **View Results**.

       The **Status** column displays the number of violations.
     - Click Close.
   - To run a policy at a later time or date, click **Run Later**.

     The Schedule Job page opens.
     - Enter a task name and description, and select the time and day for the task to start.
     - Click **Next**.

       The Summary page opens.
     - Click **Schedule**.

       The scan job is scheduled for the desired day and time.

9 Oracle Identity Analytics Reports

This chapter contains the following sections:

9.1 Overview

This chapter documents reports and reporting features that are available to business administrators, but not to general business users. Reports information for general business users is documented in the *User's Guide for Oracle Identity Analytics* "Reports" chapter.

See the *User's Guide for Oracle Identity Analytics* to learn more about the following Reports topics:

- Understanding the reports user interface
- Working with reports: How to schedule and sign off on reports
- Defining and generating business structure reports
- Defining and generating system reports
- Defining and generating identity audit reports

> **Note:** Business structure reports, system reports, and identity audit reports are standard reports that are included with Oracle Identity Analytics.

9.2 Working With Custom Reports

You can run custom reports in Oracle Identity Analytics to suit the requirements of your organization.

Complete the following steps to create and run custom reports:

1. Create a reports template using JasperReports.

   JasperReports is an open source Java reporting tool that can write to screen, to a printer, or to various file formats, including PDF, HTML, Microsoft Excel, RTF, ODT, comma-separated value (CSV), and XML. It reads its instructions from an XML or `.jasper` file.

2. Use the Oracle Identity Analytics user interface to upload the reports template to Oracle Identity Analytics.

3. Run or schedule the report as needed.

9.2.1 To Upload a Custom Report Template in Oracle Identity Analytics

1. Log in to Oracle Identity Analytics.
2. Choose **Reports** > **Custom Reports**.
3. Click **New Custom Report**.

   The New Custom Report window opens.
4. Complete the form as follows:
   - **Report Name** - Type a name for the report.
   - **Sub Report** - If you require sub-reports, select this check box. Selecting this option will display additional fields that you can use to specify subreport templates to be uploaded.

     > **Note:** To establish a relationship between a master report and one or more subreports, the master report must reference the subreport(s) by file name. For example:
     >
     > ```
     > <subreportExpression class="java.io.File"><![CDATA[new
     > File($P{REPORT_LOCATION},"/mainReport_subreport1.jasper")]]></subre
     > portExpression>
     > ```
     >
     > Subreport file names should end with a `.jasper` suffix.
     >
     > For more information about configuring subreports, refer to the JasperReports documentation.

   - **Prompts** - Oracle Identity Analytics has four prompts: Business Structure, Users, Date Range, Roles, and Custom Properties.

     Custom reports can be run on any or all of the prompts that you select. Custom Properties will display five prompts where you can enter relevant values to run the report.
   - **File Uploads** - Click **Browse** to upload the XML or `.jasper` report template file. (Report templates were discussed in Section 9.2, "Working With Custom Reports.")
5. Click Save.

9.2.2 To Run a Custom Report

1. Log in to Oracle Identity Analytics.
2. Choose **Reports** > **Ad Hoc Reports**.
3. Click **Custom Reports**.
4. Click the Report that you want to view and click **Run**.
5. Select the business structure, users, date range, or roles depending on the prompt.
6. Click the **Actions** drop-down menu for options to export the file in other formats. Formats offered include PDF, XLS, CSV, HTML, XML, and Print.
7. (Optional) To download the report, click **Download** in either the **Download PDF Report** column or the **Download CSV Report** column.

10

Oracle Identity Analytics Scheduling

This chapter contains the following sections:

- Section 10.1, "Scheduling Import and Export Jobs in Oracle Identity Analytics"
- Section 10.2, "Scheduling a Job by Editing the Configuration Files"
- Section 10.3, "Scheduling Other Job Types"

10.1 Scheduling Import and Export Jobs in Oracle Identity Analytics

Oracle Identity Analytics provides a scheduler that enables you to set a specific time for imports and exports. You can schedule import and export jobs using the scheduler in the user interface (the UI-based scheduler), or you can schedule jobs by hand-editing configuration files.

Note: Before you can import data into Oracle Identity Analytics, you need to configure a provisioning server. For more information, see Section 11.1.4, "Provisioning Servers Configuration."

This section discusses how to schedule an import and export job using the user interface. For instructions on how to schedule an import and export job by editing the configuration files, see Section 10.2, "Scheduling a Job by Editing the Configuration Files."

Note: You cannot export roles, policies, or other account-related data to a file.

You can export roles from Oracle Identity Analytics to either Oracle Waveset or Oracle Identity Manager. For more information see the following chapters in the *System Integrator's Guide for Oracle Identity Analytics*:

- Integrating With Oracle Waveset (Sun Identity Manager)
- Integrating With Oracle Identity Manager, Deprecated Method

10.1.1 To Schedule an Import and Export Job Using the User Interface

Note: When scheduling a *one-time-only* job, the job runs at the scheduled date and time in your local time zone (that is, the *client computer* time zone).

When scheduling a *recurring* job, the job will run at the scheduled time in the time zone configured on the server (that is, the *server computer* time zone).

1. Log in to Oracle Identity Analytics as an administrator.
2. Choose **Administration** > **Configuration**.
3. Click **Import/Export**.
4. Click **Schedule Job**.
5. Click a job type (for example, Import Users) to select it.

   The Data Selection Source page opens.
6. Select a data selection source from the list of provisioning servers.

   It is important to select the correct server type from the drop-down menu.

   Oracle Identity Analytics does not support flat-file data exports.

   For flat-file data imports, choose the File Server option. The File Server option is a standard option that you can use to import data from a CSV or XML file.
7. Type a name and description for the job.
8. Select **Run Now** to run the job immediately, or clear this option and enter the required job scheduling information.
9. Click Finish to create the job.

Note - Each resource type has at least one resource. Therefore, it is important to select the correct resource if performing an entitlement import or export.

You do not need to specify resource type or resource information for certain kinds of imports and exports. Specifically, role imports and exports as well as users imports and exports do not require this information.

10.2 Scheduling a Job by Editing the Configuration Files

You can schedule jobs, including import and export jobs, by hand-editing configuration files and restarting the application server.

Two configuration files control the scheduler. These two files are located in the `$RBACX_HOME/WEB-INF` folder:

- `scheduling-context.xml` - Edit this file to enable (or disable) scheduled tasks, such as users import, accounts import, and others.
- `jobs.xml` - Edit the cron expressions in this file to define a schedule for each job.

Note: The contents of these files vary by application server.

To schedule a job, you must edit both `scheduling-context.xml` and `jobs.xml` and restart the application server.

The following table lists the types of jobs that can be enabled and scheduled by editing the configuration files. For each job that you are enabling or disabling, both the job name and the trigger name appear in both `scheduling-context.xml` and `jobs.xml`. If you are enabling a job, verify that both job references and both trigger references contain correct information and are not commented out. See Section 10.2.1, "To Enable a Job by Editing the Configuration Files" for more information.

Table 10–1 Jobs That can be Scheduled by Editing the Configuration Files

Job Name	Trigger Name	Description	Dependency	Input
usersImportJob	usersImportTrigger	Imports users.	Business Structure Import.	${Drop file location}/schema/filename + ${Drop file location}/in/filename +
accountsImportJob	accountsImportTrigger	Imports accounts.	Users Import.	${Drop file location}/schema/filename + ${Drop file location}/in/filename +
rolesImportJob	rolesImportTrigger	Imports roles.	Policy Import.	${Drop file location}/schema/filename + ${Drop file location}/in/filename +
glossaryImportJob	glossaryImportTrigger	Imports glossary definitions.	Policy Import.	${Drop file location}/schema/filename + ${Drop file location}/in/filename +
policiesImportJob	policiesImportTrigger	Imports policies.	Accounts Import.	${Drop file location}/schema/filename + ${Drop file location}/in/filename +
businessStructureImportJob	businessStructureImportTrigger	Imports business structure definitions.	Resources import Job.	${Drop file location}/schema/filename + ${Drop file location}/in/filename +
identityAuditContinuousViolationScanJob	identityAuditContinuousViolationScanTrigger	Scans for continuous identity audit violations	No dependency.	Database for auto scan.

Table 10–1 (Continued)Jobs That can be Scheduled by Editing the Configuration Files

Job Name	Trigger Name	Description	Dependency	Input
identityAuditViolationReminderJob	identityAuditViolationReminderTrigger	Sends out an identity violation reminder when an e-mail template is configured.	No dependency.	Reminder email template notification for audit.
certificationReminderJob	certificationReminderTrigger	Sends out a certification reminder when an e-mail template is configured.	No dependency.	Reminder e-mail templates notification for certification.
reportReminderJob	reportReminderTrigger	Sends out a report reminder when an email template is configured.	No dependency.	Reminder e-mail template notification for reports.
stableFolderCleanUpJob	stableFolderCleanUpTrigger	Cleans the stable folder.	No dependency.	$(Drop file location)/in/.stable
accountsMaintenanceJob	accountsMaintenanceTrigger	Maintenance of accounts.	Accounts Import.	Accounts in the database based on the settings from iam.properties. Cleaning up internal tables in the database.
roleMembershipRuleJob	roleMembershipRuleTrigger	Triggers the role membership rule.	Roles Import.	Database for rules of roles.
fullTextIndexMaintenancedJob	fullTextIndexMaintenancedTrigger	Maintenance of full text index.	No dependency.	Database.
workflowStepSLAJob	workflowStepSLATrigger	Triggers workflow steps.	No dependency.	Database. N/A
roleStatusAndMembershipMaintenanceJob	roleStatusAndMembershipMaintenanceTrigger	Maintenance of role status and membership.	Role membership rule job.	Database for start or end date of users.
rmPreviewCleanUpJob	rmPreviewCleanUpTrigger	Cleans preview.	No dependency.	Database cleanup.
userApplicationMaintenanceJob	userApplicationMaintenanceTrigger	Maintenance of user application.	No dependency.	Database for Applications scan.
postImportJobsLauncherJob	postImportJobsLauncherTrigger	Triggers post import jobs.	Users Import and Accounts Import.	N/A
certificationRemediationJob	certificationRemediationTrigger	Triggers certification remediation.	No dependency.	Database for remediation update.
rmScanArchivalJob	rmScanArchivalTrigger	Triggers scan archival.	No dependency.	Database cleanup.

Table 10–1 (Continued)Jobs That can be Scheduled by Editing the Configuration Files

Job Name	Trigger Name	Description	Dependency	Input
eventPublishingJob	eventPublishingTrigger	Triggers event publishing.	No dependency.	Database for Event Listener.
rmeRuleMigrationJob	rmeRuleMigrationTrigger	Triggers rule migration.	No dependency.	Database for migration from an earlier release to PS1.

10.2.1 To Enable a Job by Editing the Configuration Files

The following procedure describes how to enable a job. This example demonstrates how to enable the users import job and the accounts import jobs. The same procedure, however, can be used to enable other kinds of jobs, as well.

1. Navigate to `$RBACX_HOME/WEB-INF/`.
2. Open `scheduling-context.xml` in a text editor.
3. Edit the required lines as follows to enable import:
   - To enable users import, uncomment `usersImportJob` in the `jobDetails` property section, and uncomment `usersImportTrigger` in the triggers property section.
     - The uncommented `usersImportJob` line should look like this:

       ```
       <ref bean="usersImportJob"/>
       ```
     - The uncommented usersImportTrigger line should look like this:

       ```
       <ref bean="usersImportTrigger"/>
       ```
   - To enable accounts import, uncomment `accountsImportJob` in the `jobDetails` property section, and uncomment `accountsImportTrigger` in the `triggers` property section.
     - The uncommented `accountsImportJob` line should look like this:

       ```
       <ref bean="accountsImportJob"/>
       ```
     - The uncommented `accountsImportTrigger` line should look like this:

       ```
       <ref bean="accountsImportTrigger"/>
       ```
4. Save your changes.
5. Schedule the job by editing `jobs.xml` in a text editor.

   See Section 10.2.2, "To Schedule a Job by Editing the Configuration Files" for more information.

The portion of `scheduling-context.xml` that contains the lines that you need to edit follows:

```
<property name="jobDetails">
<list>
<!-- Uncomment the line before to use this account import job.
Multiple jobs can be added,
1. Define a job in jobs.xml
2. Add a reference to job below -->
<!--ref bean="usersImportJob"/-->
<!--ref bean="accountsImportJob"/-->
<!--ref bean="rolesImportJob"/-->
```

```
<!--ref bean="glossaryImportJob"/-->
<!--ref bean="policiesImportJob"/-->
<!--ref bean="certificationReminderJob"/-->
<!--ref bean="reportReminderJob"/-->
<!--ref bean="stableFolderCleanUpJob"/-->
<!--ref bean="accountsMaintenanceJob"/-->
<!--ref bean="roleMembershipRuleJob"/-->
<ref bean="fullTextIndexMaintenancedJob"/>
<ref bean="workflowStepSLAJob"/>
<ref bean="roleMembershipJob"/>
</list>
</property>

<property name="triggers">
<list>
<!-- Uncomment the line before to use this account import job.
Multiple triggers can be added,
1. Define a trigger in jobs.xml
2. Add a reference below -->
<!--ref bean="usersImportTrigger"/-->
<!--ref bean="accountsImportTrigger"/-->
<!--ref bean="accountsImportTrigger_2"/--> <!-- Additional triggers for account 
imports
                                                to be used in clusters -->
<!--ref bean="accountsImportTrigger_3"/--> <!-- Additional triggers for account 
imports
                                                to be used in clusters -->
<!--ref bean="rolesImportTrigger"/-->
<!--ref bean="glossaryImportTrigger"/-->
<!--ref bean="policiesImportTrigger"/-->
<!--ref bean="certificationReminderTrigger"/-->
<!--ref bean="reportReminderTrigger"/-->
<!--ref bean="stableFolderCleanUpTrigger"/-->
<!--ref bean="accountsMaintenanceTrigger"/-->
<!--ref bean="roleMembershipRuleTrigger"/-->
<ref bean="fullTextIndexMaintenanceTrigger"/>
<ref bean="workflowStepSLATrigger"/>
<ref bean="roleMembershipJobTrigger"/>
</list>
</property>
```

10.2.2 To Schedule a Job by Editing the Configuration Files

The following procedure describes how to schedule a job by editing `jobs.xml` in a text editor. This example demonstrates how to schedule the users import jobs and the accounts import jobs. The same procedure, however, can be used to schedule other kinds of jobs, as well.

Before You Begin - Before a job can run, you need to enable it. See Section 10.2.1, "To Enable a Job by Editing the Configuration Files" for instructions.

1. Navigate to `$RBACX_HOME/WEB-INF/`.
2. Open `jobs.xml` in a text editor.
3. To schedule a users import job, follow these steps:
   a. Uncomment `usersImportTrigger` and `usersImportJob` (if necessary).
   b. In `usersImportTrigger`, edit the cron expression to schedule the job.

      See Section 10.2.3, "Sample Cron Expressions" for more information.

4. To schedule an accounts import job, follow these steps:

   a. Uncomment accountsImportTrigger and accountsImportJob (if necessary).

   b. In accountsImportTrigger, edit the cron expression to schedule the job. See Section 10.2.3, "Sample Cron Expressions" for more information.

5. Save your changes.

6. Restart the application server to have your changes take effect.

> **Note:** If running Oracle Identity Analytics in a clustered environment, you need to define additional triggers for each server in the cluster that you want to run the job at the same time. Refer to the example in the jobs.xml file for more information.

The portion of jobs.xml that contains the usersImportJob and usersImportTrigger sections that you need to edit follows:

```
<bean id="usersImportTrigger"
class="org.springframework.scheduling.quartz.CronTriggerBean">
        <property name="jobDetail">
            <ref bean="usersImportJob"/>
        </property>
        <property name="cronExpression">
            <value>0 0/5 * * * ?</value>
        </property>
    </bean>

    <bean id="usersImportJob"
class="org.springframework.scheduling.quartz.JobDetailBean">
        <property name="name">
            <value>Users Import</value>
        </property>
        <property name="description">
            <value>Users import Job</value>
        </property>
        <property name="jobClass">

<value>com.vaau.rbacx.scheduling.manager.providers.quartz.jobs.IAMJob</value>
        </property>
        <property name="group">
            <value>SYSTEM</value>
        </property>
        <property name="durability">
            <value>true</value>
        </property>
        <property name="jobDataAsMap">
            <map>
                <!-- only single user name can be specified for  jobOwnerName
(optional)-->
                <entry key="jobOwnerName">
                    <value>REPLACE_ME</value>
                </entry>
                <!-- multiple user names can be specified as
                     comma delimited e.g user1,user2 (optional)-->
                <entry key="usersToNotify">
                    <value>REPLACE_ME</value>
                </entry>
                <entry key="IAMActionName">
                    <value>ACTION_IMPORT_USERS</value>
                </entry>
                <entry key="IAMServerName">
                    <value>FILE_SERVER</value>
                </entry>
                <!-- Job chaining, i.e. specify the next job to run (optional) -->
                <entry key="NEXT_JOB">
                    <value>rolesImportJob</value>
                </entry>
            </map>
        </property>
    </bean>
```

10.2.3 Sample Cron Expressions

The schedule for each job is specified using a cron expression. A cron expression is a string comprised of six or seven fields separated by white space that specify the time and day (or *time and date*) for every job. Each job has a cron expression, which is defined within the `<property name="cronExpression">` element in `jobs.xml`.

The following operators can be used in cron expressions:

- The comma operator (',') specifies a list of values, for example: `1,2,3,5,7`.
- The dash operator ('-') specifies a range of values, for example: `1-5`, which is equivalent to `1,2,3,4,5`.
- The asterisk operator ('*') specifies all possible values for a field. For example, an asterisk in the day-of-month field is equivalent to every day (unless other fields further modify the expression).
- The slash operator ('/') can be used to skip a given number of values. For example `0/5` in the minute field is equivalent to every five minutes.
- The question mark operator ('?') is allowed for the day-of-month and day-of-week fields. It is used to specify 'no specific value'. This is useful when you need to specify something in one of the two fields, but not the other.

The fields that make up a cron expression are listed here:

```
.------------------- second (0 - 59)
 |  .---------------- minute (0 - 59)
 |  |  .------------- hour (0 - 23)
 |  |  |  .---------- day of month (1 - 31)
 |  |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
 |  |  |  |  |  .---- day of week (1 - 7) (Sunday=1)  OR
 |  |  |  |  |  |     sun,mon,tue,wed,thu,fri,sat
 *  *  *  *  *  *
```

Following are a few sample cron expressions.

Table 10–2 Sample Cron Expressions

Cron Expression	Definition
`0 0 12 * * ?`	Fire at 12pm (noon) every day
`0 15 10 ? *`	Fire at 10:15am every day
`0 15 10 * * ?`	Fire at 10:15am every day
`0 15 10 * * ? *`	Fire at 10:15am every day

Table 10–2 (Continued)Sample Cron Expressions

Cron Expression	Definition
`0 15 10 * * ? 2007`	Fire at 10:15am every day during the year 2007
`0 * 14 * * ?`	Fire every minute starting at 2pm and ending at 2:59pm, every day
`0 0/5 14 * * ?`	Fire every 5 minutes starting at 2pm and ending at 2:55pm, every day
`0 0/5 14,18 * * ?`	Fire every 5 minutes starting at 2pm and ending at 2:55pm, AND fire every 5 minutes starting at 6pm and ending at 6:55pm, every day
`0 0-5 14 * * ?`	Fire every minute starting at 2pm and ending at 2:05pm, every day
`0 10,44 14 ? 3 WED`	Fire at 2:10pm and at 2:44pm every Wednesday in the month of March
`0 15 10 ? * MON-FRI`	Fire at 10:15am every Monday, Tuesday, Wednesday, Thursday and Friday
`0 15 10 15 * ?`	Fire at 10:15am on the 15th day of every month
`0 15 10 L * ?`	Fire at 10:15am on the last day of every month
`0 15 10 ? * 6L`	Fire at 10:15am on the last Friday of every month
`0 15 10 ? * 6L 2002-2005`	Fire at 10:15am on every last Friday of every month during the years 2002, 2003, 2004 and 2005
`0 15 10 ? * 6#3`	Fire at 10:15am on the third Friday of every month
`0 0/30 8-9 5,20 * ?`	Fires every half hour between the hours of 8:00am and 10:00am on the 5th and 20th of every month. Note that the trigger will NOT fire at 10:00 am, just at 8:00, 8:30, 9:00 and 9:30.
`10 0/5 * * * ?`	Fire every 5 minutes and 10 seconds
`0 0/5 * * * ?`	Fire every 5 minutes

10.3 Scheduling Other Job Types

This section lists other kinds of jobs that can be scheduled in Oracle Identity Analytics.

- **Reports** - For information about how to schedule reports, see "To Schedule Reports" in the "Reports" chapter of the *User's Guide for Oracle Identity Analytics*.
- **Email reminders** - For information about how to schedule reminder e-mails to be sent to data owners reminding them to review and sign-off on reports, see Section 11.2.4, "Reports Configuration."
- **Certifications** - For information about how to schedule certifications, see Section 7.3.1, "To Schedule a Certification" in the Oracle Identity Analytics Identity Certifications chapter.
- **Role mining tasks** - For information about how to schedule role mining tasks, see Section 5.2.3, "Running or Scheduling a Role Mining Task."
- **Risk aggregation** - For information about how to schedule risk aggregation, see Section 1.4.4.2, "To Control How Often the Risk Aggregation Job Runs."

11

Oracle Identity Analytics Configuration and Settings

This chapter has two parts: The first section documents the configuration pages that are available from the menu bar under **Administration** > **Configuration**, and the second section documents the pages that are available under **Administration** > **Settings**.

Configuration Pages Help Topics

- Section 11.1.1, "System Configuration"
- Section 11.1.2, "Risk Mapping"
- Section 11.1.3, "Resource Types Configuration"
- Section 11.1.4, "Provisioning Servers Configuration"
- Section 11.1.5, "E-mail Templates Configuration (Configuring E-mail Notification)"
- Section 11.1.6, "Import/Export"
- Section 11.1.7, "Workflows Configuration"
- Section 11.1.8, "Event Listeners Configuration"

Settings Pages Help Topics

- Section 11.2.1, "Identity Certification Configuration"
- Section 11.2.2, "Role Management Configuration"
- Section 11.2.3, "Identity Audit Configuration"
- Section 11.2.4, "Reports Configuration"
- Section 11.2.5, "Identity Warehouse Configuration"

11.1 Configuration Pages

This section documents the configuration pages that are available when you choose **Administration** > **Configuration** from the menu bar.

11.1.1 System Configuration

This section describes how to configure settings for the Proxy Assignment Notifications, Mail Server Settings, and OIA Server Settings options.

11.1.1.1 Proxy Assignment Notification

This option enables e-mail notifications to be sent to the users who have been set as proxies using the **My Settings** > **New Proxy Assignment** tab. An e-mail template can be selected for the proxy user.

11.1.1.2 Mail Server Settings

This option helps in setting up the mail server.

Email Encoding	`UTF-8`
SMTP Server Name	`mail.example.com`
SMTP Port	`25`
SMTP Authentication	Select if required

11.1.1.3 OIA Server Settings

This option helps in setting up the Oracle Identity Analytics server.

System Email	`rbacx@example.com`
OIA URL	`http://localhost:8282/rbacx`

11.1.2 Risk Mapping

For a discussion of Risk Mapping, see Section 1.4, "Understanding How Risk Summaries are Calculated."

11.1.2.1 External Provisioning (Provisioning Scenarios)

Use this screen to assign risk levels to roles and entitlements that are assigned to users outside of Oracle Identity Analytics.

Note - To use this feature, Oracle Identity Analytics must be configured to capture "provisioned-by" information for entitlements. This information needs to originate from an authoritative source, such as Oracle Identity Manager. "Provisioned-by" information cannot currently be captured in file-based imports.

Enable Provisioning Method Risks

Select to assign a *high*, *medium*, or *low* default risk level for each provisioning scenario listed on the page.

- **Reconciliation from target system** - Applies to user access that was created outside of OIA when an identity and access management (IAM) system reconciled its identities with those of the target system.
- **Direct provisioning by administrator** - Applies to user access that was manually assigned to the user outside of OIA by an administrator in an identity and access management system.
- **Access request** - Applies to access that was assigned as the result of an access request.
- **Provisioned by access policy** - Applies to user access that was assigned by an access policy that is defined outside of OIA.

- **Rule-based role-assignment** - Applies to user access that was assigned due to a rule assigning a role to a user based on one or more properties that triggered the rule.

11.1.2.2 System Defaults

Use this screen to assign risk levels to roles and entitlements that are assigned to users from within Oracle Identity Analytics.

WARNING: Do not make frequent changes to risk level mappings.

Changing risk level mappings can cause a huge ripple effect in the Identity Warehouse. Each change to a risk-level mapping affects every account or account-attribute value, every user-role assignment, and every user in the system.

For more information, see Section 1.4.3, "Understanding How Changing Risk Configuration Values Impacts the System."

Assignment Scenarios

Assign *high*, *medium*, or *low* risk levels to the following provisioning actions applied from within OIA:

- **Rule-based role assignment** - Applies to user access that was assigned because of a rule in OIA.
- **Role mining role assignment** - Applies to user access that was assigned during the OIA role mining process. The role mining process discovers relationships between users based on similar access permissions that can logically be grouped to form a role.
- **Approval request** - Applies to an access request that was assigned after an OIA approval process was completed.
- **Import process** - Applies to user access that was created during the role import process, during which roles from one or more external systems are imported into OIA.
- **Unknown action** - Applies to user access that was assigned, but details about the assignment are not available in OIA.

Warehouse Settings

Assign *high*, *medium*, or *low* Item-Risk levels to OIA data warehouse items. If you do not directly assign an Item-Risk level to a metadata object in the Identity Warehouse, the system references the following settings to assign a default Item-Risk level for you.

- **Roles** - Select the risk level that should be applied to Roles that otherwise do not have an assigned Item-Risk level.

  Roles represent unique job functions performed by users. Roles contain Policies that describe the access that individuals have on a directory.

- **Resources** - Select the risk level that should be applied to Resources that otherwise do not have an assigned Item-Risk level.

  Resources are the applications and enterprise information assets that users need to do their jobs.

- **Entitlements** - Select the risk level that should be applied to Entitlements that otherwise do not have an assigned Item-Risk level.

Note: If you change the Entitlements setting, the system assigns the new risk level to all Resource-Attribute Values that (1) were imported into the Identity Warehouse by way of an Account import, and (2) do not have a directly-assigned Item-Risk level. Resource-Attribute Values that were imported by way of a Glossary import, however, are not assigned a new risk level when the Entitlements risk-mapping setting is changed

Each Entitlement is a specific *value* of a specific resource-attribute. A particular resource-attribute may have many values, each of which could be defined as an entitlement that confers a specific access-privilege.

Last Certification Action

Assign *high*, *medium*, or *low* risk levels to the last action performed against a certification entry, as follows:

- **Certified** - Applies to a certification item that was approved during the previous certification.
- **Revoked** - Applies to a certification item that was revoked during the previous certification.
- **Abstain** - Applies to a certification item whereby during the previous certification the certifier indicated that they are not responsible for reviewing or certifying the item.
- **Certify Conditionally** - Applies to a certification item that was temporarily certified during the previous certification, even though the certification may not be valid. Certifiers who select this action are required to enter an end date. The system does not revoke the access or send out notices regarding expired end dates
- **Unknown Action** - Applies to a certification item that has not been acted on yet. This occurs in systems when a certification is run for the first time so there is not a base value to refer to.

Audit Violations

Assign *high*, *medium*, or *low* risk levels to items associated with an audit trail, as follows:

- **Open audit violations** - Applies to items that are associated with an unresolved audit violation.
- **No audit violations** - Applies to items that are not associated with an audit violation.
- **Closed as risk-accepted** - Applies to items that were flagged during an Identity Audit, but were closed as risk-accepted.

11.1.3 Resource Types Configuration

In Oracle Identity Analytics, a *resource* is an application or some other enterprise information asset that users need to do their jobs, whereas a *resource type* is a grouping of like resources. A resource type defines meta-data common to all resources of that type. For example, a resource type of "Oracle DBMS" might define entitlements (that is, attribute-values of Oracle database accounts) that are common to all database instances. Each resource of that type represents a specific database instance to which a user might have access.

Systems such as UNIX®, Windows, Oracle DBMS, and so on are commonly defined as resource types, whereas individual servers or databases are examples of resources.

Administrators need to create and define resource types in Oracle Identity Analytics. Oracle Identity Analytics makes it possible to create detailed descriptions of the hierarchy levels and user entitlements associated with resource types. The Oracle Identity Analytics metadata module enables the user to define resource types, list the entitlements for each resource type, and define the various levels of hierarchy associated with each entitlement.

To define metadata in Oracle Identity Analytics, choose **Administration** > **Configuration** > **Resource Types** in the user interface.

11.1.3.1 To Create or Delete a Resource Type

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

   To create, rename, or delete a resource type, do one of the following:

- To *create* a new resource type, do this:
   a. Click **New Resource Type**.
   b. Complete the form and click Save.

      For **Short Name**, type a three-letter abbreviation.
- To *delete* a resource type, do this:
   a. Click the resource type to be deleted.
   b. Click **Delete**.

      A dialog box confirming the action appears.

11.1.3.2 Understanding Resource Type Attributes and Attribute Categories

Resource type metadata is defined in Oracle Identity Analytics using the following hierarchy:

Resource Type > Attribute Categories > Attributes

Attributes are entitlements that map to different objects in a resource type. For example, *database name* is an attribute of MySQL™, *UID* is a UNIX attribute, and so on. A collection of similar types of attributes makes up an *attribute category*. Attributes and attribute categories are uniquely defined for each resource type.

11.1.3.3 To Create, Rename, and Delete an Attribute Category

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

   To create, rename, or delete an attribute category, do one of the following:

- To *create* an attribute category for a given resource type, do this:
   a. Click the resource type and click **New Attribute Category**.

b. Complete the form as follows:

   - **Attribute Category Name** - Type the name of the attribute category.
   - **Category Order** - Type a number to specify where the tab for this attribute category should appear relative to the other tabs in the tab sequence on the Accounts and Policies pages. For example, type 1 to have the tab appear in the first position.
   - **Link Attributes** option and **Parent** menu - The Link Attributes option should only be selected when Oracle Identity Analytics is integrated with Oracle Identity Manager. In the **Parent** menu select the field that is defined as the `OIAParentAttribute` in Oracle Identity Manager. This property is needed so that OIA can exchange data with OIM.

     For more information, see "Integrating With Oracle Identity Manager, Preferred Method" in the *System Integrator's Guide for Oracle Identity Analytics*.

Oracle Identity Analytics creates the new attribute category.

- To *rename* an attribute category, do this:

  a. Click the attribute category and click **Rename**.

  b. Type the new name and click Save.

- To *delete* an attribute category, do this:

  a. Click the attribute category.

  b. Click **Delete**.

  A dialog box confirms the deletion.

11.1.3.4 Configuring Resource Type Attributes

Oracle Identity Analytics provides a detailed properties page to define an attribute. The following parameters are used to define an attribute.

Table 11–1 Attribute Parameters

Name	Attribute Description
Description	Description of the attribute
Min Length	The minimum length that can be specified for an attribute
Max Length	The maximum length that can be specified for an attribute
Case	Specifies whether the attribute value can be uppercase or lowercase
Edit Type	Specifies the data type of the attribute
Order	Specifies the order in which the attribute is listed or imported
Min Value	The minimum value that the attribute can have
Default Value	The default value an attribute should have when it is imported
Values	A predefined list of values that the attribute can have
Excluded Value	A value that an attribute cannot have when it is imported
Label	The display label for the attribute
Classifications	Free-form labels or tags that should be associated with the attribute. For example, *Invoicing*, *Purchasing*, *Accounting*.

In addition, the following flags further define an attribute:

Table 11–2 Additional Attribute Flags

Flag	Flag Description
Space Allowed	Allows the attribute values to have a space in them
Hidden	The attribute value can be hidden (for password fields)
Managed	To display an attribute or import it, the managed flag needs to be set for the attribute
Importable	Allows the attribute to be imported from a CSV / Text File
Certifiable	Specifies that the attribute can be certified, for example in a Data Owner certification.
Multiple Value	Allows an attribute to have comma-separated multiple values
Mandatory	This flag, when selected, specifies all the privileges for the attribute such as managed, importable, and so on.
Auditable	Allows the attribute to be checked for audit exceptions
Minable	Allows Oracle Identity Analytics to perform role engineering operations

11.1.3.5 To Create, Rename, Edit, and Delete an Attribute

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

- To create an attribute, do this:
  a. Highlight the Attribute Category under which you want to create an Attribute and click the **New Attribute** tab.

     A dialog box appears.

  b. Enter the **New Attribute** values.
- To *rename* an attribute, do this:
  a. Click **Rename** for the appropriate attribute.

     A dialog box appears.

  b. Enter the new name and save it.
- To *edit* an attribute, do this:
  a. Click **Modify** for the appropriate attribute.

  b. Modify the required values.
- To *delete* an attribute, do this:
  a. Click **Delete** for the appropriate attribute.

     A dialog box confirming the action appears.

11.1.4 Provisioning Servers Configuration

A Provisioning Server is a server or system that administers user accounts on target resources. Oracle Identity Analytics supports four provisioning platforms. In addition, Oracle Identity Analytics can import provisioning information from a file, as well as export to a file.

Supported provisioning platforms include:

- Oracle Identity Manager (OIM)
- Oracle Waveset (*previously* Sun Identity Manager)
- File

Note: By default, the **Administration > Configuration > Provisioning Servers** tab displays **file** and **sun** as the available options. To display other supported provisioning servers, edit `iam-context.xml` in the `RBACX_Home/WEB-INF` folder.

For more information, refer to the following chapters in the *System Integrator's Guide for Oracle Identity Analytics*.

- For Oracle Identity Manager, see the "Integrating With Oracle Identity Manager, Preferred Method" chapter.
- For Oracle Waveset, see the "Integrating With Oracle Waveset (Sun Identity Manager)" chapter.

11.1.4.1 To Create a New Provisioning Server Connection

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. Choose the correct provisioning server type for your environment and click **Next**.
6. Complete the form:
   - If you selected Oracle Identity Manager- refer to Table 11–3 for information about how to complete the form.
   - If you selected Oracle Waveset (Sun Identity Manager) - refer to Table 11–4 for information about how to complete the form.
   - If you selected File - refer to Table 11–5 for information about how to complete the form.

Table 11–3 Help on Completing the Oracle Identity Manager New Provisioning Server Connection 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.

Table 11–3 (Continued)Help on Completing the Oracle Identity Manager New Provisioning Server Connection Form

Login Config	Type the path to the authentication configuration (`auth.config`) 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 priviliges.
Password	Enter the OIM password.

Table 11–4 Help on Completing the Oracle Waveset (Sun Identity Manager) New Provisioning Server Connection Form

Connection Name	Type a new connection name for Oracle Waveset (Sun Identity Manager). 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`

User Name	Type a user name that Oracle Identity Analytics will use to connect to Oracle Waveset. You should create a special Oracle Waveset user account for this purpose. For details, see the "System Integrator's Guide" portion of the *Administrator's Guide for Oracle Identity Analytics*, "Integrating With Oracle Waveset (Sun Identity Manager)" chapter, "To Create an Oracle Waveset User That Oracle Identity Analytics Will use to Connect." Do not use the configurator account
Password	Type the password that Oracle Identity Analytics will use to connect to Oracle Waveset.
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 Identity Manager. ■ **Now** - Send changes immediately. ■ **Later**- Send updates on a daily, weekly, or monthly basis, or just one time, and select the time and date for the update task to start.

Table 11–5 Help on Completing the New Provisioning Server Connection Form - File Option

Connection Name	Type a name for the new connection being created. This connection name is used to denote the file import process.
Import Drop Location	Specify the complete path to the drop folder where the input file to be imported is located.
Import Complete Location	Specify the complete path to the folder used in the import process.

Table 11–5 (Continued)Help on Completing the New Provisioning Server Connection Form - File Option

Import Schema Location	Specify the complete path to the schema folder where the schema file for the import process is located.
Export Drop Location	Specify the path to the location where the output file will be dropped after a successful export.
Export Schema Location	Specify the path to the schema folder where the schema file for the export process is located.

11.1.5 E-mail Templates Configuration (Configuring E-mail Notification)

Oracle Identity Analytics enables you to create notifications, reminders, and escalation e-mails based on the organization's need. The e-mail templates are HTML-supported.

11.1.5.1 To Create and Configure E-mail Notifications

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Configuration**.
3. Click **E-mail Templates**.
4. Click **New E-mail Template**.
5. Complete the form using variable entries wherever required and click the **Show Parameter** hyperlink to select from the list of pre-configured parameters.

   See Section 11.1.5.2, "E-mail Parameter Definitions"for more information.
6. Click Save.

11.1.5.2 E-mail Parameter Definitions

Oracle Identity Analytics has 36 e-mail parameters (or variables) that can be selected when you create e-mail templates. Not every e-mail variable can be used with every template. If a variable is used in an unsupported scenario, the variable may appear as plain text in the e-mail, or, if the variable is used in the *To* or *CC* fields in an unsupported scenario, the e-mail may not be sent. Test your template before putting it into production.

Table 11–6 E-Mail Parameters

Name	Parameter	Definition	Applicable Modules
System Email	`$(systemEmail)`	Used for specifying system e-mail. Example: `rbacx@example.com` This variable can be used in the *From* and *Body* fields in all e-mails.	All

Table 11–6 (Continued)E-Mail Parameters

Name	Parameter	Definition	Applicable Modules
User Email	`$(userEmail)`	Used to specify the user's e-mail address and the user's manager's e-mail address in cases where escalations occur within certifications. May also be used in workflow e-mail reminders, but not for escalations of workflow reminder e-mails. This variable can be used in the *To* field.	Certification (IDC) and Workflows
User Secondary Email	`$(userSecondaryEmail)`	Used to specify the user's secondary e-mail address and the user's manager's secondary e-mail address in cases where escalations occur within certifications. This variable can be used in the *To* field.	Certification (IDC)
User Full Name	`$(userFullName)`	Used to specify the user's full name. Example: Baker, Angela. This variable can be used in the *Subject* and *Body* fields.	Certification (IDC)
User Last Name	`$(userLastName)`	Used to specify the user's last name. This variable can be used only in certain templates. Use *User Full Name*, otherwise. This variable can be used in the *Subject* and *Body* fields.	Certification (IDC)
User First Name	`$(userFirstName)`	Used to specify the user's first name. This variable can be used only in certain templates. Use *User Full Name*, otherwise. This variable can be used in the *Subject* and *Body* fields.	Certification (IDC)
Url	`$(url)`	Used to embed the Oracle Identity Analytics URL in an e-mail. This variable can be used in the *Body* field.	Certification (IDC)
Certification Name	`$(certificationName)`	Used to specify the name of the certification being processed. This variable can be used in the *Subject* and *Body* fields.	Certification (IDC)

Table 11–6 (Continued)E-Mail Parameters

Name	Parameter	Definition	Applicable Modules
Report Name	`$(reportName)`	User to specify the name of the report being processed.(It can be used to attach report name in certifications, but not in reminders.) This variable can be used in the *Subject* and *Body* fields.	Certification (IDC)
Proxy User Email	`$(proxyUserEmail)`	Used to specify the e-mail of the proxy user. This variable can be used in the *To* and *CC* and *BCC* fields of the proxy assignment e-mail template.	Certification (IDC) and Proxy (System)
Proxy User Fullname	`$(proxyUserFullname)`	Used to specify the proxy user's full name. This variable can be used in the *Subject* and *Body* fields of the proxy assignment e-mail template.	Proxy (System)
Proxy StartDate	`$(proxyStartDate)`	Used to specify the start date of the proxy period. This variable can be used in the *Body* of the proxy assignment e-mail template.	Proxy (System)
Proxy EndDate	`$(proxyEndDate)`	Used to specify the end date of the proxy period. This variable can be used in the *Body* of the proxy assignment e-mail template.	Proxy (System)
User Manager Email	`$(manager.email)`	Used to specify the e-mail address of the manager of the roleOwner, policyOwner, or other Owners. Used in workflow escalation e-mails. This variable can be used in the *To*, *CC*, and *BCC* fields.	Workflows
User Request RequesterName	`$(request.requesterName)`	Used to specify the name of the user who has initiated a request. This variable can be used in the *Subject* and *Body* fields.	Workflows
User Request Type	`$(request.type)`	Used to specify the request type (for example, "role change request"). This variable can be used in the *Subject* and *Body* fields.	Workflows
User Request Date	`$(request.date)`	Used to specify the date when a request was created. This variable can be used in the *Subject* and *Body* fields.	Workflows

Table 11–6 (Continued)E-Mail Parameters

Name	Parameter	Definition	Applicable Modules
User Role Name	`$(role.name)`	Used to specify the name of the role sent for approval. This variable can be used in the *Subject* and *Body* fields.	Workflows
User Role VersionNumber	`$(role.versionNumber)`	Used to specify the version number of the role sent for approval. This variable can be used in the *Subject* and *Body* fields.	Workflows
User RoleOwner Email	`$(roleOwner.email)`	Used to specify the e-mail addresses of role owners who own roles for which a version is sent for approval. This variable can be used in the *To, Subject*, and *Body* fields.	Workflows
User PolicyOwner Email	`$(policyOwner.email)`	Used to specify the e-mail addresses of policy owners who own policies for which a version is sent for approval. This variable can be used in the *To, Subject*, and *Body* fields.	Workflows
User Policy Name	`$(policy.name)`	Used to specify the name of the policy whose version is sent for approval. This variable can be used in the *Subject* and *Body* fields.	Workflows
User Policy VersionNumber	`$(policy.versionNumber)`	Used to specify the version number of the policy that is sent for approval. This variable can be used in the *Subject* and *Body* fields.	Workflows
Newly Reviewed Policy Owner Email	`$(newlyReviewedPolicyOwner.email)`	Used to send an e-mail notification to individual policy owners when a policy they own is approved or rejected during the Policy Owner Approval step of the Role Modification workflow. This variable should only be used with the *Approve Role* and *Reject Role* workflow steps. Added in release 11.1.1.5.	Workflows
User Manager Name	`$(userManagerFullName)`	Used to specify the full name of the user's manager. This variable can be used in the *Subject* and *Body* fields.	Identity Audit (IDA)

Table 11–6 (Continued)E-Mail Parameters

Name	Parameter	Definition	Applicable Modules
User Manager	`$(userManagerEmail)`	Used to specify the e-mail address of the user's manager. This variable can be used in the *To*, *CC*, *BCC*, *Subject*, and *Body* fields.	Identity Audit (IDA)
Identity Audit Violation Name	`$(identityAuditViolationName)`	Used to display the name of the identity audit policy violation. This variable can be used in the *Subject* and *Body* fields.	Identity Audit (IDA)
Identity Audit Violation Action	`$(identityAuditViolationAction)`	Used to display the event or type of action that resulted in an e-mail being sent to the user. This variable can be used in the *Subject* and *Body* fields.	Identity Audit (IDA)
Identity Audit Policy Owner Name	`$(identityAuditPolicyOwnerFullName)`	Used to display the full name of the identity audit policy owner associated with the violation. This variable can be used in the *Subject* and *Body* fields.	Identity Audit (IDA)
Identity Audit Policy Owner Email	`$(identityAuditPolicyOwnerEmail)`	Used to display the e-mail address of the identity audit policy owner associated with the violation. This variable can be used in the *To*, *CC*, *BCC*, *Subject*, and *Body* fields.	Identity Audit (IDA)
Identity Audit Violation Remediator Name	`$(identityAuditViolationRemediatorFullName)`	Used to display the full name of the identity audit violation remediator associated with the violation. This variable can be used in the *Subject* and *Body* fields.	Identity Audit (IDA)
Identity Audit Violation Remediator Email	`$(identityAuditViolationRemediatorEmail)`	Used to display the e-mail address of the identity audit violation remediator associated with the violation. This variable can be used in the *To*, *CC*, *BCC*, *Subject*, and *Body* fields.	Identity Audit (IDA)
Identity Audit Violation Old Remediator Name	`$(identityAuditViolationOldRemediatorFullName)`	Used to display the full name of the previous identity audit violation remediator associated with the violation for which a new user is being assigned as a remediator. This variable can be used in the *Subject* and *Body* fields.	Identity Audit (IDA)

Table 11–6 (Continued)E-Mail Parameters

Name	Parameter	Definition	Applicable Modules
Identity Audit Violation Old Remediator Email	`$(identityAuditViolationOldRemediatorEmail)`	Used to display the e-mail address of the previous identity audit violation remediator associated with the violation for which a new user is being assigned as a remediator. This variable can be used in the *To, CC, BCC, Subject*, and *Body* fields.	Identity Audit (IDA)
Identity Audit Violation Remediator Manager Email	`$(identityAuditViolationRemediatorManagerEmail)`	Used to display the e-mail address associated with the manager of a user who is currently the remediator of a violation. This variable can be used in the *Subject* and *Body* fields.	Identity Audit (IDA)

11.1.6 Import/Export

You can import the following in Oracle Identity Analytics:

- Users
- Roles
- Accounts
- Policies
- Business Structures
- Resource Metadata
- Resources
- Glossary

Details about importing are discussed in Chapter 2, "Oracle Identity Analytics Importing."

11.1.7 Workflows Configuration

A *workflow* is a specific sequence of actions or tasks that are related to a business process. In Oracle Identity Analytics, workflows enumerate each step involved in the various process, such as role and policy creation, role and policy modification, and so on. It lists all the actors, who play a pivotal role in management of roles and policies, and their function.

Oracle Identity Analytics has eight workflows:

- Role Creation Workflow
- Role Modification Workflow
- Role Membership Workflow
- Mass Modification Workflow
- Policy Creation Workflow

- Policy Modification Workflow
- Role Membership Rule Creation Workflow
- Role Membership Rule Modification Workflow

Details about understanding and designing workflows are discussed in Chapter 6, "Oracle Identity Analytics Workflows."

11.1.8 Event Listeners Configuration

The Event Listener mechanism allows a user to create listeners to business events that are happening in the system and take some actions when those events happen. An example of a business event is a user update, which occurs when some of the user attributes are updated. A listener, when created, defines the events to examine based on a condition, and also defines the actions that are to be executed by the system in response to those events.

11.1.8.1 To Create a New Event Listener

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Configuration**.
3. Click **Event Listeners**.
4. Click **Add Event Listener**.

   The new event listener form opens.
5. Add the name with which the event will be identified in the name section, the description, and the status, and click **Next**.
6. Add a condition that will be evaluated when an event takes place, then click **Next**.

   (For example, when a user is updated, a condition can check if the user's title property or location property has changed.)

   The **Action Types** form opens, specifying a list of actions that will be taken by the system when events that match the condition occur in the system.
7. Select one or more of the following actions to execute when an event condition is met:
   - **Run Business Structure Membership Rules** - Runs selected user-to-business structure rules.
   - **Run Role Membership Rules** - Runs the selected role membership rules on users.
   - **Run Identity Audit Scans** - Run selected identity audit policies on users based on a condition.
   - **Create User Entitlement Certifications** - Creates a user entitlement certification.
8. Configure the form, then click **Finish**.

Table 11–7 Action Types Selected (Add Event Listener) Form Properties

Listener Action Properties	Description
Status	Select **Enable** to run the action. Clear the checkbox if the action should not be executed.

Table 11–7 (Continued)Action Types Selected (Add Event Listener) Form Properties

Listener Action Properties	Description
Threshold Levels	For **Time Delay**, type the **Hours** and/or **Minutes** to wait before executing the actions. The timer begins when the first event occurs. All events after the timer starts are queued until the timer expires.
Event Count	Select **Event Count** and type a number to limit the number of events that can occur during the specified time period. Specifies the upper limit of the number of events that can occur in the time interval for an action. If the event count exceeds this limit, then the action will not be executed. Use this to avoid executing an action in case of bulk updates.
Actions	Add the rules that will run against the subjects that match this event listener when the threshold levels are met.
Certification Configuration	Enter details about the certification that should be created when an event condition is met. For help completing the **Configuration Details** section, see Section 11.2.1.2, "Help on Completing the Identity Certification Configuration Options."

11.2 Settings Pages

This section documents the configuration pages that are available when you choose **Administration** > **Settings** from the menu bar.

11.2.1 Identity Certification Configuration

This section describes how to configure the Oracle Identity Analytics identity certification feature. In addition, the following identity certification configuration topic is covered in the *System Integrator's Guide for Oracle Identity Analytics*:

- "Configuring Identity Certification Batch Sizes in the UI" is covered in the *System Integrator's Guide for Oracle Identity Analytics* in the "Customizing the Oracle Identity Analytics User Interface" chapter.

11.2.1.1 To Configure Identity Certification

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Settings**.
3. Click **Identity Certification**.

   The Certification Configuration page opens.
4. Click a section to expand it.
5. Complete the form and click Save.

   For help completing the form, see the following sections.

11.2.1.2 Help on Completing the Identity Certification Configuration Options

Before You Begin - See Section 11.2.1.1, "To Configure Identity Certification" for help opening the Certification Configuration page.

11.2.1.2.1 General Panel, "General" Section

Business Structure Hierarchy / Hierarchy Depth	Select the Business Structure Hierarchy option to include in a certification all the users in the business structure and all the users in business structures under it, up to the hierarchy depth chosen by the administrator.
Allow multiple open certifications per business structure	Select to allow the system to open more than one certification with an open status per business structure.
Password required to complete certifications	Select to require users to sign off in order to complete a certification.
Send E-mail copies to Admin for new certifications	Select to send a copy to the admin when a new certification is created.
Create single certification for all managers of a business structure	Select to allow multiple managers to review a single certification. The system will track the actions each manager performs along with a timestamp. Clear this option to create one certification per business structure manager.
Disallow self-certification	Select to prevent managers from being able to certify their own access. Enabling this option allows the certification creator to assign the certification to an alternate reviewer.
Enable access to Oracle Identity Manager Provisioning Server	Select to enable Oracle Identity Manager (OIM) to revoke or re-provision target system accounts based on the revocations and certifications that occurred during the Oracle Identity Analytics certification process.

"Status Options" Section

Allow comments on all non-certify selections	Select to allow the user to type a comment if a revoke action is selected. (The system does not require the user to type a comment.)
Allow comments on certify selections	Select to allow the user to type a comment if a certify action is selected. (The system does not require the user to type a comment.)

11.2.1.2.2 User Entitlement Panel, "General" Section

Select the users to certify based on the following criteria	Complete this section to select which entitlements should be reviewed. ■ **Any level of risk** - Select all users, regardless of risk level. ■ **High-risk summaries** - Select users whose overall risk is high. ■ **High-risk roles** - Select users who have high-risk roles assigned to them. ■ **High-risk resources** - Select users who have high-risk resources assigned to them. ■ **High-risk entitlements** - Select users who have high-risk entitlements assigned to them. ■ **Include users with no accounts** - Allow managers to select users under them who do not have an account. ■ **Include accounts with no certifiable attributes** - Allow managers to select users under them who do not have any certifiable attributes.

Select the items to certify for each user	Complete this section to select what will be certifed. ■ **Entitlements** ■ **All Entitlements** - Certify all entitlements. ■ **Entitlements outside roles** - Certify entitlements that are not part of a role. ■ **Accounts with high-risk entitlements** - Certify only accounts that have one or more entitlements marked as high-risk. ■ **Only high-risk entitlements** - Certify only those entitlements classified as high-risk. ■ **None** - Do not certify accounts or entitlements. ■ **Roles** ■ **All roles** - Certify all roles. ■ **Only high-risk roles** - Certify only roles that are high risk. ■ **None** - Do not certify roles.
View User Activity Information	Allows the certifier to see the user's recent account activity. **Note -** This feature is functional if Oracle Identity Analytics is integrated with Intellitactics Security Manager. To learn about this feature, see "Integrating with Intellitactics Security Manager" in the *System Integrator's Guide for Oracle Identity Analytics*.
Employee Verification Required	Select this to require managers to verify the work status (Works For Me, Does Not Work For Me, Terminated, Reports To...) of their assigned employees, then select the **Create new certification per reporting manager** option.
Create new certification per reporting manager	Select this to create a new certification if, during the employee verification process, the certifier selects "Reports To" and names a new manager for the user.

"Status Options" Section

Employee Verification	Select the following options to make them available to managers during the employee verification process. Click **Edit Label** to change the name of an employee verification action option. ■ **Claim** - The user works for you and you are the correct person to complete the certification. ■ **Decline** - The user does not work for you and you are not responsible for verifying his or her assigned roles and entitlements. ■ **Disclaim** - The user is no longer part of the organization. All of the user's roles, entitlements, and accounts will be revoked and the user is removed from the certification process. ■ **Delegate** - The user reports to another manager who is responsible for verifying this user's assigned roles and entitlements. You will not approve or revoke roles and entitlements for this user.

Certification Sign off	Select the following options to make them available to managers during the certification process. Click **Edit Label** to change the name of a certification action option. ■ **Certify** - The certification is valid. ■ **Revoke** - The certification is not valid. ■ **Abstain** - The user does not work for you and you are not responsible for the certification. ■ **Certify Conditionally** - Issue a temporary certification. An end date when the certification expires must be specified.

11.2.1.2.3 Data Owner Panel, "General" Section

Certify Entitlements	Choose one of the following: ■ **All entitlements** - Certify all entitlements. ■ **Only high risk entitlements** - Certify only entitlements that have been marked as high risk.

"Status Options" Section

Data Owner Verification	Select the following options to make them available to certifiers during the data owner verification process. Click **Edit Label** to change the name of a data owner verification action option. ■ **Claim** - The data source belongs to you and you are the correct person to complete the certification. ■ **Decline** - The data source does not belong to you and you are not responsible for completing the certification.
Approve or Revoke Data Access	Select the following options to make them available to certifiers during the certification process. Click **Edit Label** to change the name of a data owner certification action option. ■ **Certify** - The certification is valid. ■ **Revoke** - The certification is not valid. ■ **Abstain** - The user does not work for you and you are not responsible for the certification. ■ **Certify Conditionally** - Issue a temporary certification. An end date when the certification expires must be specified.

11.2.1.2.4 Resource Entitlement Panel "General" Section

Certify Resources	Choose one of the following: ■ **All resources** - Certify all resources. ■ **Only high risk resources** - Certify only resources that have been marked as high risk.

"Status Options" Section

Resource Verification	Select the following options to make them available to end-users during the resource-entitlement verification process. Click **Edit Label** to change the name of a resource verification action option. ■ **Claim** - The resource belongs to you and you are the correct person to complete the certification. ■ **Decline** - The resource does not belong to you and you are not responsible for completing the certification.
Verify employee access	Select the following options to make them available to end-users during the certification process. Click **Edit Label** to change the name of a verify employee access action option. ■ **Certify** - The user entitlement is valid for this resource for this certification. ■ **Revoke** - The user entitlement is not valid for this resource for this certification. ■ **Abstain** - You are not responsible for verifying the entitlement. ■ **Certify Conditionally** - The user entitlement should be temporarily certified for this certification. An end date when the certification expires must be specified.

11.2.1.2.5 Role Entitlement Panel, "General" Section

Certify Roles	Choose one of the following: ■ **All roles** - Certify all roles. ■ **Only high risk roles** - Certify only roles that have been marked as high risk.
Certify Policies	Also certify policies that belong to roles, as well as attributes of the policy.
Certify Members	Also certify members that belong to roles.

"Status Options" Section

Role Verification	Select the following options to make them available to end-users during the role verification process. Click **Edit Label** to change the name of a role verification action option. ■ **Claim** - The role belongs to you and you are the correct person to complete the certification. ■ **Decline** - The role does not belong to you and you are not the correct person to complete the certification.

Policy, Entitlement, and Member Access	Select the following options to make them available to end-users during the certification process. Click **Edit Label** to change the name of a verification or certification action option. ■ **Members** ■ **Certify** - The user assigned to this role is valid for this certification. ■ **Revoke** - The user assigned to this role is not valid for this certification. ■ **Abstain** - The role does not belong to you and you are not responsible for verifying any users assigned to the role. ■ **Certify Conditionally** - The user assigned to this role should be temporarily certified for this certification. An end date when the certification expires must be specified. ■ **Policies and Entitlements** ■ **Certify** - The policy or entitlement assigned to this role is valid for this certification. ■ **Revoke** - The policy or entitlement assigned to this role is not valid for this certification. ■ **Abstain** - The role does not belong to you and you are not responsible for verifying any policies or entitlements assigned to the role. ■ **Certify Conditionally** - The policy or entitlement assigned to this role should be temporarily certified for this certification. An end date when the certification expires must be specified.

11.2.1.2.6 Reminders Panel

New Certification Notification

- **Send New Certification Notification** - When a new certification is assigned, send e-mail to the certifier. Click **E-mail Template** to select which notification template to use.
- **Send E-mail When Certifier is Updated** - When a certification is assigned to a new certifier, send e-mail to the new certifier. Click **E-mail Template** select the notification template to use.

Upcoming Certification Notification

- **Reminder to Manager** - Before the certification process is scheduled to begin, send a reminder e-mail to the managers affected. Use the **Reminder Interval** list to select when the e-mail notice should be sent. Click **E-mail Template** to select the notification template to use.

Pending Certification Notification

- **Pending Certification Notifications** - From the list select if pending notifications should be based on the **Certification Create Date** (the date the certification was created), the **Certification Start Date** (the date that the certification is scheduled to start), or the **Certification End Date** (the date that the certification is scheduled to end).
- **First Reminder to Manager** - Select to schedule when a first reminder e-mail should be sent to a manager who has an assigned certification to complete. Use the **Reminder Interval** list to select when the e-mail notice should be sent. Click **E-mail Template** to select the notification template to use.
- **Second Reminder to Manager** - Select to schedule when a second reminder e-mail should be sent to a manager who has an assigned certification to complete. Use the **Reminder Interval** list to select when the e-mail notice should be sent. Click **E-mail Template** to select the notification template to use.
- **First Reminder to Manager's Manager** - Select to schedule when a first reminder e-mail should be sent to the manager of the manager who has an assigned certification to complete. Use the **Reminder Interval** list to select when the e-mail notice should be sent. Click **E-mail Template** to select the notification template to use.
- **Second Reminder to Manager's Manager** - Select to schedule when a second reminder e-mail should be sent to the manager of the manager who has an assigned certification to complete. Use the **Reminder Interval** list to select when the e-mail notice should be sent. Click **E-mail Template** to select the notification template to use.
- **Reminder to Information Security Department** - Select to schedule when a notification e-mail should be sent to the information security manager who is responsible for ensuring that certifications are completed. Use the **Reminder Interval** list to select when the e-mail notice should be sent. Click **E-mail Template** to select the notification template to use.

Certification Completion Notification

- **Send Certification Completion E-mail** - When a certification has been completed, send a notification e-mail to the certifier. Click **E-mail Template** to select which notification template to use.

Certification Expiry Notification	■ **Certification About to Expire Notification** - Select to schedule when a reminder e-mail should be sent to a manager who has an assigned certification that is about to expire. Use the **Reminder Interval** list to select when the e-mail notice should be sent (that is, choose how many days in advance of the certification expiring the notice should be sent). Click **E-mail Template** to select the notification template to use. ■ **Expired Certification Notification** - When a certification has expired, send a notification e-mail to the certifier. Click **E-mail Template** to select which notification template to use.

11.2.1.2.7 Revoke and Remediation Panel

Access Revoke	■ **Send e-mail to security administrators on access revoke** - Select to send e-mail to security administrators when a certifier revokes access. Choose from the following options how the security administrator should be notified. ■ **By certification** - Send a notification e-mail that summarizes revoked access for the certification. ■ **By each resource type in the certification** - Send a notification e-mail that, for a given certification, summarizes revoked access by each resource type. ■ **By each account in the certification** - Send a notification e-mail that, for a given certification, summarizes revoked access per account.

Reporting Changes	■ **Send reporting changes to HR** - Select to send e-mail to Human Resources (HR) when a manager *declines*, *delegates*, or *disclaims* an employee because the employee does not work for the manager, the employee works for another manager, or the employee is no longer part of the organization. Choose from the following options how HR should be notified. ■ **By certification** - Send one notification e-mail that summarizes reporting changes for the certification. ■ **By user** - Send one e-mail per user.
Remediation	■ **Display Remediation Instructions** - Select to display instructions to help end-users complete remediation steps. ■ **Perform Closed Loop Remediation** - Select to enable closed loop remediation. See Section 7.4, "Understanding Closed-Loop Remediation and Remediation Tracking" for more information. ■ **Certification End Date** - The date that the certification is scheduled to end. ■ **Certification Completion Date** - The date that the certification is completed.

11.2.2 Role Management Configuration

This section describes how to configure the Oracle Identity Analytics role mining and "SoD evaluation of role assignment" feature.

11.2.2.1 To Configure Mining

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Settings**.
3. Click **Role Management**.

   The Role Management page opens
4. Click on **New Excluded Value**.
5. Complete the form by selecting the attribute value that needs to be excluded from mining and click Ok.

11.2.2.2 To Configure Roles

1. Log in to Oracle Identity Analytics.

2. Choose **Administration** > **Settings**.
3. Click **Role Management**.

   The Role Management page opens.
4. Click on **Roles**.
5. Select from the following to perform an SoD evaluation of a role assignment:
   - **Disallow Assignment -** Blocks the assignment if there is a SoD Violation.
   - **Allow Assignment and Flag Audit Exception -** Allows the assignment even if there is a SoD violation, but flags the audit exception.

11.2.3 Identity Audit Configuration

The identity audit configuration page provides the interface for setting up the e-mail notification preferences for audit policy violation events and actions.

11.2.3.1 To Configure the Identity Audit Module

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Settings**.
3. Click **Identity Audit**.
4. Select the desired configurations based on the requirements of the organization.

11.2.3.2 To Prevent Self-Remediation of Audit Violations

Follow these steps to prevent users from being able to remediate their own violations if their attributes, roles, or entitlements are causing a Segregation of Duties violation.

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Settings**.
3. Click **Identity Audit**.
4. Select **Prevent Self-Remediation**.

Note: Self-remediation is allowed by default for Oracle Identity Analytics customers who upgraded from a version older than 11gR1 PS1 because previous versions of the product allowed self-remediation. Self-remediation, however, is not considered a best practice and customers are encouraged to choose the **Prevent Self-Remediation** option.

5. Use the **Alternate reviewer** select box to specify who should be the designated alternate reviewer. Choose from the following:
   - **User Manager** - Make the original reviewer's manager the designated reviewer/remediator.
   - **Select** - Type a name in the user search box to make a specific user the designated reviewer/remediator.

11.2.3.3 To Configure E-mails for Violation Reminder and Escalation

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

3. Click **Identity Audit**.
4. Do one of the following in the **Violation Reminder and Escalation** section:
   - Select **Send Email Reminder(s)** to choose when and how frequently reminder e-mails are sent to the violation assignee when no action is taken on the violation after it is assigned. You can also choose the template for the reminder e-mail.
   - Select **Escalate After Reminders** to choose the maximum number of reminders to send before escalating the violation to the assignee's manager. You can also choose an e-mail template to use for the escalation notice.
5. Click Save.

11.2.3.4 To Configure E-mails For Violation Lifecycle Event Notifications

1. Log in to Oracle Identity Analytics.
2. Go to **Administration** > **Settings**.
3. Click **Identity Audit**.
4. Select from the following options in the **Violation Lifecycle Event Notifications section**:
   - **Send E-mail For New Violations** - Choose an e-mail template and also send e-mail notifications to actors associated with the new violations that are created.
   - **Send E-mail For Reopened Violations** - Choose an e-mail template and send e-mail notifications to actors associated with the violations that are reopened.
   - **Send E-mail For User or System Remediated Violations** - Choose an e-mail template and also send e-mail notifications to actors associated with the violations that are closed as resolved by the system or user.
   - **Send E-mail When Violation is Assigned** - Choose an e-mail template and send e-mail notifications to actors associated with the violation that is assigned to a user.
   - **Send E-mail When Violation Closed as Risk Accepted** - Choose an e-mail template and send e-mail notifications to actors associated with the violation that is closed as risk accepted.
5. Click Save.

11.2.4 Reports Configuration

You can configure Oracle Identity Analytics to send e-mails to data owners using pre-defined e-mail templates. Reminder e-mails can be sent to data owners, the data owners' managers, and to the Information Security Department.

11.2.4.1 To Configure Report Reminder E-mails

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Settings**.
3. Click **Reports**.

   The Report Configuration page opens.
4. To configure the send-reminder-email workflow, select a reminder, select a reminder interval, and select an e-mail template.

E-mail templates are created on the E-mail Templates tab. For help, see Chapter 11.1.5, "E-mail Templates Configuration (Configuring E-mail Notification)" in the Oracle Identity Analytics Configuration chapter.

5. Click Save.

11.2.5 Identity Warehouse Configuration

Candidate List

Only Privileged Users in Candidate Owner List - When associating role owners with roles or policy owners with policies, you can restrict the menu to only include those users who have sufficient access rights to perform the job. To do so, enable this option. If this option *is not* enabled, the menu of users will list all users, which means it is possible to select a user who does not posses the permissions required to do the job.

Note: If this feature is enabled, to appear in the menu the user must be assigned an OIA Role containing these user privileges:

- Create Role (Policy)
- Decommission Role (Delete Policy)
- Update Role (Policy)

To manage Identity Warehouse Roles (Policies) from the UI, the following additional privileges must be assigned:

- Access to Role (Policy) View
- Access to My Requests

12

Oracle Identity Analytics Access Control

This chapter describes how to assign privileges to Oracle Identity Analytics users. It contains the following sections:

12.1 Overview

In Oracle Identity Analytics, you use the Access Control tab (**Administration** > **Access Control**) to assign Oracle Identity Analytics roles to Oracle Identity Analytics users. Oracle Identity Analytics users are actors who need privileges within Oracle Identity Analytics to attest, revoke, and remediate certifications and policies, or carry out various other tasks. Oracle Identity Analytics roles are the privileges or permissions assigned to Oracle Identity Analytics users.

Oracle Identity Analytics access control has two components: system-level privileges and business-level privileges. Usually system-level privileges are most appropriate for administrator roles, and business-level privileges are most appropriate for business user roles. System-level privileges and business-level privileges are added to roles as needed, and roles are assigned to Oracle Identity Analytics users based on the tasks that users need to complete.

Oracle Identity Analytics includes nine roles that work out-of-the-box that you can edit or delete as needed.

Table 12–1 Oracle Identity Analytics Default System Roles

Role Name	Description	Privileges
OIA Admin	Oracle Identity Analytics administrator	OIA Administrator
Certification Manager	Grants certification privileges	Access to the Identity Certification view
Policy Violation Remediator	Grants a user the ability to remediate policy violations	Access Policy Violations sub-tab under Identity Audit tab, Read access to Assigned Policy Violations, Write access to Assigned Policy Violations

Table 12–1 (Continued)Oracle Identity Analytics Default System Roles

Role Name	Description	Privileges
Role Engineer - Administrator	Role Engineer - Administrator	Access to Role Management tab, access to My Requests tab, access to Policies view, access to Roles view, Create Role, Delete Role, Update Role, Create Policy, Delete Policy, and Update Policy
Policy Owner (Identity Audit)	Policy Owner (Identity Audit)	Access the Dashboard sub-tab under the Identity Audit tab, access the Policies sub-tab under the Identity Audit tab, access the Rules sub-tab under the Identity Audit tab, access Policy Violations sub-tab under the Identity Audit tab
Warehouse Administrator	Warehouse administrator	Create Business Structure, delete Business Structure, update Business Structure, create User, delete User, update User, create role, delete Role, update Role, create Policy, delete Policy, update Policy, access to Business Structures view, access to Policies view, access to Roles view, access to Users view, access the Users tab in Business Structure view, access the Roles tab in Business Structure view, access the Policies tab in Business Structure view, access the Policies tab in the Resources view, access the Business Structure tab in the Roles view, access the users tab in the Roles view, access the Policies tab in the Roles view, access the Exclusion Roles tab in Roles view, access the roles tab in Users view, access the Business Structure tab in the Users view, access the Accounts tab in the Users view, run Business Structure reports.
Workflow Designer	Workflow designer	Access the Workflow Design sub-tab under Administration / Configuration
Reporting Administrator	Reporting administrator	Run Business Structure reports, access the reports dashboard, upload custom reports, run system reports, run Audit reports, run custom reports, access the scheduling reports sub-tab under the Reports tab
Compliance Administrator	Compliance Administrator	Access to Identity certification View, Create IDC Certification, access the Dashboard sub-tab under the Identity Audit tab, access the Policies sub-tab under the Identity Audit tab, access the Rules sub-tab under the Identity Audit tab, access the Policy Violations sub-tab under the Identity Audit tab, run business structure reports, upload custom reports, run system reports, run Audit reports, run Custom reports, access to the Scheduling Reports sub-tab under the Reports tab, access to the Reports dashboard, access to Identity Certification Remediation Tracking, access to the Resource type view, configure Identity certification, configure email template, and access the Configuration system sub-tab

12.2 System Privileges

Table 12–2 OIA System Privileges

Privilege	Description
CREATE Business Unit	Allows a user to add new Business Units
UPDATE Business Unit	Allows a user to modify existing Business Units
DELETE Business Unit	Allows a user to delete existing Business Units
CREATE User	Allows a user to add new Global Users
UPDATE User	Allows a user to modify existing Global Users
DELETE User	Allows a user to delete existing Global Users
CREATE Role	Allows a user to add new Roles
UPDATE Role	Allows a user to modify existing Roles
DELETE Role	Allows a user to delete existing Roles
CREATE Policy	Allows a user to add new Policies
UPDATE Policy	Allows a user to modify existing Policies
DELETE Policy	Allows a user to delete existing Policies
CREATE Resource	Allows a user to add new Resources
UPDATE Resource	Allows a user to modify existing Resources
DELETE Resource	Allows a user to delete existing Resources
CREATE Schedule Job	Allows a user to add new Schedule Jobs
UPDATE Schedule Job	Allows a user to modify existing Schedule Jobs
DELETE Schedule Job	Allows a user to delete existing Schedule Jobs
Access Report Dashboard	Allows a user to review compliance performance
Import Data	Allows a user to import data from ETrust Admin to Oracle Identity Analytics
Export Data	Allows a user to export data from Oracle Identity Analytics to ETrust Admin
Configure System	Allows a user to configure the IAM servers and attributes
Access Configuration system subtab	Allows a user to access the Configuration system sub-tab
Access Resource type view	Allows a user to access Resource Type view
Configure Resource type definitions	Allows a user to configure Resource Type definitions
Configure Identity Certification	Allows a user to configure identity certifications
Configure Email Templates	Allows a user to configure email templates
Access to Audit view	Allows a user to access Audit view
Access to Business Structures view	Allows a user to access Business Structures view
Access to Resource view	Allows a user to access Resource view
Access to Policies view	Allows a user to access Policies view
Access to Roles view	Allows a user to access Roles view

Table 12–2 (Continued)OIA System Privileges

Privilege	Description
Access to Scheduler view	Allows a user to access Scheduler view
Access to Users view	Allows a user to access Users view
Run Business Structure Reports	Allows a user to run Business Structure reports
Upload Custom Reports	Allows a user to upload custom reports
Run System Reports	Allows a user to run System Reports
Run Audit Reports	Allows a user to run Audit Reports
Run Custom Reports	Allows a user to run custom reports
Access the Users tab in Business Structure View	Grants a user access to the Users tab in Business Structure view
Access the Roles tab in Business Structure View	Grants a user access to the Roles tab in Business Structure view
Access the Policies tab in Business Structure View	Grants a user access to the Policies tab in Business Structure view
Access the Policies tab in Resources view	Grants a user access to the Policies tab in Resources view
Access the Business Structure tab in Roles view	Grants a user access to the Business Structure tab in Roles view
Access the Users tab in Roles view	Grants a user access to the Users tab in Roles view
Access the Policies tab in Roles view	Grants a user access to the Policies tab in Roles view
Access the Exclusion Roles tab in Roles view	Grants a user access to the Exclusion Roles tab in Roles view
Access the Roles tab in Users view	Grants a user access to the roles tab in Users view
Access the Business Structure tab in Users view	Grants a user access to the Business Structure tab in Users view
Access the Accounts tab in Users view	Grants a user access to the Accounts tab in Users view
Create IDC Certification	Allows a user to create a new identity certification
Access to Access Control tab	Grants a user access to the Access Control tab
Access to Glossary tab	Grants a user access to the Glossary tab
Access to Auditing & Events tab	Grants a user access to the Auditing & Events tab
Access to Password Configuration tab	Grants a user access to the Password Configuration tab
Access to Audit Event Logs sub-tab under Auditing & Events tab	Grants a user access to the Audit Event Logs subtab under Auditing & Events tab
Access to Import Logs subtab under Auditing & Events tab	Grants a user access to the Import Logs subtab under Auditing & Events tab

Table 12–2 (Continued)OIA System Privileges

Privilege	Description
Access Workflow Design subtab under Administration > Configuration	Grants a user access to the Workflow Design subtab under Administration > Configuration
Access to web service method Find Users in a given role	Grants a user access to the web service method Find Users in a given role
Read Access to Assigned Policy Violations	Grants a user read access to the Assigned Policy Violations
Write Access to Assigned Policy Violations	Grants a user write access to the Assigned Policy Violations
Access to Identity Certification View	Grants a user access to the Identity Certification View
Access to Identity Certification Dashboard	Grants a user access to the Identity Certification Dashboard
Access to Identity Certification Remediation Tracking	Grants a user access to the Identity Certification Remediation Tracking
Access Dashboard subtab under Identity Audit tab	Grants a user access to the Dashboard subtab under Identity Audit tab
Access Policies subtab under Identity Audit tab	Grants a user access to the Policies subtab under Identity Audit tab
Access Rules subtab under Identity Audit tab	Grants a user access to the Rules subtab under the Identity Audit tab
Access Policy Violations subtab under Identity Audit tab	Grants a user access to the Policy Violations subtab under Identity Audit tab
Access the Role Management tab	Grants a user access to the Role Management tab in the main view
Access to My Requests tab	Grants a user access to the My Requests tab in the main view
Access to scheduling reports subtab under Reports tab	Grants a user access to the Scheduling Reports subtab under the Reports tab

12.3 Business Privileges

Table 12–3 OIA Business Privileges

Privilege	Description
Access Business Structure	Allows a user to access Business Structure details
Add Child Business Structure to Business Structure	Allows a user to add child Business Structure
Add/Remove User to/From Business Structure	Allows a user to add/remove Global users
Add/Remove Role to/From Business Structure	Allows a user to add/remove Roles
Add/Remove Policy to/From Business Structure	Allows a user to add/remove Policies

Table 12–3 (Continued)OIA Business Privileges

Privilege	Description
Sign off Reports	Allows a user to sign off on reports
Certify Entitlements	Allows a user to certify associated entitlements

12.4 Working With Oracle Identity Analytics Users And Roles

This section describes how to create and manage users who will be using Oracle Identity Analytics. It also describes how to create Oracle Identity Analytics roles.

12.4.1 To Create, Update, and Delete an Oracle Identity Analytics User

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Access Control**.
3. Click **OIA Users**.
   - The **Search** field searches on the **User Name** column. Searching on `la*`, for example, might return the users with user names *ladams* and *lapple*.
   - To delete a user, find the user and click **Delete** in the **Action** column.
   - To update a user, find the user, click the user name, make updates as needed, and click Save.
   - To create a new user, click **New OIA User**.

   1. Complete the user information form and click **Next**.
   2. Use the arrow buttons to move system roles between the **Available System Roles** column and the **Selected System Roles** column, and click **Next**.

      The available Business Roles are listed on the left-hand side.
   3. Select the desired Business Role by using the arrow keys and click **Finish**.
   4. Once the Roles have been assigned to the user, click Save.

      A New user will be created and will appear in the OIA Users List.

12.4.2 To Modify User Password

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Access Control**.
3. Click **OIA Users**.
4. Find the user whose password you need to change and click the User Name.

   The **Search** field searches on the **User Name** column. Searching on `la*`, for example, might return the users with user names *ladams* and *lapple*.
5. Click **Change Password**.

   The Change Password dialog box opens.
6. Type the new password in the **New Password** and **Confirm Password** fields and click OK.

12.4.3 To Create OIA Roles

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Access Control**.
3. Click **OIA Roles**.
4. Click **New OIA Role**.
5. Type a name for the role and a description, and click **Next**.

   The New OIA Role Manager Wizard opens.
6. Use the arrow buttons to move system privileges between the **Available System Privileges** column and the **Selected System Privileges** column, and click Next.
7. Use the arrow buttons to move business privileges between the **Available Business Structure Privileges** column and the **Selected Business Structure Privileges** column, and click Next.
8. Click Finish.

   The new OIA Role is created.

12.5 Configuring Password Policy Settings

Password policy settings in OIA consist of password quality and password expiration settings.

12.5.1 To Configure Password Policy Settings

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Access Control**.
3. Click **Password Policy Settings**.
4. Complete the form and click Save.

12.5.1.1 Password Quality Settings

To configure password quality settings, select **Enable Quality Check** and/or **Enable Dictionary Check**. Use these options to enforce password quality guidelines when creating OIA user account passwords.

Table 12–4 Password Quality Configuration Settings

Quality Settings	Description
Minimum Password Length	Set the minimum password length
Minimum Alphabetics Characters	Set the minimum alphabet characters required in the password
Minimum Upper Case Characters	Set the minimum upper case characters required in the password
Minimum Lower Case Characters	Set the minimum lower case characters required in the password
Minimum Numeric Characters	Set the minimum numeric characters required in the password
Minimum Special Characters	Set the minimum special characters required in the password

Table 12–4 (Continued)Password Quality Configuration Settings

Quality Settings	Description
Minimum Alpha Numeric Characters	Set the minimum alpha numeric characters required in the password

Select **Enable Dictionary Check** to reject passwords that appear in the system's dictionary.

12.5.1.2 Password Expiration Settings

Table 12–5 Password Expiration Configuration Settings

Expiration Settings	Description
Maximum Change Interval	Set the number of days after which the password expires
Expiration Warning Interval	Set the number of days prior to password expiration to start redirecting user logins to the password expiration warning page
Force Change By Date	Set the date by which every user must change his password. When this field is set to a date in the future, the current date is recorded in a hidden configuration variable to establish the force-change-by-date interval start. Any user logging in having no last-password-change value or one prior to the start of the force-change-by-date interval will be directed to the expiring password page. Once the force-change-by-date has passed, any user who has not changed his password since the start of the force-change-by-date interval will be directed to the expired password page. The normal password expiration policy is in effect once a user has satisfied the force-change-by-date policy.

13

Audit Event Log and Import-Export Log

This chapter contains the following sections:

- Section 13.1, "Overview"
- Section 13.2, "Audit Event Log"
- Section 13.3, "Import-Export Log"

13.1 Overview

Oracle Identity Analytics writes messages to several logs. The two logs most commonly used by business administrators, however, are the following:

- Oracle Identity Analytics Audit Event Log
- Oracle Identity Analytics Import/Export Log

These logs can be viewed from the user interface. Audit Event log records and reports user operations in Oracle Identity Analytics, whereas Import/Export log captures all the information that is imported and exported from Oracle Identity Analytics. In addition, select records can be saved as CSV files, which you can open using your preferred spreadsheet or reporting software.

13.2 Audit Event Log

User operations in Oracle Identity Analytics are recorded and reported in the Audit Event log. The following Oracle Identity Analytics events are logged:

- Add, Modify, and Delete user actions
- Login and Logout actions
- User password updates

The details captured by the audit events are described in this table.

Table 13–1 Information Recorded in the Audit Event Log

Function	Description
Timestamp	Denotes the time when the audit event was captured
User Name	Denotes the user ID of the account that initiates the change
Full Name	Denotes the first and last name of the user account that initiates the change
Action	One of these actions are shown in this column: ADD, MODIFY, DELETE, LOGIN, LOGOUT

Table 13–1 (Continued)Information Recorded in the Audit Event Log

Function	Description
Description	Description of the audit event
Remote IP Address	IP address of the machine that initiates the change
Remote Host Name	Host name of the machine that initiates the change
Server IP Address	IP address of the Oracle Identity Analytics instance
Server Host Name	Host name of the Oracle Identity Analytics instance

13.2.1 To View Audit Log Events

Follow these steps to use the user interface to view Audit Log events.

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Auditing & Events**.
3. Use the panel on the left side of the screen to search for audit events:
   a. Click an action type (*add*, *modify*, *delete*, *login/logout*, or *all*) to view events that fit the chosen criteria.
   b. Type a name in the **User Name** field or the **Full Name** field, and click **Filter** to further narrow your search.
   c. Use the calendar controls to further narrow your search.
   d. Click **Refresh** to view the updated results.
4. Select an event and click **View Details** to view additional information about the event.

13.2.2 To Export Audit Log Events to a Spreadsheet

Follow these steps to save audit event log records as a CSV file that you can open using a spreadsheet application.

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Auditing & Events**.
3. Use the panel on the left side of the screen to search for audit events:
   a. Click an action type (*add*, *modify*, *delete*, *login/logout*, or *all*) to view events that fit the chosen criteria.
   b. Type a name in the **User Name** field or the **Full Name** field, and click **Filter** to further narrow your search.
   c. Use the calendar controls to further narrow your search.
   d. Click **Refresh** to view the updated results.
4. Click **Export** to save audit event log records as a CSV file that you can open using a spreadsheet application.

13.3 Import-Export Log

To verify that import and export jobs successfully completed, review the Import-Export log. Job status is listed in the **Result** column.

The details captured by the import logs are described in the following table.

Table 13–2 Import Information Displayed on the Import/Export Log Page

Field	Description
User Name	Describes the method used to import the feed files (for example, BATCH).
Source/Target	Describes the source of the import (for example, FILE_IMPORT).
Import/Export	Denotes whether the action was an import or export action.
Type	Describes the import/export type. Must be one of the following: Accounts, Glossary, or Users.
Description	The file name is specified in the description.
Start time	The time that the import started.
End Time	The time that the import ended.
Result	Denotes whether or not the action was successful.

The following details are captured in the import logs and can be viewed within the user interface by selecting a record and clicking View Details.

Table 13–3 Additional Import Information Displayed on the Import/Export Log Details Page

Field	Description
Number of Input Records	Total number of records in the feed file
Number of Output Records	Total number of records imported by Oracle Identity Analytics
Number of Errors	Number of errors encountered during the feed import
Show Exceptions	Displays a table that lists import exceptions, including for each exception the Timestamp, Exception Level, Exception Type, and Description

The details captured by the export logs are described in the following table.

Table 13–4 Export Information Displayed on the Import/Export Log Page

Field	Description
User Name	Describes the method used to export the feed files (for example, BATCH).
Source/Target	Describes the source of the export (for example, FILE_EXPORT).
Import/Export	Denotes whether the action was an import or export action.
Type	Describes the import/export type. Must be one of the following: Accounts, Glossary, or Users.
Description	The file name is specified in the description.
Start time	The time that the export started.
End Time	The time that the export ended.
Result	Denotes whether or not the action was successful.

The following details are captured in the export logs and can be viewed within the user interface by selecting a record and clicking View Details.

Table 13–5 Additional Export Information Displayed in the Import/Export Log Details Page

Field	Description
Total number of records	Total number of records in the feed file
Records Exported	Total number of records exported by Oracle Identity Analytics
Number of Errors	Number of errors encountered during the feed export

13.3.1 To View Import and Export Log Events

Follow these steps to use the user interface to view Import/Export Log events.

1. Log in to Oracle Identity Analytics.
2. Choose **Administration** > **Auditing & Events**.
3. Click **Import/Export Logs** in the secondary menu.
4. Use the panel on the left side of the screen to search for import/export events:
    a. Click an action type (**All**, **Accounts**, **Glossary**, or **Users**) to view import/export events that fit the chosen criteria.
    b. In the **Filter** section, type search criteria and click **Filter** to further narrow your search.
    c. Use the calendar controls to narrow your search further.
    d. Click **Refresh** to view the updated results.
5. Select an event and click **View Details** to view additional information about the event.

13.3.2 To Export Import-Job Log Details to a Spreadsheet

Follow these steps to export to a CSV file the details of an individual import job.

Before You Begin - View the details of the import or export job that you want to export. Use the procedure described in Section 13.3.1, "To View Import and Export Log Events."

1. On the Import Log Details page, click **Export** at the bottom of the page.

    The Export Logs dialog box opens.
2. In the **Export Format** drop-down menu, select **CSV** and click OK.

    You are prompted to open the file or save the CSV file to your system.
3. Open the CSV file in a spreadsheet or some other application.

System Administrator's Guide

Part II is the System Administrator's Guide, which describes how to configure and administer the Oracle® Identity Analytics software at a systems level.

14

Securing Oracle Identity Analytics

This chapter contains the following sections:

- Section 14.1, "Overview"
- Section 14.2, "Understanding the Property Encryption Utility"
- Section 14.3, "Enabling SSL Encryption Between Oracle Identity Analytics and the Database"

14.1 Overview

This chapter covers topics that have to do with securing Oracle Identity Analytics at the system level.

14.2 Understanding the Property Encryption Utility

Oracle Identity Analytics (OIA) includes a property encryption utility that can encrypt sensitive property data that the system requires. Upon encrypting a property, the utility saves it with a `.encrypted` suffix appended to the property name. When OIA reads a property file and encounters a property name with the `.encrypted` suffix, the system decrypts the property value and assigns the clear-text value to the base property name in memory. The system can then use the clear-text value in internal references to the property.

14.2.1 To Run the Property Encryption Utility

1. Open a command prompt
2. At the command-line type the following command (all on one line):

```
$ java -jar <servlet-container>/rbacx/WEB-INF/lib/vaau-commons-crypt.jar
-encryptProperty -cipherKeyProperties <arg> -propertyFile <arg> -propertyName
<arg>
```

where:

`-encryptProperty`	The property encryptor command
`-cipherKeyProperties <arg>`	The filesystem path to the cipher key properties file
`-propertyFile <arg>`	The filesystem path to the property file containing the property to encrypt

`-propertyName <arg>`	The name of the property to encrypt

Following is a sample usage of the Property Encryption Utility:

```
$ java -jar <webapp-root>/WEB-INF/lib/vaau-commons-crypt.jar
-encryptProperty -cipherKeyProperties ${RBACX_HOME}/conf/cipherKey.properties
-propertyFile ${RBACX_HOME}/conf/jdbc.properties -propertyName jdbc.password
```

14.2.2 To Encrypt the Database Password

Use the steps in this section to change your database password and encrypt it in Oracle Identity Analytics.

> **Note:** You should change and encrypt your database password if you upgraded from a version of Oracle Identity Analytics that is older than version 11.1.1.5.0.

1. Shut down all instances of Oracle Identity Analytics that use the JDBC database account for which you will be encrypting the password.
2. Log on to the database and change your database password.
3. On the OIA application server, open a text editor and set the `jdbc.password` property in the `jdbc.properties` file to the new clear-text database password.
4. At a command-line, type the following to run the Property Encryption Utility (see Section 14.2, "Understanding the Property Encryption Utility" for more information about this command):

   - **Windows:**

     ```
     C:\> java -jar <webapp-root>\WEB-INF\lib\vaau-commons-crypt.jar
     -encryptProperty -cipherKeyProperties
     %RBACX_HOME%\conf\cipherKey.properties
     -propertyFile %RBACX_HOME%\conf/jdbc.properties -propertyName jdbc.password
     ```

   - **UNIX:**

     ```
     $ java -jar <webapp-root>/WEB-INF/lib/vaau-commons-crypt.jar
     -encryptProperty -cipherKeyProperties
     ${RBACX_HOME}/conf/cipherKey.properties
     -propertyFile ${RBACX_HOME}/conf/jdbc.properties -propertyName
     jdbc.password
     ```

   The password is encrypted and stored as `jdbc.password.encrypted`.
5. Start the OIA instance and confirm it can access the OIA database.
6. Repeat these steps for each additional instance that you shut down in step 1, or, if every OIA instance uses identical JDBC connection properties, copy the `jdbc.properties` file to all instances.

14.3 Enabling SSL Encryption Between Oracle Identity Analytics and the Database

You can encrypt communication between the Oracle Identity Analytics server and the database by enabling SSL.

14.3.1 To Configure OIA to use SSL with the Database

These steps describe how to enable SSL encryption between OIA and the database. Instructions for enabling client-authentication and server-authentication are not provided.

1. Shut down all instances of Oracle Identity Analytics.
2. Open the `RBACX_HOME/conf/jdbc.properties` file for editing.
3. Add the following line to the file. Replace the host, port, and service name values with the values that point to your database server:

   For Oracle Database:

   ```
   jdbc.url=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=10.0.0.15
   )(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=orcl)))
   ```

   For example:

   ```
   jdbc.url=jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps)(HOST=psdb6011.
   us.example.com)(PORT=2484))(CONNECT_DATA=(SERVICE_NAME=orcl)))
   ```

4. Save your changes.
5. Open the `RBACX_HOME/conf/jdbcConnectionFactory.properties` file for editing.
6. Add the following line to the file and save your changes:

   For Oracle Database:

   ```
   oracle.net.ssl_cipher_suites=(SSL_DH_anon_WITH_3DES_EDE_CBC_SHA,
   SSL_DH_anon_WITH_RC4_128_MD5,SSL_DH_anon_WITH_DES_CBC_SHA)
   oracle.net.ssl_server_dn_match=false
   ```

7. Start the OIA instance and confirm it can access the OIA database.
8. Repeat these steps for each additional instance that you shut down in step 1, or, if every OIA instance uses identical JDBC connection properties, copy the `jdbc.properties` file and the `jdbcConnectionFactory.properties` file to all instances.

SSL encryption is now enabled for your JDBC connections.

15

Understanding and Configuring the System Log

This chapter contains the following sections:

- Section 15.1, "Overview"
- Section 15.2, "The System Log"
- Section 15.3, "Configuring the System Log"

15.1 Overview

The Oracle® Identity Analytics System Log (`rbacx.log`) captures information that is useful for both troubleshooting and general monitoring purposes. In particular, the System Log captures information about exceptions that arise while running the application.

15.2 The System Log

The system log is located in the *$RBACX_HOME*`/logs` folder.

Note: The `$RBACX_HOME` environment variable denotes the path to the directory in which the Oracle Identity Analytics 11gR1 software is installed.

Note: Oracle Identity Analytics writes messages to two other logs: the Audit Event Log and the Import-Export Log.

- The Audit Event Log records actions that affect users, such as Add, Modify, and Delete user actions, user password updates, and login and logout actions.
- The Import-Export Log records details about import jobs, including user imports, account imports, and glossary imports, and export jobs.

These logs are documented in Chapter 13, "Audit Event Log and Import-Export Log."

15.3 Configuring the System Log

This document explains how to configure Oracle Identity Analytics logging.

Oracle Identity Analytics uses a Java™ logging framework called log4j. Oracle Identity Analytics log files are listed in the `log4j.properties` file, which is located in the `$RBACX_HOME/WEB-INF` folder. The `log4j.properties` file is used to configure different logging levels within Oracle Identity Analytics and also to enable and disable logging as needed. Each line in the `log4j.properties` file corresponds to a component in Oracle Identity Analytics, and each component can output messages to a log.

> **Note:** If Oracle Identity Analytics is deployed on WebSphere and the system is not writing messages to the System Log file, try the following:
>
> 1. Open the following file in a text editor:
>
>    ```
>    $RBACX_WAR/META-INF/services/org.apache.commons.
>    logging.LogFactory
>    ```
>
> 2. Replace the existing value with the following value and save your changes:
>
>    ```
>    org.apache.commons.logging.impl.Log4jFactory
>    ```

15.3.1 Logging Levels

The following table defines the four levels of logging that can be set within log4j for Oracle Identity Analytics components.

Table 15–1 Logging Levels in log4j for Oracle Identity Analytics Components

Level	Description
FATAL	This level will record events only if a severe error condition occurs. Use this setting if the minimum amount of logging is desired.
ERROR	This level will record events if there is an ERROR condition.
WARN	This is the default level. It records events if potentially harmful situations occur.
DEBUG	Use this setting if the maximum amount of logging is desired.

15.3.2 Understanding How the log4j.properties File Is Organized

The following table describes the more than two dozen sections that make up the Oracle Identity Analytics `log4j.properties` file. Set properties in a given section to control logging for individual components. Sections are listed in the table in the same order that they appear in the default Oracle Identity Analytics `log4j.properties` file. For reference, see Section 15.3.3, "log4j.properties File" at the end of this chapter.

Table 15–2 Configuration Settings in the Oracle Identity Analytics `log4j.properties` ***File***

Section	Description
Console Appender	These properties control how Java console logging events are formatted. **Note** - These properties apply to the logging *format* only.

Table 15–2 (Continued)Configuration Settings in the Oracle Identity Analytics `log4j.properties` ***File***

Section	Description
File Appender	These properties configure the `rbacx.log` file.
Tomcat logging	Configures Tomcat-related logging if Oracle Identity Analytics is deployed to a Tomcat application server. Logs are generated and stored in the *$RBACX_HOME*`/tomcat55/logs/` folder in a file named `rbacx.log`.
VAAU commons logging	Configures message logging having to do with component interactions within Oracle Identity Analytics.
Oracle Identity Analytics Core logging	Configures the logging of core events inside Oracle Identity Analytics. **Note - These properties should be changed when troubleshooting in Oracle Identity Analytics.**
Oracle Identity Analytics Security logging	Configures the logging of events related to security in Oracle Identity Analytics. This setting includes user creation and login/logout events in Oracle Identity Analytics.
Oracle Identity Analytics Scheduling logging	Configures scheduler component logging in Oracle Identity Analytics. Events recorded by the Quartz Job Scheduler component can be configured using this property.
Oracle Identity Analytics ETL	Configures the logging of events output by the ETL (Extract, Transform, and Load) process inside Oracle Identity Analytics.
Oracle Identity Analytics IAM logging	Configures the logging of events based on activity between Oracle Identity Analytics and an IAM (Identity Access Management) server. This includes any file-based imports that occur inside Oracle Identity Analytics.
Oracle Identity Analytics Reporting logging	Configures the logging of events related to the running of reports inside Oracle Identity Analytics.
Oracle Identity Analytics Audit logging	Configures the logging of auditing events inside Oracle Identity Analytics, such as login/logout events and changes made inside Oracle Identity Analytics.
Oracle Identity Analytics IDC logging	Configures the logging of events related to the Oracle Identity Analytics Identity Certification component.
System	Configures the logging of System component events in Oracle Identity Analytics.
Sandbox	Configures the logging of identity audit (IDA) inside Oracle Identity Analytics.
Workflow	Configures the logging of Oracle Identity Analytics workflow events.
SqlMap logging configuration	Configures the logging of events having to do with communications between the database and Oracle Identity Analytics.
Spring Framework	Configures the logging of events that have to do with the underlying Spring Framework. Oracle Identity Analytics is built using the Spring Framework. Note - These properties should be changed when troubleshooting in Oracle Identity Analytics.
JIAM log	Configures the logging of events based on activity between a JIAM connection, such as CA-Admin, and Oracle Identity Analytics.

Table 15–2 (Continued)Configuration Settings in the Oracle Identity Analytics `log4j.properties` ***File***

Section	Description
Quartz scheduler	Configures the logging of events that have to do with the Quartz Job Scheduler that is used in Oracle Identity Analytics. Also see the "Oracle Identity Analytics Scheduling logging" property, above.
DWR	Configures the logging of events related to the web client (user interface) JSP™ pages.
ehcache	Configures the logging of events related to the cache on the Oracle Identity Analytics web client (user interface). (Ehcache is a Java cache library that is used in Oracle Identity Analytics.)
CloverETL	Configures the logging of events related to the CloverETL framework. The CloverETL framework is used in support of the Oracle Identity Analytics ETL (extract, transform, load) functionality.
C3pO	Configures the logging of events related to the c3p0 library. Oracle Identity Analytics uses the c3pO library to support common database pooling.
JasperReports	Configures the logging of events related to the JasperReports library. Oracle Identity Analytics uses the JasperReports library to create and output reports.

15.3.3 log4j.properties File

This section provides a sample `log4j.properties` file.

```
log4j.rootLogger=INFO, file
# Console Appender
log4j.appender.console=org.apache.log4j.ConsoleAppender
log4j.appender.console.layout=org.apache.log4j.PatternLayout
log4j.appender.console.layout.ConversionPattern=%d{ABSOLUTE} %-5p [%c{1}] %m%n


# File Appender
log4j.appender.file=org.apache.log4j.DailyRollingFileAppender
log4j.appender.file.file=logs/rbacx.log
log4j.appender.file.layout=org.apache.log4j.PatternLayout
log4j.appender.file.layout.ConversionPattern=%d{ABSOLUTE} %-5p [%c{1}] %m%n
log4j.appender.file.ImmediateFlush=true
log4j.appender.file.DatePattern='.'yyyy-MM-dd


# Tomcat logging
log4j.logger.org.apache.catalina=WARN

# DON'T EDIT FOLLOWING
log4j.logger.com.vaau.commons.springframework.context.ContextLifecycleListener=INF
O

#VAAU commons logging
log4j.logger.com.vaau.commons=WARN

#RBACx Core logging
log4j.logger.com.vaau.rbacx= WARN
log4j.logger.com.vaau.rbacx.core= WARN
log4j.logger.com.vaau.rbacx.service= WARN
log4j.logger.com.vaau.rbacx.manager= WARN
```

```
# RBACx Security logging
log4j.logger.com.vaau.rbacx.security=WARN

#RBACx Scheduling logging
log4j.logger.com.vaau.rbacx.scheduling=DEBUG

# RBACx ETL
log4j.logger.com.vaau.rbacx.etl.manager=WARN

#RBACx IAM logging
log4j.logger.com.vaau.rbacx.iam= DEBUG

#RBACx Reporting logging
log4j.logger.com.vaau.rbacx.reporting=WARN

#RBACx Audit logging
log4j.logger.com.vaau.rbacx.audit=WARN

# RBACx IDC logging
log4j.logger.com.vaau.rbacx.idc=WARN

# SYSTEM
log4j.logger.com.vaau.rbacx.system=DEBUG

# Sandbox
log4j.logger.com.vaau.rbacx.sandbox.ida=WARN
log4j.logger.com.vaau.rbacx.sandbox.rme=WARN

# Workflow
log4j.logger.com.vaau.rbacx.workflow=WARN
log4j.logger.com.opensymphony.workflow.AbstractWorkflow=ERROR

# SqlMap logging configuration. Change WARN to DEBUG if want to see all sql
statements
log4j.logger.com.ibatis=WARN
log4j.logger.com.ibatis.common.jdbc.SimpleDataSource=WARN
log4j.logger.com.ibatis.common.jdbc.ScriptRunner=WARN
log4j.logger.com.ibatis.sqlmap.engine.impl.SqlMapClientDelegate=WARN
log4j.logger.org.springframework.jdbc.datasource.DataSourceTransactionManager=WARN
log4j.logger.java.sql.Connection=WARN
log4j.logger.java.sql.Statement=WARN
log4j.logger.java.sql.PreparedStatement=WARN

#Spring Framework
log4j.logger.org.springframework=WARN
log4j.logger.org.springframework.rules.values=WARN
log4j.logger.org.springframework.context.support=WARN
log4j.logger.org.springframework.transaction=WARN
log4j.logger.org.springframework.aop.interceptor=WARN
log4j.logger.org.springframework.security=WARN
log4j.logger.org.springframework.security.event.authentication.LoggerListener=FATA
L

# For Trace Logging change them TRACE
log4j.logger.org.springframework.aop.interceptor.PerformanceMonitorInterceptor=WAR
N
log4j.logger.org.springframework.aop.interceptor.CustomizableTraceInterceptor=WARN

##JIAM log
```

```
log4j.category.com.ca=WARN
#log4j.category.com.ca.commons.jndi=DEBUG

#Quartz scheduler
log4j.logger.org.quartz=WARN

#DWR
log4j.logger.uk.ltd.getahead.dwr=FATAL
log4j.logger.org.directwebremoting=FATAL

#ehcache
log4j.logger.net.sf.ehcache=ERROR

#CloverETL
log4j.logger.org.jetel=ERROR

#C3p0
log4j.logger.com.mchange=ERROR

# JasperReports
log4j.logger.net.sf.jasperreports=ERROR
log4j.logger.com.vaau.rbacx.search=WARN
log4j.logger.com.vaau.commons.search=WARN
```

16
Using System Logs

This chapter contains the following sections:

16.1 Overview

This chapter provides guidance about messages that should be monitored in order to maintain system performance. Examples show the type of function, the message severity, the module name, and the log message.

16.2 Tomcat Logging

Tomcat logging captures messages related to the Tomcat application server.

All Tomcat-related errors are shown in the following manner in the log file. Monitor anything that contains this string:

[org.springframework.web.context.ContextLoader]

```
15:11:56,500 ERROR [org.springframework*] **
15:11:56,500 FATAL [org.springframework*] **
```

Note -

* Refers to the specific module.

** Refers to the actual error message.

Examples are shown in the subsections below.

16.2.1 Context Initialization

The following error is a context initialization error that can occur when Oracle Identity Analytics starts. The error indicates that there is a context initialization failure, and the log message indicates which file caused the error.

In the following sample error message, the `job.xml` file under `WEB-INF` has caused the error.

```
Severity: ERROR

Module name: ContextLoader

Log message:

15:11:56,500 ERROR [org.springframework.web.context.ContextLoader] Context
initialization failed

org.springframework.beans.factory.BeanCreationException: Error creating bean with
name 'usersImportTrigger' defined in ServletContext resource [/WEB-INF/jobs.xml]:
Error setting property values; nested exception is
org.springframework.beans.PropertyAccessExceptionsException:
PropertyAccessExceptionsException (1 errors); nested propertyAccessExceptions are:
[org.springframework.beans.MethodInvocationException: Property 'cronExpression'
threw
exception; nested exception is java.text.ParseException: '?' can only be specfied
for
Day-of-Month or Day-of-Week.]

PropertyAccessExceptionsException (1 errors)
```

In the following example, the log message shows that the `scheduling-context.xml` file under `WEB-INF` has caused the error. The log message also shows the line in the file that caused the error.

```
Severity: ERROR

Module name: ContextLoader

Log message:

15:22:03,109 ERROR [org.springframework.web.context.ContextLoader]
Context initialization failed

org.springframework.beans.factory.BeanDefinitionStoreException: Line 137 in XML
document from ServletContext resource [/WEB-INF/scheduling-context.xml] is
invalid;
nested exception is org.xml.sax.SAXParseException: The string "--" is not
permitted
within comments.
```

16.3 VAAU Commons Logging

VAAU Commons logging captures messages having to do with component interactions within Oracle Identity Analytics.

VAAU Commons errors are shown as follows in the log file. For monitoring purposes, monitor anything that contains `[com.vaau.commons]`.

```
15:11:56,500 ERROR [com.vaau.commons*] **
15:11:56,500 FATAL [com.vaau.commons*] **
```

Note -

* Refers to the specific module.

** Refers to the actual error message.

Examples are shown in the subsections below.

16.3.1 Context Initialization

The following example contains information about Oracle Identity Analytics. The log message shows the version of Oracle Identity Analytics that is running and the application status.

```
Severity: INFO

Module name: ContextLifecycleListener

Log message:

10:30:19,859 INFO
[com.vaau.commons.springframework.context.ContextLifecycleListener]
Oracle Identity Analytics (build: 5.1.0.20080903_406_3061) Started
```

16.4 Oracle Identity Analytics Core Logging

Oracle Identity Analytics Core logging logs messages having to do with core Oracle Identity Analytics events.

This section provides sample Oracle Identity Analytics core logging messages. For monitoring purposes, monitor anything that contains [`com.vaau.rbacx`].

```
15:11:56,500 ERROR [com.vaau.rbacx *] **
15:11:56,500 FATAL [com.vaau.rbacx *] **
15:11:56,500 ERROR [com.vaau.rbacx.service *] **
15:11:56,500 FATAL [com.vaau.rbacx.service *] **
15:11:56,500 ERROR [com.vaau.rbacx.core*] **
15:11:56,500 FATAL [com.vaau.rbacx.core*] **
15:11:56,500 ERROR [com.vaau.rbacx.manager*] **
15:11:56,500 FATAL [com.vaau.rbacx.manager *] **
```

Note -

* Refers to the specific module.

** Refers to the actual error message.

Examples are shown in the subsections below.

16.4.1 Sequence Update

The following message shows Oracle Identity Analytics back-end activities. The log messages show that Oracle Identity Analytics is updating the sequence table in the database.

```
Severity: DEBUG

Module name: SequenceGeneratorServiceImpl
```

```
Log message:

13:22:35,203 DEBUG [com.vaau.rbacx.service.impl.SequenceGeneratorServiceImpl]
Getting MemorySequence for sequence name NamespaceKey

13:22:35,203 DEBUG [com.vaau.rbacx.service.impl.SequenceGeneratorServiceImpl]
Creating new MemorySequence for sequence name NamespaceKey

13:22:35,203 DEBUG [com.vaau.rbacx.dao.ibatis.SqlMapSequenceDao]
Getting next count for sequenceName=NamespaceKey, increment=10

13:22:35,218 DEBUG [com.vaau.rbacx.dao.ibatis.SqlMapSequenceDao]
Returning next count for sequenceName=NamespaceKey, count=1010

13:22:35,234 DEBUG [com.vaau.rbacx.service.impl.SequenceGeneratorServiceImpl]
Returning count for sequence name Name
```

16.5 Oracle Identity Analytics Security Logging

Oracle Identity Analytics Security logging logs events related to security, including user creation events, and login and logout events.

Oracle Identity Analytics security logging errors are logged as shown here. For monitoring purposes, monitor anything that contains [`com.vaau.rbacx.security`].

```
15:11:56,500 ERROR [com.vaau.rbacx.security *] **
15:11:56,500 FATAL [com.vaau.rbacx.security *] **
```

Note -

* Refers to the specific module.

** Refers to the actual error message.

Examples are shown in the subsections below.

16.5.1 Login Error

The following message shows a Oracle Identity Analytics security warning. The warning indicates that the user's login or password is incorrect.

```
Severity: WARN

Module name: UserManagerImpl

Log message:

14:14:45,359 WARN [com.vaau.rbacx.security.manager.impl.UserManagerImpl]
RbacxUser with username: 'testuser' not found
```

16.5.2 User Creation

The following message shows that the user `testuser` has been created.

```
Severity: DEBUG

Module name: RbacxSecurityServiceImpl

Log message:
```

```
15:35:00,750 DEBUG
[com.vaau.rbacx.security.service.impl.RbacxSecurityServiceImpl]
adding user testuser

15:35:00,750 DEBUG
[com.vaau.rbacx.security.manager.impl.UserManagerImpl]
creating user: Last name: User; First name: Test; Email: testuser@oracle.com

15:35:00,765 DEBUG
[com.vaau.rbacx.security.manager.impl.UserManagerImpl]
setting credentials for testuser: 3dbb4a67672880904958500b68d4ab481116a1b9
```

16.5.3 User Deletion

The following user deletion message shows that the user `testuser` has been deleted.

```
Severity: DEBUG

Module name: RbacxSecurityServiceImpl

Log message:

15:34:23,359 DEBUG [com.vaau.rbacx.security.service.impl.RbacxSecurityServiceImpl]
deleting user testuser

15:34:23,375 DEBUG [com.vaau.rbacx.security.manager.impl.UserManagerImpl]
deleting user: Last name: user; First name: test; Email: testuser@oracle.com
```

16.6 Oracle Identity Analytics Scheduling Logging

Oracle Identity Analytics Scheduling logging logs messages related to the scheduler component.

This section shows example Oracle Identity Analytics scheduling error messages. For monitoring purposes, monitor anything that contains `[com.vaau.rbacx.scheduling]`.

```
15:11:56,500 ERROR [com.vaau.rbacx.scheduling *] **
15:11:56,500 FATAL [com.vaau.rbacx.scheduling *] **
```

Note -

* Refers to the specific module.

** Refers to the actual error message.

Examples are shown in the subsections below.

16.6.1 Scheduled Certification Reminder

The following message shows the information for a scheduled execution. The message shows that a certification reminder has executed as scheduled.

```
Severity: INFO

Module name: VaauSchedulerEventListenerImpl

Warn message:

14:19:00,187 INFO
```

```
[com.vaau.rbacx.scheduling.impl.VaauSchedulerEventListenerImpl]
Job executed: Certification Reminder, SYSTEM
```

16.6.2 Scheduled Account Import Job

The following message shows the information for a scheduled execution. The message shows that an account import job has executed as scheduled.

```
Severity: DEBUG

Module name: IAMJob

Warn message:

14:21:00,062 DEBUG
[com.vaau.rbacx.scheduling.manager.providers.quartz.jobs.IAMJob]
Accounts Import job executed successfully = true
```

16.7 Oracle Identity Analytics Identity Access Management (IAM) Logging

Oracle Identity Analytics Identity Access Management (IAM) logging logs events based on activity between Oracle Identity Analytics and an Identity Access Management (IAM) server. This includes any file-based imports that occur inside Oracle Identity Analytics.

This section shows example Oracle Identity Analytics IAM (Identity Access Management) errors. For monitoring purposes, monitor anything that contains `[com.vaau.rbacx.iam]`.

```
15:11:56,500 ERROR [com.vaau.rbacx.iam *] **
15:11:56,500 FATAL [com.vaau.rbacx.iam *] **
```

Note -

* Refers to the specific module.

** Refers to the actual error message.

Examples are shown in the subsections below.

16.7.1 User Import

The following message shows an error from a user file import. The error indicates that there is a data type violation. The first column in the schema file is specified by `statusKey`, and in the user file, it has `Active` corresponding to the `statusKey`. The `statusKey`, however, is defined to be either `1` as active, or `2` as inactive. The correct data type corresponding to the statusKey should be either `1` or `2`.

```
Severity: ERROR

Module name: UserFileReader

Log message:

11:29:00,593 ERROR [UserFileReader] PropertyAccessExceptionsException (1 errors)

Schema file:

statusKey,manager,primaryEmail,firstName,middleName,username

User file imported with error:
```

```
Active,testmanager,testuser@email.com,Test,User,testuser

Correct user file:

1,testmanager,testuser@email.com,Test,User,testuser
```

16.7.2 Account Import

The following message shows an account file import error. The error indicates that the account file does not match the schema file. The schema file shows that one role will be imported to the account. However, the account file has two roles. Instead of importing two roles as two attributes, import the two roles into the `role` attribute as a single attribute.

```
Severity: ERROR

Module name: CSVAccountFileReader

Log message:

11:53:02,625 ERROR [CSVAccountFileReader] BAD RECORD FORMAT:
File: UNX_01_accounts, line no. 1, doesn't match schema,
found [testuser,JOB_1,JOB_2,UNX]

Schema file:

name<CorrelationKey>,role,endpoint

Account file imported with error:

testuser,JOB_1,JOB_2,UNX

Correct user file:

testuser,"JOB_1,JOB_2",UNX
```

16.7.3 Unknown User

In this example of an account file import error, the error indicates that the user of the account file does not match any users in the database. In this case, configure the system to either drop the account or to correlate to a default global user.

```
Severity: ERROR

Module name: CSVAccountFileReader

Log message:

12:12:01,015 ERROR
[CSVAccountFileReader] CORRELATION ERROR: Unknown global user 'test-user' for
account 'test-user'

Schema file:

name<CorrelationKey>,role,endpoint

Account file imported with error:

test-user, "JOB_1,JOB_2",UNX
```

```
Correct user file:

testuser,"JOB_1,JOB_2",UNX
```

16.8 Oracle Identity Analytics Reports Logging

Oracle Identity Analytics Reports logging logs events related to the running of reports inside Oracle Identity Analytics.

All Oracle Identity Analytics reporting-related errors will be shown in the following manner. For monitoring purposes, monitor anything that contains `[com.vaau.rbacx.reporting]`.

```
15:11:56,500 ERROR [com.vaau.rbacx.reporting *] **
15:11:56,500 FATAL [com.vaau.rbacx.reporting *] **
```

Note -

* Refers to the specific module.

** Refers to the actual error message.

Examples are shown in the subsections below.

16.8.1 Generating Reports

The following example shows the information that is logged when reports are generated. The log messages show the type of report that is generated and the location of the file.

```
Severity: DEBUG

Module name: JasperReportsUtils

Log message:

10:33:09,390 DEBUG
[com.vaau.rbacx.reporting.renderer.jasperreports.JasperReportsUtils] --->
checking if 'C:\Vaau\rbacx-4.0\reports\BusinessUnitUsers.jrxml' has
any sub-reports that need compiling

10:33:09,406 DEBUG
[com.vaau.rbacx.reporting.renderer.jasperreports.JasperReportsUtils] --->
C:\Vaau\rbacx-4.0\reports\BusinessUnitUsers.jrxml has following
sub-reports --> []

10:33:09,406 DEBUG
[com.vaau.rbacx.reporting.renderer.jasperreports.JasperReportsUtils] --->
following sub-reports require compilation []

10:33:09,406 DEBUG
[com.vaau.rbacx.reporting.renderer.jasperreports.JasperReportsUtils]
checking if report file --> 'C:\Vaau\rbacx-4.0\reports\BusinessUnitUsers.jrxml'
requires compilation

10:33:09,406 DEBUG
[com.vaau.rbacx.reporting.renderer.jasperreports.JasperReportsUtils] --->
compiling reports []
```

16.9 Oracle Identity Analytics Audit Logging

Oracle Identity Analytics Audit logging logs auditing events inside Oracle Identity Analytics, such as login and logout events and changes made inside Oracle Identity Analytics.

The following example messages show audit-related errors. For monitoring purposes, monitor anything that contains `[com.vaau.rbacx.rbacxaudit]`.

```
15:11:56,500 ERROR [com.vaau.rbacx.rbacxaudit *] **
15:11:56,500 FATAL [com.vaau.rbacx.rbacxaudit *] **
```

Note -

* Refers to the specific module.

** Refers to the actual error message.

Examples are shown in the subsections below.

16.9.1 Audit Logging

These example messages show the information that is logged when users log in to or log out of Oracle Identity Analytics. The log also captures changes made in Oracle Identity Analytics.

```
Severity: DEBUG
Module name: RbacxAuditUtil
Log message:
10:33:09,390 DEBUG [com.vaau.rbacx.rbacxaudit.util.RbacxAuditUtil] ---> User
"testuser" logged in
```

16.10 Oracle Identity Analytics Identity Certification (IDC) Logging

Oracle Identity Analytics Identity Certification (IDC) logging logs events related to the Oracle Identity Analytics Identity Certification component.

Identity certification (IDC) errors are shown as follows in the log file. For monitoring purposes, monitor anything that contains `[com.vaau.rbacx.idc]`.

```
15:11:56,500 ERROR [com.vaau.rbacx.idc *] **
15:11:56,500 FATAL [com.vaau.rbacx.idc *] **
```

Note -

* Refers to the specific module.

** Refers to the actual error message.

Examples are shown in the subsections below.

16.10.1 Certification Reminder

This message shows the number of certification reminders that have fired.

```
Severity: DEBUG

Module name: ReminderManagerImpl

Log message:

12:43:00,171 DEBUG [ReminderManagerImpl] No. of first certification
reminders = 19
```

```
12:43:00,171 DEBUG [ReminderManagerImpl] No. of second certification
reminders = 0

12:43:00,171 DEBUG [ReminderManagerImpl] No. of third certification
reminders = 0

12:43:00,171 DEBUG [ReminderManagerImpl] No. of fourth certification
reminders = 0

12:43:00,171 DEBUG [ReminderManagerImpl] No. of fifth certification
reminders = 0

12:43:00,171 DEBUG [ReminderManagerImpl] [finished] firing certification
reminders, took 31ms
```

16.10.2 Certification Creation, Example 1

The following message shows certification information. The messages show that the users and the accounts involved in the certification are not being created because the users or the accounts are not active.

```
Severity: DEBUG

Module name: RbacxIDCServiceImpl

Log message:

16:20:59,375 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
creating full certification 'T2'

16:20:59,390 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
loading global users from business units --> [3066]

16:20:59,453 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
loaded 2 GlobalUsers, took 63ms

16:20:59,453 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
creating IDC Users...

16:20:59,500 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
loading Accounts, Roles and Policies for 2 users

16:20:59,515 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
loaded Accounts, Roles and Policies for 2 users, took 15ms

16:20:59,515 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
--> user: ZRC0217

16:20:59,546 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
----> user 'ZRC0217' has no accounts to certify

16:20:59,546 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
---> user Craig, Ryan has not accounts, and will not inlcluded

16:20:59,546 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
--> user: ZTJ0071

16:20:59,546 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
----> user 'ZTJ0071' has no accounts to certify
```

```
16:20:59,546 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
---> user Jorgensen, Thomas has not accounts, and will not inlcluded

16:20:59,546 DEBUG [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
created 0 IDC Users , took 93ms
```

16.10.3 Certification Creation, Example 2

In this example, the message shows that the business unit involved in the certification is not being created because either the users or the accounts are not active.

```
Severity: ERROR

Module name: RbacxIDCServiceImpl

Log message:

16:40:01,203 ERROR [com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl]
ERROR: unable to create certification: T3_Aaron Hackett - ZAH0140

com.vaau.rbacx.idc.IDCInvalidArgumentException: BusinessUnit 'Aaron Hackett -
ZAH0140' has no acitve users to certify

at com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl.
createCertification(RbacxIDCServiceImpl.java:511)

at com.vaau.rbacx.idc.service.impl.RbacxIDCServiceImpl.
createCertifications(RbacxIDCServiceImpl.java:256)

at com.vaau.rbacx.scheduling.executor.certification.
CertificationJobExecutor.execute(CertificationJobExecutor.java:22)

at com.vaau.rbacx.scheduling.manager.providers.quartz.
jobs.AbstractQuartzJob.execute(AbstractQuartzJob.java:58)

at org.quartz.core.JobRunShell.run(JobRunShell.java:191)

at org.quartz.simpl.SimpleThreadPool$WorkerThread.
run(SimpleThreadPool.java:516)
```

17

Oracle Identity Analytics Troubleshooting

This chapter contains the following sections:

17.1 Overview

This chapter lists solutions for common (and uncommon) system problems.

17.2 To Verify That Oracle Identity Analytics Started Properly

To verify that Oracle Identity Analytics started properly, do one of the following:

- Check the log file.

  A successful launch of Oracle Identity Analytics is recorded in the application log file, which is named `rbacx.log`. The entry listed in the log file includes the Oracle Identity Analytics version number and a time stamp that records when the application started.

  An example log entry is listed here:

  ```
  "17:27:11,218 INFO [ContextLifecycleListener] Oracle Identity Analytics (build:
  4.1.0.20080903_406_3061) Started"
  ```

- Open the application in a browser.

  You can verify that Oracle Identity Analytics started correctly by typing `http://localhost:9080/rbacx` in a browser on the local application server machine.

  The *localhost* portion of the URL assumes that you are checking the application from the local application server (that is, you are not checking from a remote machine). The URL also assumes that Oracle Identity Analytics is deployed on TCP port `9080`.

  If you are opening the URL from a remote machine, format the URL as follows:

  `http://`*<application server hostname>*`:`*<port>*`/rbacx`

17.3 To Start / Stop Oracle Identity Analytics

Start and stop Oracle Identity Analytics using the Application Control Panel of your application server. For example, if you are using the Glassfish™ application server, use the Administrative Console to start and stop Oracle Identity Analytics.

17.4 Troubleshooting Common Errors

This section describes solutions to errors that are commonly encountered when working with Oracle Identity Analytics.

17.4.1 JDBC Connection Error

This error occurs when Oracle Identity Analytics is unable to connect to the database. The error is logged in the `rbacx.log` file.

```
Failed to obtain DB connection from data source
'springNonTxDataSource.QuartzScheduler': java.sql.SQLException:
Connections could not be acquired from the underlying database!
[ See nested exception: java.sql.SQLException: Connections
could not be acquired from the underlying database!  ]
```

17.4.1.1 To Resolve the Error

- Check the `jdbc.properties` configuration file in the *$RBACX_HOME*`/conf` folder.
- Check the `conf-context.xml` file in the `/WEB-INF/` folder.
- Ensure that JDBC drivers corresponding to the database type are present in `/WEB-INF/lib`.
- Verify that database server connectivity can be established from the application server.

17.4.2 Error Loading Workflow

The following error occurs when the `workflows.xml` file is not configured properly in the `/WEB-INF/classes` folder.

```
Error loading workflow Role Membership Workflow
com.opensymphony.workflow.FactoryException:
Error in workflow descriptor: [file:/]
<WORKFLOWS_FILE_PATH>role-user-membership-workflow.xml:
root cause: <$RBACX_HOME>\conf\workflows\role-user-membership-workflow.xml
(The device is not ready)
```

17.4.2.1 To Resolve the Error

Verify that the `$RBACX_HOME` variable in `workflows.xml` in `/WEB-INF/classes` is set correctly.

17.4.3 Error Rendering Report

The following error is generated when Oracle Identity Analytics reports cannot be rendered by the system:

```
20:44:43,498 ERROR [JasperPrintRenderer] Error rendering report:
java.io.FileNotFoundException:<$FILE_PATH>\<$FILE_NAME>.jasper
```

17.4.3.1 To Resolve the Error

- Validate the file path listed in `reporting-context.xml`.
- Verify that the report being rendered (<*$FILE_NAME*>`.jasper`) exists in the reports folder.

17.4.4 Oracle Identity Analytics Configuration Error

Any inaccuracies in the Oracle Identity Analytics configuration would generate errors and cause Oracle Identity Analytics not to launch. Two common files where configuration errors can cause failure are `conf-context.xml` and `reporting-context.xml`.

Some of the common errors are listed here:

```
java.io.FileNotFoundException: C:\Vaau\rbacx-4.1\conf\jdbc.properties
(The system cannot find the path specified)
java.io.FileNotFoundException: C:\Vaau\rbacx-4.1\conf\mail.properties
(The system cannot find the path specified)
java.io.FileNotFoundException: C:\Vaau\rbacx-4.1\conf\ldap.properties
(The system cannot find the path specified)
java.io.FileNotFoundException: C:\Vaau\rbacx-4.1\conf\iam.properties
(The system cannot find the path specified)
```

17.4.4.1 To Resolve the Error

Verify that the `$RBACX_HOME` path outlined in `conf-context.xml` and `reporting-context.xml` is accurate.

17.4.5 Java Heap Out of Memory Error

The `java.lang.OutOfMemoryError` exception in the log is caused by Java heap fragmentation. This fragmentation occurs when no contiguous chunk of free Java heap space is available from which to allocate Java objects.

17.4.5.1 To Resolve the Error

Increase the size of the JVM™ memory pool and clear out the Java cache. The recommended setting for min. / max. value is 1024 MB / 2048 MB, respectively.

17.4.6 RACF Account Import Error

Importing RACF accounts from a file fails when running OIA on WebLogic. The following error is logged:

```
Error reading object from byte stream
```

17.4.6.1 To Resolve the Error

1. Go to the following location and open `iam.properties` in a text editor:

   $RBACX_HOME`/conf/iam.properties`

2. Locate the following line in `iam.properties` and change the value from `5` to `0`:

   Old value for WebLogic:

   ```
   com.vaau.rbacx.iam.file.import.sharedAttributesCompressionLevel=5
   ```

   New value for WebLogic:

   ```
   com.vaau.rbacx.iam.file.import.sharedAttributesCompressionLevel=0
   ```

3. Restart the server and try the account import again.

18

Tuning Server Configuration Properties

This chapter contains the following sections:

- Section 18.1, "Overview"
- Section 18.2, "Configuring Identity Certification Settings on the Server"

18.1 Overview

This chapter includes configuration settings that you can modify to fine-tune system performance.

18.2 Configuring Identity Certification Settings on the Server

You can configure the maximum number of records that the Oracle Identity Analytics server will process in a single batch when performing identity certification. If the batch size is set too high, system performance is adversely affected and the certification process may run out of memory. If batch sizes are set too low, certification times may take longer.

> **Note:** To configure the maximum number of records that users see on screen when viewing certifications on the My Certifications screen, modify batching in the UI.
>
> See "Configuring the Maximum Number of Identity Certification Records That Should Display in the UI" in the "Customizing the Oracle Identity Analytics User Interface" chapter in the *System Integrator's Guide for Oracle Identity Analytics*.

18.2.1 To Modify Identity Certification Batch Sizes on the Server

1. Open the `idc.properties` file located in *$RBACX_WAR*`/conf` to configure how many identity certification records will be processed in a batch.
2. Scroll to the section that says `IDC Server side 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.certification.usersBatchSize` key and change the numeric value up or down.

- For resource entitlement certifications, find the `com.vaau.rbacx.idc.certification.resourcesBatchSize` key and change the numeric value up or down.

4. Save the file.