

Oracle Identity Analytics Business Administrator's Guide

11g Release 1

Copyright © 2010, Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

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

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

| | |
|-------------------------------------------------------------|----|
| Preface | 9 |
| 1 Oracle Identity Analytics Identity Warehouse | 11 |
| Working With Resources | 11 |
| To Create or Modify Resources | 12 |
| To Delete Resources | 12 |
| Working With Applications | 12 |
| To Create Applications | 12 |
| To Schedule a Job for Assigning Users to Applications | 13 |
| Working With Extended User Custom Properties | 14 |
| To Enable Extended User Custom Properties | 14 |
| Working With Orphan Accounts | 15 |
| To Assign an Orphan Account to a User | 15 |
| Creating Business Structure Rules | 15 |
| To Create Business Structure Rules | 15 |
| To Preview Results Of A Business Structure Rules Job | 16 |
| To Run Business Structure Rules Job | 17 |
| To Edit Business Structure Rules | 18 |
| 2 Oracle Identity Analytics Importing | 19 |
| Understanding the Import Process | 19 |
| Importing Users | 20 |
| Importing Accounts | 20 |
| Importing Roles | 22 |
| Importing Policies | 23 |
| Importing Business Structures | 24 |
| Importing Glossary Definitions | 24 |

| | |
|-------------------------------------------------------|-----------|
| Scheduling Import and Export Jobs | 25 |
| Configuring the Import Process | 25 |
| Verifying Imports | 26 |
| To Verify Success of Imports From the Front-End | 26 |
| To Verify Success of Import From the Back-End | 27 |
| 3 Oracle Identity Analytics ETL Process | 29 |
| Introduction | 29 |
| Transformation Process | 29 |
| Transformation Graphs | 30 |
| Oracle Identity Analytics CloverETL Extensions | 32 |
| Oracle Identity Analytics ETL Reference | 33 |
| DelimitedDataReader and DelimitedDataWriter | 33 |
| ExcelDataReader | 33 |
| Transformation Examples | 34 |
| Merge | 34 |
| Filter | 35 |
| Fixed Length Data Reader | 36 |
| Database Input | 37 |
| Load and Unload Data From the Database | 42 |
| How CloverETL Works With Databases | 42 |
| DBConnection | 42 |
| Using the AnalyzeDB Utility | 46 |
| DBInputTable Component | 47 |
| DBOutputTable Component | 48 |
| Executing SQL/DML/DDDL Statements against DB | 50 |
| CloverETL DataRecord Reference | 52 |
| How Data is Represented Within CloverETL | 52 |
| Supported Data Field Types | 52 |
| Specification of Record Format | 53 |
| Delimiters | 53 |
| Field Formats and Other Features | 54 |
| Specifying Default Values for Fields | 57 |

| | |
|---------------------------------------------------------------------------------|----|
| 4 Oracle Identity Analytics Data Correlation | 59 |
| Understanding Data Correlation | 59 |
| Writing Correlation Rules | 59 |
| Example | 60 |
| Pattern Matching Scenarios | 61 |
| Manual Correlation | 62 |
| To Correlate an Orphan Account to a User | 62 |
| To Change Ownership of an Account | 63 |
| | |
| 5 Oracle Identity Analytics Role Engineering and Management | 65 |
| Understanding Role Mining, Role Consolidation, and Entitlements Discovery | 65 |
| Role Mining | 65 |
| Role Consolidation | 66 |
| Entitlements Discovery | 66 |
| Performing Role Mining | 66 |
| Setting Role Mining Attributes | 66 |
| Creating a Role Mining Task | 67 |
| Running or Scheduling a Role Mining Task | 70 |
| Validating and Saving Role Mining Results | 71 |
| Performing Role Consolidation | 74 |
| To Consolidate Roles | 74 |
| Performing Entitlements Discovery | 75 |
| To Perform Entitlements Discovery | 75 |
| Creating and Using Role Provisioning Rules | 76 |
| To Create New Rules | 76 |
| To Approve/Reject Role Provisioning Rules | 77 |
| To Deactivate or Decommission Rules | 77 |
| To Preview Role Provisioning Rules Job | 78 |
| To Run Role Provisioning Rules Job | 79 |
| To Manage Lifecycle of Rules | 79 |
| | |
| 6 Oracle Identity Analytics Workflows | 81 |
| Understanding Workflows | 81 |
| To View a Workflow | 81 |
| Types of Workflows in Oracle Identity Analytics | 82 |

| | |
|----------------------------------------------------------------------|------------|
| Understanding the Edit Workflow Page | 82 |
| Designing Workflows | 83 |
| To Add a Step in a Workflow | 83 |
| To Delete a Step | 84 |
| To Edit Workflow Action Details | 85 |
| 7 Oracle Identity Analytics Identity Certifications | 87 |
| Creating New Certifications | 87 |
| To Create a User Entitlement Certification | 88 |
| To Create a Role Entitlement Certification | 89 |
| To Create a Resource Entitlement Certification | 90 |
| To Create a Data Owner Certification | 91 |
| Understanding the Incremental Certification Option | 92 |
| Scheduling Certifications | 93 |
| To Schedule a Certification | 93 |
| To Delete a Certification Job | 93 |
| Understanding Closed-Loop Remediation and Remediation Tracking | 94 |
| Configuring Closed-Loop Remediation | 94 |
| To Track Remediation | 95 |
| 8 Oracle Identity Analytics Identity Audit | 97 |
| Working With Audit Rules | 97 |
| Impact of Rule Condition Modifications | 97 |
| Impact of Adding / Removing Rules in a Policy | 98 |
| To Create Audit Rules | 98 |
| To Edit / Change the State of an Audit Rule | 99 |
| Working With Audit Policies | 99 |
| To Create Audit Policies | 99 |
| To Edit / Change the State of an Audit Policy | 100 |
| To Preview Audit Policy Scan Results | 100 |
| To Run An Audit Policy | 101 |
| 9 Oracle Identity Analytics Reports | 103 |
| Working With Custom Reports | 103 |

| | | |
|-----------|-----------------------------------------------------------------------------------------|------------|
| | To Upload a Custom Report Template in Oracle Identity Analytics | 104 |
| | To Run a Custom Report | 104 |
| 10 | Oracle Identity Analytics Scheduling | 105 |
| | Scheduling Import and Export Jobs in Oracle Identity Analytics | 105 |
| | To Schedule an Import and Export Job Using the User Interface | 105 |
| | Scheduling a Job by Editing the Configuration Files | 106 |
| | To Enable a Job by Editing the Configuration Files | 108 |
| | To Schedule a Job by Editing the Configuration Files | 109 |
| | Sample Cron Expressions | 111 |
| | Scheduling Other Job Types | 112 |
| 11 | Oracle Identity Analytics Configuration | 115 |
| | System Configuration | 115 |
| | Proxy Assignment Notification | 115 |
| | Mail Server Settings | 115 |
| | OIA Server Settings | 115 |
| | Resource Types Configuration | 116 |
| | To Create, Rename, and Delete a Resource Type | 116 |
| | Understanding Resource Type Attributes and Attribute Categories | 117 |
| | To Create, Rename, and Delete an Attribute Category | 117 |
| | Configuring Resource Type Attributes | 117 |
| | To Create, Rename, Edit, and Delete an Attribute | 118 |
| | Provisioning Servers Configuration | 119 |
| | To Create a New Provisioning Server Connection | 119 |
| | Identity Certification Configuration | 122 |
| | To Configure Identity Certification | 122 |
| | Completing the Certification Configuration Form "General" Section | 122 |
| | To Complete the Certification Configuration Form "Status Options" Section | 124 |
| | To Complete the Certification Configuration Form "Reminders" Section | 125 |
| | To Complete the Certification Configuration Form "Revoke and Remediation" Section | 125 |
| | Role Management Configuration | 126 |
| | To Configure Mining | 126 |
| | To Configure Roles | 126 |
| | Identity Audit Configuration | 127 |

| | |
|------------------------------------------------------------------------|------------|
| To Configure Identity Audit | 127 |
| To Configure E-Mails for Violation Reminder and Escalation | 127 |
| To Configure E-mails For Violation Lifecycle Event Notifications | 128 |
| Reports Configuration | 128 |
| To Configure Report Reminder E-mails | 128 |
| E-mail Templates Configuration (Configuring E-mail Notification) | 129 |
| To Create and Configure E-mail Notifications | 129 |
| E-mail Parameters Definitions | 129 |
| Import/Export | 131 |
| Workflows Configuration | 132 |
| Event Listeners Configuration | 132 |
| To Create a New Event Listener | 132 |
| 12 Oracle Identity Analytics Access Control | 135 |
| Oracle Identity Analytics Access Control Introduction | 135 |
| System Privileges | 137 |
| Business Privileges | 139 |
| Working With Oracle Identity Analytics Users And Roles | 140 |
| To Create OIA Roles | 140 |
| To Create, Update, and Delete an Oracle Identity Analytics User | 140 |
| Password Quality Settings | 141 |
| To Modify User Password | 141 |
| 13 Audit Event Log and Import-Export Log | 143 |
| Audit Event Log | 143 |
| To View Audit Log Events | 144 |
| To Export Audit Log Events to a Spreadsheet | 144 |
| Import-Export Log | 145 |
| To View Import and Export Log Events | 146 |
| To Export Import-Job Log Details to a Spreadsheet | 146 |

Preface

About This Guide

This guide provides detailed information about configuring and administering the role management and compliance functionality available in Oracle® Identity Analytics 11gR1 software.

Who Should Read This Guide

The *Oracle Identity Analytics 11gR1 Business Administrator's Guide* is written for administrators, compliance officers, and IT specialists.

- Business managers and users in a supervisory role who will use Oracle Identity Analytics 11gR1 to grant employees and partners access to applications, check for access violations, and so on should see the *Oracle Identity Analytics 11gR1 User's Guide*.
- System administrators and service providers who need information about how to monitor and administer the Oracle Identity Analytics software at a systems level should see the *Oracle Identity Analytics 11gR1 System Administrator's Guide*.
- Deployment engineers who are responsible for integrating Oracle Identity Analytics with other IT systems should see the *Oracle Identity Analytics 11gR1 System Integrator's Guide*.

Oracle Identity Analytics Identity Warehouse

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 *Oracle Identity Analytics 11gR1 User's Guide Identity Warehouse chapter*.

See the *Oracle Identity Analytics 11gR1 User's Guide* 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*

Working With Resources

Resources are instances of a resource type. A resource type can have multiple resources assigned to it. For example, an Oracle® resource can have various databases as resources.

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 endpoint.
 - **Comments** - Additional comments can be entered here.
5. Click Save.

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.

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.

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 *Searching for a User*.
8. Click Next.

The Attributes and Attribute Values page opens.
9. Click the Add Attribute button.

The Add Attribute Values window opens.
10. From the table select the resource types, resources, attribute names, and attribute values. Click OK.

You do not have to select from all four columns.
11. Click Next.

The summary page opens.
12. Click Create.

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 “Scheduling a Job by Editing the Configuration Files” on page 106

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.

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 the same way.

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.

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
```

See *To Modify User Labels* for more information.

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.

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 *Searching for a User*.
8. Click OK.

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.

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 *Searching For a User*.
 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 e-mail 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 [“To Preview Results Of A Business Structure Rules Job” on page 16](#).
 - **Run** - Means Oracle Identity Analytics runs the rule and saves the results. To run and save the results of the rule, see [“To Preview Results Of A Business Structure Rules Job” on page 16](#).
 - **View results** - Oracle Identity Analytics displays the results of the rule, after you have clicked preview or run.

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.

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.
 - a. 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.
 - a. Complete the form and click Next.
 - b. Review the summary and click Schedule.

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.

Oracle Identity Analytics Importing

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

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

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 by using the Oracle Waveset (Sun Identity Manager) Data Exporter feature (if using Oracle Waveset / Sun Identity Manager as a provisioning server). Oracle Identity Analytics inserts or updates data in the data warehouse, and archives all of the data feeds.

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

- User import
- Resource metadata import
- Resources import
- Account import
- Roles import
- Policies import
- Glossary import
- Business structure import

To execute import jobs, you must have the schema file and the input file.

Note - You can import resource metadata and resources only if Oracle Identity Analytics is integrated with Oracle Waveset (Sun Identity Manager). For more information on importing

resource metadata and resources, see “Integrating With Oracle Waveset (Sun Identity Manager)” in the *Oracle Identity Analytics System Integrator's Guide*.

Importing Users

Schema file - 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,fullname,street,city,state,zip,country
```

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

Input File - 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 `users <file number>`.

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

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

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\schemas`
 - For UNIX - `/opt/Oracle/OIA_11gR1/rbacx/import/schemas`
3. Schedule the import.

See “[Scheduling Import and Export Jobs in Oracle Identity Analytics](#)” on page 105 in the Oracle Identity Analytics Scheduling chapter for more information.
4. To Verify the Import, see “[Verifying Imports](#)” on page 26.

Importing Accounts

Schema file - 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. 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>"
```

username, endpoint, and domain are mandatory fields, whereas others are optional. The naming convention for the schema file is *<resource type's Short 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 previous example illustrates the list of attributes or entitlements that are defined for the LDAP resource type. The first entry has the name of the user account, and this is also the correlation or cross-reference key between user accounts and global users. The correlation key should have *<Correlation Key>* defined next to it. The resource refers to the target directories on the resource type. A list of entitlements used in LDAP are defined, and each entitlement is comma-separated from the other. If a custom entitlement from a resource type is to be imported, it can be defined in the schema file by adding the attribute in Oracle Identity Analytics and adding an entry in the schema file.

Input file — 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 files is *<resource type's Short Name>_<file number>_accounts*.

Sample content from this input file is shown here:

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

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 [“Scheduling Import and Export Jobs in Oracle Identity Analytics” on page 105](#) in the Oracle Identity Analytics Scheduling chapter for more information.
 4. To Verify the Import, see [“Verifying Imports” on page 26](#).

Importing Roles

Schema file - 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">,customProperty2<use=required defaultValue="No Role Owner">
```

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

Input file - 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 file name for the role import file needs to be roles <file number>. The contents of a sample mapped role import file are shown here:

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

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 [“Scheduling Import and Export Jobs in Oracle Identity Analytics” on page 105](#) in the Oracle Identity Analytics Scheduling chapter for more information.

Importing Policies

Schema file - 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 EndPointName and policyname fields are mandatory, whereas the other fields are optional. The naming convention for the schema file is *<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,Roles,policycomments,PolicyDescription,ldapGroups
```

Input file - 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 *<resource type's Short Name>_<filename>_policies*. The contents of a sample policy import file mapped are shown here:

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

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 [“Scheduling Import and Export Jobs in Oracle Identity Analytics”](#) on page 105 in the Oracle Identity Analytics Scheduling chapter for more information.

Importing Business Structures

Schema file - 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
```

Input file - 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 `businessstructure_<file number>`

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 “[Scheduling Import and Export Jobs in Oracle Identity Analytics](#)” on page 105 in the Oracle Identity Analytics Scheduling chapter for more information.

Importing Glossary Definitions

Schema file - The schema file for the glossary import is a standard .rbx file that needs to be located in the schema folder. Previously, glossary import did not require a schema file. 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,highPrivileged,classification,definition,comments
```

Input file - 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 *<resource type's Short Name>_glossary<file number>*.

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. Glossary import jobs can only be scheduled through the back-end. See [“Scheduling Import and Export Jobs in Oracle Identity Analytics” on page 105](#) in the Oracle Identity Analytics Scheduling chapter for more information.

Scheduling Import and Export Jobs

For information about scheduling import and export jobs, see [“Scheduling Import and Export Jobs in Oracle Identity Analytics” on page 105](#) in the Oracle Identity Analytics Scheduling chapter.

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.

| Property Name | Variable | Description | Default Value |
|----------------------------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Maximum Concurrent Imports | <code>com.vaau.rbacx.iam.file.import.maxConcurrentImports=2</code> | Specifies the number of files to import concurrently. | 2 |
| Maximum Errors Limit | <code>com.vaau.rbacx.iam.file.import.rowErrorsLimit=3</code> | Specifies the maximum number of errors per file before aborting the process. | 3 |
| Batch Size | <code>com.vaau.rbacx.iam.file.import.batchSize=100</code> | Specifies the number of records to read and process in a batch during an import. | 100 |
| Correlation Parameters | <code>com.vaau.rbacx.iam.correlation.dropOrphanAccounts=true</code> | 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 | <code>com.vaau.rbacx.iam.correlation.correlate=orphan</code> | 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 | <code>com.vaau.rbacx.iam.file.import.dropLocation=\$RBACX_HOME/import/in</code> | Specifies the location where the feeds to be imported are placed. | <code>\$RBACX_HOME/import/in</code> |
| Complete Location | <code>com.vaau.rbacx.iam.file.import.completeLocation=\$RBACX_HOME/import/complete</code> | Specifies the location where the input files are stored after processing. | <code>\$RBACX_HOME/import/complete</code> |
| Schema Location | <code>com.vaau.rbacx.iam.file.import.schemaLocation=\$RBACX_HOME/import/schema</code> | Specifies the location where the schema files are placed. | <code>\$RBACX_HOME/import/schema</code> |

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

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.

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 the *Audit Event Log and Import-Export Log* chapter.

Oracle Identity Analytics ETL Process

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.

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 the [“Transformation Graphs” on page 30](#).

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.

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.

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>
```

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.

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.

Phase

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

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`.

Transformation Configuration

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

| Property Name | Variable | Description |
|-----------------------|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ETL Graphs Location | <code>eTLManager.graphsLocation=\$RBACX_HOME/imports/etl/graphs</code> | Directory in which to place the CloverETL graph files. |
| ETL Drop Location | <code>eTLManager.dropLocation=\$RBACX_HOME/imports/etl/drop</code> | Directory in which to place data files that need transformation. |
| ETL Complete Location | <code>eTLManager.completeLocation=\$RBACX_HOME/imports/etl/complete</code> | All processed files are moved to this directory after the ETL Manager completes the processing of the file. |
| ETL Output Location | <code>eTLManager.outputLocation=\$RBACX_HOME/imports/drop</code> | 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. |

Oracle Identity Analytics ETL Reference

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

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}"/>
```

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" />
```

Transformation Examples

Merge

The following graph is executed when a file with the pattern `tss_ \w*_accounts[\.\w]*` is found in the drop location by the ETL Manager. 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>

```

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>

```

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>

```

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() + " ->ocured 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>
```

Load and Unload Data From the Database

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

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.

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.

| 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:

```
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:

```
<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.

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.

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.

| 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 datatypes.

```
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)
);

<?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>

```

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.

| JDBC Type | CloverETL Type | Conversion Performed |
|-----------|----------------|-----------------------------------------------------------------------------------------------------|
| Timestamp | Date | Date is converted to Timestamp, and the target is set using the <code>setTimestamp()</code> method. |

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

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 the “[DBConnection](#)” on [page 42](#) section.

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:

| Parameter | Meaning |
|------------------------|-----------------------------------------------|
| <code>-dbDriver</code> | JDBC driver to use |
| <code>-dbURL</code> | Database name (URL) |
| <code>-config</code> | Config or Property file containing parameters |
| <code>-user</code> | User name |
| <code>-password</code> | User's password |
| <code>-d</code> | Delimiter to use (a comma , is standard) |

| Parameter | Meaning |
|-----------|-----------------------------------------|
| -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"
```

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 the [“JDBC to CloverETL” on page 44](#)). 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:

```
<?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"/>
  </Phase>
</Graph>
```

```
<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.

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 [“CloverETL to JDBC” on page 45](#).

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 `DBOutputTable` `cloverFields` 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 |

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.

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,'Fores /
t,
Phil');
</SQLCode>
</Node>
</Phase>
</Graph>
```

CloverETL DataRecord Reference

This section provides additional information about the CloverETL DataRecord.

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.

Supported Data Field Types

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

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

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)

Naming

There 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.

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.

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>
```

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.

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.

Date

| 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 |
| z | Time zone | General time zone | Pacific Standard Time; PST; GMT-08:00 |
| Z | Time zone | RFC 822 time zone | -0800 |

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 |

Number

| 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'". |

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" />
```

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.

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.

Oracle Identity Analytics Data Correlation

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.

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.
- 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.

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.

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. |

| Rule | Result | Description |
|-----------------------------------------------------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>\$account.FirstName(-1.1)</code> | "J" | Deletes all characters after the first one from the left side of the <code>FirstName</code> . |
| <code>\$account.FirstName(-1.1)\$account.LastName</code> | "JCook" | Deletes all characters after the first one from the left side of the <code>FirstName</code> and inserts <code>LastName</code> . |
| <code>\$account.FirstName(-1.1)_\$account.LastName</code> | "J_Cook" | Deletes all characters after the first one from the left side of the <code>FirstName</code> and inserts an underscore and <code>LastName</code> . |

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.

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.

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.

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.

Oracle Identity Analytics Role Engineering and Management

This chapter describes how role mining works in Oracle Identity Analytics.

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.

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 bottom-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.

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

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.

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

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.

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.

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.

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 [“To Create a Role Mining Task” on page 67](#) later in this chapter.

- 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 available 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 [“Using the Role Mining Wizard Display Controls” on page 69](#) later in this chapter 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 [“Using the Mining Criteria Page” on page 69](#) 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 [“Using the Role Engineering Data Preview Page” on page 70](#) later in this chapter for more information.
- Click Run Later to schedule the task.

See “[Using the Role Engineering Data Preview Page](#)” on page 70 later in this chapter for help using the scheduler.

- Click Save & Exit to save the task without scheduling it.

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 “[Creating a Role Mining Task](#)” on page 67 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  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.

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 table describes parameters that you can set to tune the role mining process.

| | | |
|-------------------------------|----------------------------------------------|-----------------------------------------------------|
| Role Mining Parameters | 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. |

| | | |
|----------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HR Attributes | 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. |
|----------------------|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | | |
|----------------------------|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advanced Parameters | Ignore attributes with a frequency lower than - . | Attributes might not be relevant if the frequency they show is low and they might introduce noise. 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). |
| | Consider subtree raising | Another mechanism to simplify the classification model (smaller number of final roles). |
| | Unpruned | Generates a more complex decision tree (later decomposed into more rules) |

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 [“Creating a Role Mining Task” on page 67](#).

- 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.

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.

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. Do one of the following tasks:
 - In the Action column, click Run to run a given task now.
 - Click Schedule to open the schedule for a task.
 - 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.

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.

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 "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 the [“Using the Role Mining Results Page”](#) on [page 72](#) for information about this page.

Using the Role Mining Results Page

This section describes the Role Mining Results page. To open this page, see *To Validate and Adjust Role Mining 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.

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.

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:

| | |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| % of users correctly / incorrectly assigned | This mining statistic tells what percentage of users has been assigned correctly and what percentage has not. |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------|

| | |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kappa value | The higher the Kappa value, the stronger the agreement. Depending on the application, a Kappa value of less than 0.7 indicates that your measurement 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. |

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.

| | |
|----------------|---------------------------------------------------------------|
| 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. |

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.

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

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.

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.

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 Movable 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.

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.

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 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.

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.

To Deactivate or Decommission Rules

- 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 *To Approve/Reject Role Provisioning Rules* for information.

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.

To Run Role Provisioning Rules Job

Role provisioning rules can be run only if the rule is in the active state. See [“To Approve/Reject Role Provisioning Rules” on page 77](#) 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. Choose one of the following:
 - To run now, click Run Now.
Click View Results to view the results.
 - To run the job later, click Run Later.
 - 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.

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.

Oracle Identity Analytics Workflows

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 and e-mail integration, to expose web services to communicate with third-party applications, and so on.

Understanding Workflows

This section introduces workflows.

To View a Workflow

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

Nine workflows are listed.

4. Click the desired workflow to view the steps that make up that workflow.

To understand the Edit Workflow page, see the [“Understanding the Edit Workflow Page” on page 82](#).

Types of Workflows in Oracle Identity Analytics

There are nine out-of-the-box 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. |
| Role membership activation | Runs to activate memberships which are pending activation. This workflow is automatically triggered by Oracle Identity Analytics. |
| 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. |

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.

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. |

| Column Name | Description |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assignee Type | Displays the type of actor that is assigned to complete this step. The assignee types are usually one of the following: <ul style="list-style-type: none"> ▪ -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. |

Designing Workflows

In Oracle Identity Analytics, each workflow has pre-configured default steps to complete the tasks listed in the “[Understanding Workflows](#)” on page 81.

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.

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.

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.

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, <i>Approve Role</i> , <i>Reject Role</i> , 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 <code>global_user</code> , use the search feature to select the global user that you want to assign. |

| Pre-Functions Tab | |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Add Pre-functions | <p>Pre-function is an action that will be triggered when the workflow reaches this step.</p> <p>To add a pre-function, do the following:</p> <ol style="list-style-type: none"> a. Click the Add Pre-Functions button. b. Select a pre-function from the list. c. Complete the form as needed. d. Click Save. |
| Delete Pre-functions | <p>Deletes the selected pre-functions.</p> <p>To delete a pre-function, do the following:</p> <ol style="list-style-type: none"> a. Select the pre-function by selecting the check box. b. Click Delete pre-functions. |

| | |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Post-Functions Tab | |
| Add Post-functions | <p>A post-function is an action that will be triggered when the workflow completes.</p> <ol style="list-style-type: none"> a. Click the Add Post-functions button. b. Select a post-function from the list. c. Complete the form as needed. d. Click Save. |
| Delete Post-function | <p>Deletes the selected post-functions.</p> <p>To delete a post-function, do the following:</p> <ol style="list-style-type: none"> a. Select the post-function by selecting the check box. b. Click Delete post-functions. |

Oracle Identity Analytics Identity Certifications

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 *Oracle Identity Analytics 11gR1 User's Guide Identity Certification* chapter.

See the *Oracle Identity Analytics 11gR1 User's Guide* 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:

- [“Identity Certification Configuration” on page 122](#)
- *Configuring identity certification batch sizes in the UI*

Creating New Certifications

Four types of certifications can be created in Oracle Identity Analytics.

| Identity Certification Type | Description |
|------------------------------------|------------------------------------------------------------------------------------|
| User Entitlement Certification | Allows managers to certify employee access to roles and other related entitlements |
| Role Entitlement Certification | Allows role owners to certify roles and role content |
| Resource Entitlement Certification | Allows resource owners to certify user access to resources |

| Identity Certification Type | Description |
|-----------------------------|-------------------------------------|
| Data Owner Certification | Allows data owners to certify users |

To Create a User Entitlement Certification

1. Log in to Role Manger.
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 *To Understand And Work With 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. Click Next.
 - **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*. You can preview the results of this selection.
 - **Selected users** - Allows you to manually select the users in the system. Click Next.
6. Complete the Period and Certifier form as follows, then click Next:
 - **Certifier** - You can select a Business Structure Manager, a User Manager, 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 *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 [“Scheduling Certifications” on page 93](#) for instructions.
8. Click Create.

To Create a Role Entitlement Certification

1. Log in to Role Manger.
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 *To Understand And Work With 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.
 - **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 the Business Structure Manager, Role 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 [“Identity Certification Configuration” on page 122](#).

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 *Scheduling Certifications* for instructions.
8. Click Create.

To Create a Resource Entitlement Certification

1. Log in to Role Manger.
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 *To Understand And Work With 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.
 - **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*. You can preview the results of this selection.
 - **Selected users** - Allows you to manually select the 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 the Business Structure Manager, User Manager, 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 [“Identity Certification Configuration” on page 122](#).

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 [“Scheduling Certifications” on page 93](#) for instructions.

11. Click Create.

To Create a Data Owner Certification

1. Log in to Role Manger.
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 *To Understand And Work With 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.
 - a. Click Add Data Owner, select the user, and click OK.

For help using search, see *Searching for a User*.
- **By Attribute** - Creates a certification for data owners of the selected attribute values.
 - a. Click the Add Attributes button.

The Attribute Selection table appears.

- b. 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 [“Identity Certification Configuration” on page 122](#).
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 *Scheduling Certifications* for instructions.
9. Click Create.

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 Last 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.

Scheduling Certifications

Certifications are scheduled as part of the new certification creation process. For more information, see [“Creating New Certifications” on page 87](#).

Certifications can be scheduled to run once, or to repeat on a daily, weekly, or monthly basis.

To Schedule a Certification

Before You Begin - You need to create a new certification before you can schedule it. See [“Creating New Certifications” on page 87](#).

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.

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.

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 Sun Identity Manager (Oracle Waveset).

However, for non-managed applications, 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.

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

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 Sun Identity Manager (Oracle Waveset) to revoke the account. The account is subsequently revoked in Oracle Identity Analytics after the next updated feed is imported. Select the Connection.
 - Closed-loop remediation functions only with Sun Identity Manager (Oracle Waveset).

- **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.

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.

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.

Oracle Identity Analytics Identity Audit

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 *Oracle Identity Analytics 11gR1 User's Guide Identity Audit Chapter*.

See the *Oracle Identity Analytics 11gR1 User's Guide* to learn more about the following identity audit topics:

- *Identity audit overview*
- *Understanding the identity audit user interface*
- *Acting on audit policy violations*

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.

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 such impacted violation are scanned against the policies associated with the modified rule, the following actions are taken on the violation:

1. A check is done if the modified condition still causes an exception.
2. If the rule condition still results in an exception, then the violation cause status is set to "Active." Otherwise, it is set to "Inactive."
3. The parent violation is updated accordingly.

Impact of Adding / Removing Rules in a Policy

Removing one or more rules from a policy is allowed 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.

Adding of new rules to an existing policy is allowed. 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.

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 / 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.

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.
A decommissioned rule is inactive permanently. This rule cannot be activated again.
However, all information about the rule is retained in Oracle Identity Analytics.
6. Click Save.

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 it.

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.

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.

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.

A decommissioned policy is inactive permanently. This policy cannot be activated again. However, all information about the policy is retained in Oracle Identity Analytics.
6. Click Save.

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.

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 Preview.
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.

- 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.

- a. To view the policy scan results, click View Results.

The Status column displays the number of violations.

- b. Click Close.

- To run a policy at a later time or date, click Run Later.

The Schedule Job page opens.

- a. Enter a task name and description, and select the time and day for the task to start.

- b. Click Next.

The Summary page opens.

- c. Click Schedule.

The scan job is scheduled for the desired day and time.

Oracle Identity Analytics Reports

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 *Oracle Identity Analytics 11gR1 User's Guide Reports* chapter.

See the *Oracle Identity Analytics 11gR1 User's Guide* 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 out-of-the-box reports in Oracle Identity Analytics.

Working With Custom Reports

You can run custom reports in Oracle Identity Analytics to suit the requirements of your organization.

The following steps are involved in creating and running custom reports:

1. Creating 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. Using the Oracle Identity Analytics user interface, upload the reports template to Oracle Identity Analytics.
3. Running or scheduling the report as needed.

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.
 - **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 the previous topic, “[Working With Custom Reports](#)” on page 103.)
5. Click Save.

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.

Oracle Identity Analytics Scheduling

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 [“Provisioning Servers Configuration” on page 119](#) in the Oracle Identity Analytics Configuration chapter.

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 the *Scheduling a Job by Editing Configuration Files* section.

To Schedule an Import and Export Job Using the User Interface

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.

The File Server option is a standard option that you can use to specify a flat file data import or export, for example, a CSV or XML file type.

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.

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 [“Scheduling a Job by Editing the Configuration Files” on page 106](#) for more information.

| Job Name | Trigger Name | Description |
|-------------------|-----------------------|-------------------|
| usersImportJob | usersImportTrigger | Imports users. |
| accountsImportJob | accountsImportTrigger | Imports accounts. |
| rolesImportJob | rolesImportTrigger | Imports roles. |

| Job Name | Trigger Name | Description |
|------------------------------------------|---------------------------------------------|---------------------------------------------------------------------------------|
| glossaryImportJob | glossaryImportTrigger | Imports glossary definitions. |
| policiesImportJob | policiesImportTrigger | Imports policies. |
| businessStructureImportJob | businessStructureImportTrigger | Imports business structure definitions. |
| identityAuditContinuousViolationsScanJob | identityAuditContinuousViolationScanTrigger | Scans for continuous identity audit violations |
| identityAuditViolationReminderJob | identityAuditViolationReminderTrigger | Sends out an identity violation reminder when an e-mail template is configured. |
| certificationReminderJob | certificationReminderTrigger | Sends out a certification reminder when an e-mail template is configured. |
| reportReminderJob | reportReminderTrigger | Sends out a report reminder when an e-mail template is configured. |
| stableFolderCleanUpJob | stableFolderCleanUpTrigger | Cleans the stable folder. |
| accountsMaintenanceJob | accountsMaintenanceTrigger | Maintenance of accounts. |
| roleMembershipRuleJob | roleMembershipRuleTrigger | Triggers the role membership rule. |
| fullTextIndexMaintenancedJob | fullTextIndexMaintenancedTrigger | Maintenance of full text index. |
| workflowStepSLAJob | workflowStepSLATrigger | Triggers workflow steps. |
| roleStatusAndMembershipMaintenanceJob | roleStatusAndMembershipMaintenanceTrigger | Maintenance of role status and membership. |
| rmPreviewCleanUpJob | rmPreviewCleanUpTrigger | Cleans preview. |
| userApplicationMaintenanceJob | userApplicationMaintenanceTrigger | Maintenance of user application. |
| postImportJobsLauncherJob | postImportJobsLauncherTrigger | Triggers post import jobs. |
| certificationRemediationJob | certificationRemediationTrigger | Triggers certification remediation. |
| rmScanArchivalJob | rmScanArchivalTrigger | Triggers scan archival. |
| eventPublishingJob | eventPublishingTrigger | Triggers event publishing. |
| rmeRuleMigrationJob | rmeRuleMigrationTrigger | Triggers rule migration. |

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 [“To Enable a Job by Editing the Configuration Files” on page 108](#) 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="fullTextIndexMaintenanceJob"/>
<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>

```

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 a job can run, you need to enable it. See [“Scheduling a Job by Editing the Configuration Files” on page 106](#) 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 [“Sample Cron Expressions” on page 111](#) 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 “[Sample Cron Expressions](#)” on page 111 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>

```

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.

| 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 |

| Cron Expression | Definition |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0 15 10 * * ? * | Fire at 10:15am every day |
| 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 |

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 *Oracle Identity Analytics 5.0.3 User's Guide*.

- **e-mail 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 *Sending Reminder E-mails to Data Owners* in the Oracle Identity Analytics Reports chapter.
- **Certifications** - For information about how to schedule certifications, see “[Scheduling Certifications](#)” on page 93 in the Oracle Identity Analytics Identity Certifications chapter.
- **Role mining tasks** - For information about how to schedule role mining tasks, see “[Running or Scheduling a Role Mining Task](#)” on page 70 in the Role Manager Identity Certifications chapter.

Oracle Identity Analytics Configuration

System Configuration

This section describes how to configure settings for the Proxy Assignment Notifications, Mail Server Settings, and OIA Server Settings options.

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.

Mail Server Settings

This option helps in setting up the mail server.

| | |
|---------------------|--------------------|
| Email Encoding | UTF-8 |
| SMTP Server Name | mail.vaau.com |
| SMTP Port | 25 |
| SMTP Authentication | Select if required |

OIA Server Settings

This option helps in setting up the Oracle Identity Analytics server.

| | |
|--------------|-----------------------------|
| System Email | rbacx@vaau.com |
| OIA URL | http://localhost:8282/rbacx |

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. Systems such as UNIX®, Windows, SAP, Oracle, 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.

To Create, Rename, and 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 *rename* a resource type, do this:
 - a. Click the resource type, then click Rename.
 - b. Type a new name and click Save.
- 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.

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.

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. Type the name of the attribute category, and type a number for the category order.
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.

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 | Name of the Attribute |
|---------------|---------------------------------------------------------------------|
| 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 |
| Max Value | The maximum value that the attribute can have |
| Default Value | The default value an attribute can have when it is imported |
| Values | A predefined list of values that the attribute can have |
| Label | The display label for the attribute |

In addition, the following flags further define an attribute:

| | |
|----------------|------------------------------------------------------------------------------------------------------------------|
| Space Allowed | Allows the attribute values to have a space in them |
| Multiple Value | Allows an attribute to have comma-separated multiple values |
| 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 |
| Auditable | Allows the attribute to be checked for audit exceptions |
| Minable | Allows Oracle Identity Analytics to perform role engineering operations |
| Mandatory | This flag, when selected, specifies all the privileges for the attribute such as managed, importable, and so on. |
| Importable | Allows the attribute to be imported from a CSV / Text File |

To Create, Rename, Edit, and Delete an Attribute

1. Log in to Oracle Identity Analytics.
2. Choose Administration > Configuration.
3. Click Resource Type.
4. To create an attribute, highlight the Attribute Category under which you want to create an Attribute and click the New Attribute tab.

A dialog box appears.

5. Enter the New Attribute values.
6. To rename, edit, or delete an attribute, do one of the following:
 - To *rename* an attribute, do this:
 - a. Click the Rename icon in the right-most column for the appropriate attribute.
A dialog box appears.
 - b. Enter the new name and save it.
 - To *edit* an attribute, do this:
 - a. Click the Edit Attribute icon located in the right-most column for the appropriate attribute.
 - b. Modify the required values.
 - To *delete* an attribute, do this:
 - a. Click the Delete icon in the right-most column for the appropriate attribute.

A dialog box confirming the action appears.

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.

Note - If you are using Sun Identity Manager or Oracle Waveset as your provisioning server, see the *Integrating With Sun Identity Manager* chapter in the *Oracle Identity Analytics 11gR1 System Integrator's Guide*.

Supported provisioning platforms include:

- Sun Identity Manager (Oracle Waveset)
- Computer Associates
- IBM
- Oracle Identity Manager
- File

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 CA - refer to table 11-2 for information about how to complete the form.
- If you selected Sun Identity Manager (Oracle Waveset) - refer to table 11-3 for information about how to complete the form.
- If you selected IBM - refer to table 11-4 for information about how to complete the form.
- If you selected Oracle Identity Manager - refer to table 11-5 for information about how to complete the form.
- If you selected File - refer to table 11-6 for information about how to complete the form.

Table 11-2 - Help on Completing the CA New Provisioning Server Connection Form

| | |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connection Name | Enter a name for the new connection being created with the CA eTrust Admin. This connection name is used during the import process instead of the host name and port, which are difficult to remember. |
| Host Name | Enter the host name. |
| Clear Port | "20380" <Default Value> |
| TLS Port | "20390" <Default Value> |
| Domain Name | Enter the name of your domain. |
| User Name | "etaadmin" <default username> |
| Password | "*****" Enter the password set for the ETA user. |

Table 11-3 - 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: <code>http://OracleWavesetApplicationServerName:PortNumber/idm/servlet/rpcrouter2</code> For example: <code>http://localhost:8080/idm/servlet/rpcrouter2</code> |

| | |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <i>Oracle Identity Analytics 11gR1 System Integrator's Guide</i> , "Integrating With Oracle Waveset (Sun Identity Manager)" chapter, <i>To Create an Oracle Waveset User That Oracle Identity Analytics Will use to Connect</i> . 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 Oracle Waveset. <ul style="list-style-type: none"> ▪ 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 11-4 - Help on Completing the IBM Provisioning Server Connection Form

| | |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connection Name | Enter a name for the new connection being created with the IBM provisioning server software. This connection name is used during import process instead of the host name and port because they are difficult to remember, for example: VAAU-TIM. |
| Host Name | Enter the host name. |
| Port | 2809 <Default Port Number> |
| LDAP Context | Enter ou=vaau, dc=com. |
| User Name | "itim manager " <default username> |
| Password | "secret" <default password> |

Table 11-5 - Help on Completing the Oracle New Provisioning Server Connection Form

| | |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connection Name | Enter a name for the new connection being created with the Oracle provisioning server software. This connection name is used during the import process instead of the host name and port, which are difficult to remember. |
| Host Name | Enter the IP where Oracle Identity Manager (xelWebApp) is running |
| Port | Enter the application server's port number where Oracle Identity Manager is running |
| User Name | Type the user name for Identity Manager |

Figure 11-6 - 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. |
| 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. |

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 *Oracle Identity Analytics 11gR1 System Integrator's Guide*:

- *Configuring Identity Certification Batch Sizes in the UI* is covered in the *Oracle Identity Analytics 11gR1 System Integrator's Guide* in the "Customizing the Oracle Identity Analytics User Interface" chapter.

To Configure Identity Certification

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

Completing the Certification Configuration Form "General" Section

Before You Begin - See ["Identity Certification Configuration"](#) on page 122 for help opening the Certification Configuration page.

Table 11-6 - "General" Panel

| Field | Description |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Business Structure Hierarchy / Hierarchy Depth | Select the Business Structure Hierarchy option to include all the users in the business structure and the users in business structures under it in a certification, depending on the hierarchy depth chosen by the administrator. |
| Comment required on all non-certify selections | Select to allow the user to type a comment if a revoke action is selected. (Note: The system does not require the user to type a comment.) This option also activates the comment field on the certification of entitlements screen. |
| 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 copy to admin for new certifications | Select to send a copy to the admin when a new certification is created. |

Table 11-7 - "User Entitlement Options" Panel

| Field | Description |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certify Entitlements | For user entitlement certifications, select this option to enable entitlements certifications. Then select which entitlements should be certified. <ul style="list-style-type: none"> ■ All Entitlements: Select to display all entitlements ■ Entitlements Outside Roles: Select to display entitlements that are not part of the role ■ Accounts with High Privileged Entitlements: Select to display only accounts that have one or more entitlements marked as high-privileged. ■ Only High Privileged Entitlements - Select to display only those entitlements classified as high-privileged. |
| Certify Roles | Allows managers to certify roles of users under them. |
| Certify user with no accounts | Allow managers to certify users under them, who do not have an account. |
| Certify account with no certifiable attributes | Allow managers to certify users under them, who do not have any certifiable attributes. |
| View user activity information | Allows the certifier to see the user's recent account activity. Note - This feature is functional if Role Manger is integrated with Intellitactics Security Manager. To learn about this feature, see <i>Integrating with Intellitactics Security Manager</i> . |
| Employee verification required | Select this to include the first step (employee verification) during the certification completion process, then select the "Create new certification per reporting manager" option. |

| Field | Description |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Create new certification per reporting manager | Select this to create a new certification if the certifier selects "Reports To" and names the new manager for the user. |

To Complete the Certification Configuration Form "Status Options" Section

Before You Begin - See [“Identity Certification Configuration”](#) on page 122 for help opening the Certification Configuration page.

1. In the User Access Tab, select the options that the manager will see when certifying users under him.
For example, 'Works for me,' 'Does not work for me,' 'Terminated,' and 'Reports To' in the Employee Verification section, and 'Certify,' 'Revoke,' 'Unknown,' and 'Exception Allowed' in the Certification Sign off section. Oracle Identity Analytics also includes the option of renaming these labels according to an organization's preference.
2. In the Data Owner Tab, select the options that the data owner will see when certifying the users' Access under him.
For example, 'Belongs To Me,' and 'Does Not Belong To Me' in the Data Owner Verification section, and 'Certify,' 'Revoke,' 'Unknown,' and 'Exception Allowed' in the Approve or Revoke Data Access section. Oracle Identity Analytics also includes the option to renaming these labels according to an organization's preference.
3. In the Resource Entitlement Tab, select the options that the manager will see when he is certifying the users' Access under him.
For example, 'Certify,' 'Revoke,' 'Unknown,' and 'Exception Allowed' in the Verify employee access section. Oracle Identity Analytics also includes the option of renaming these labels according to an organization's preference.
4. In the Role Entitlement Tab, select the options that the manager will see when he is certifying the roles of users under him.
For example 'Belongs To Me' and 'Does Not Belong To Me' in Role Entitlement section, and 'Certify,' 'Revoke,' 'Unknown,' and 'Exception Allowed' in the Certify Policy and Entitlement Access section. Oracle Identity Analytics also includes the option of renaming these labels according to an organization's preference.
5. Click Save.

To Complete the Certification Configuration Form "Reminders" Section

Before You Begin - See ["Identity Certification Configuration"](#) on page 122 for help opening the Certification Configuration page.

1. In New Certification Notification tab, choose one or both of the following:
 - If an e-mail goes out every time a new certification is created, and, if so, the format of the e-mail.
 - If an e-mail goes out when the certifier is updated, and, if so, the format of the e-mail.
2. In the Upcoming Certification Notification tab, choose if a notification e-mail should be sent to the manager of any upcoming certifications. You also have an option to choose the reminder interval and the format of the e-mail.
3. In the Pending Certification Notification tab, choose when to start sending pending certification notification e-mails to the manager, and when to escalate the notification e-mails to the manager's manager in case certification is not completed.
4. In the Certification Completion Notification tab, choose if an e-mail goes out every time a certification is completed, and, if so, the format of the e-mail.
5. In the Certification Expiry Notification tab, choose if a notification e-mail should be sent to the manager of certifications that have expired and certifications that are about to expire. Administrator also has an option to choose the notification interval and the format of the e-mail.
6. Click Save

To Complete the Certification Configuration Form "Revoke and Remediation" Section

Before You Begin - See ["Identity Certification Configuration"](#) on page 122 for help opening the Certification Configuration page.

1. In the Access Revoke section, configure the certification to send appropriate e-mails along with manager's comments when user access is revoked by a manager.

E-mails can be sent when a manager selects 'Does Not Work For Me' or 'Revoke Access' from the roles and entitlements certification screen.
2. Use the Reporting Changes option when considering the action to be taken when employee verification options "Does Not Work for Me", "Terminated," and "Works for Some One Else" are selected.

When reporting changes is enabled, the details of employees verified by selecting the options mentioned is recorded separately. The Create New Certification Per Reporting Manager option creates a new certification for each user selected as the actual "certifier" by using the "Works for Some One Else" option.

3. Use the Remediation section when considering the display information during the remediation process. Select Display Remediation Instructions to allow the certifier access to remediation instructions by clicking the hyperlinked resource button during the certification process.

Select Perform Closed-Loop Remediation, to start the remediation process on one of the following dates:

- **Certification End Date** - The remediation process takes place on the day the certification ends or expires.
- **Include Expired Certification** - The remediation process takes place on the completed portion of the incomplete certification when it expires.
- **Certification Completion Date** - The remediation process takes place on the day the certifier completes the certification.

4. Click Save.

Role Management Configuration

This section describes how to configure the Oracle Identity Analytics role mining and "SoD evaluation of role assignment" feature.

To Configure Mining

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

To Configure Roles

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

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.

To Configure Identity Audit

1. Log in to Oracle Identity Analytics.
2. Choose Administration > Configuration.
3. Click Identity Audit.
4. Select the desired configurations based on the requirements of the organization.

To Configure E-Mails for Violation Reminder and Escalation

1. Log in to Oracle Identity Analytics.
2. Choose Administration > Configuration.
3. Click Identity Audit.
4. Do one of the following:
 - 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.

To Configure E-mails For Violation Lifecycle Event Notifications

1. Log in to Oracle Identity Analytics.
2. Go to Administration > Configuration.
3. Click Identity Audit.
4. Select Send Email For New Violations to choose an e-mail template and also send e-mail notifications to actors associated with the new violations that are created.
5. Select Send Email For Reopened Violations to choose an e-mail template and send e-mail notifications to actors associated with the violations that are reopened.
6. Select Send Email For User or System Remediated Violations to 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.
7. Select Send Email When Violation is Assigned to choose an e-mail template and send e-mail notifications to actors associated with the violation that is assigned to a user.
8. Select Send Email When Violation Closed as Risk Accepted to choose an e-mail template and send e-mail notifications to actors associated with the violation that is closed as risk accepted.
9. Click Save.

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.

To Configure Report Reminder E-mails

1. Log in to Oracle Identity Analytics.
2. Choose Administration > Configuration.
3. Click Reports.
The Report Configuration page opens.
4. To configure the send-reminder-e-mail workflow, select a reminder, select a reminder interval, and select an e-mail template.

E-mail templates are created on the Email Templates tab. For help, see [“E-mail Templates Configuration \(Configuring E-mail Notification\)”](#) on page 129 in the Oracle Identity Analytics Configuration chapter.

5. Click Save.

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.

To Create and Configure E-mail Notifications

1. Log in to Oracle Identity Analytics.
2. Choose Administration > Configuration.
3. Click Email Templates.
4. Click New Email 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 [“E-mail Parameters Definitions” on page 129](#) for more information.
6. Click Save.

E-mail Parameters Definitions

Oracle Identity Analytics has 35 e-mail parameters or variables that can be selected when you are creating e-mail templates.

Table 11-8 - E-mail Parameters

| E-mail Parameter | Definition |
|----------------------|----------------------------------------------------------------------------------------------------------------------------|
| System Email | Used for specifying system e-mail. Example: rbacx@oracle.com |
| User Email | Used to specify the user's e-mail address. This field can be used in the To fields of all e-mail templates. |
| User Secondary Email | Used to specify the user's secondary e-mail address. |
| User Full Name | Used to specify the user's full name. Example: Baker, Angela. This variable can be used in the subject and body fields. |
| User Last Name | Used to specify the user's last name. |

| E-mail Parameter | Definition |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User First Name | Used to specify the user's first name. |
| Url | Used to embed the Oracle Identity Analytics URL in an e-mail. This variable can be used in the body of all e-mail templates. |
| Certification Name | Used to specify the name of the certification being processed. This field can be used in the subject and body fields of all certification related e-mails. |
| Report Name | User to specify the name of the report being processed. This field can be used in the subject and body fields of all report-related e-mail templates. |
| Proxy User Email | Used to specify the e-mail of the proxy user. This can be used in the To and CC fields of the proxy assignment e-mail template. |
| Proxy User Fullname | Used to specify the proxy user's full name. This can be used in the subject and body fields of the proxy assignment e-mail template. |
| Proxy StartDate | Used to specify the start date of the proxy period. This can be used in the proxy assignment e-mail template. |
| Proxy EndDate | Used to specify the end date of the proxy period. This can be used in the proxy assignment e-mail template. |
| Access Revoke Details | Used to embed the revocation details of the certification. This can be used in the body field of the access revoke e-mail template. |
| User Manager Email | Used to specify the e-mail address of the user's manager. This can be used in the To, CC, and BCC fields. |
| User Request RequesterName | Used to specify the name of the user who has initiated a request. |
| User Request Type | Used to specify the request type (for example, "role change request"). |
| User Request Date | Used to specify the date when a request was created. |
| User Role Name | Used to specify the name of the role sent for approval. |
| User Role VersionNumber | Used to specify the version number of the role sent for approval. |
| User RoleOwner Email | Used to specify the e-mail addresses of role owners who own roles for which a version is sent for approval. |

| E-mail Parameter | Definition |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User PolicyOwner Email | Used to specify the e-mail addresses of policy owners who own policies for which a version is sent for approval. |
| User Policy Name | Used to specify the name of the policy whose version is sent for approval. |
| User Policy VersionNumber | Used to specify the version number of the policy that is sent for approval. |
| User Manager Name | Used to specify the full name of the user's manager. |
| User Manager | Used to specify the e-mail address of the user's manager. |
| Identity Audit Violation Name | Used to display the name of the identity audit policy violation. |
| Identity Audit Violation Action | Used to display the event or type of action that resulted in an e-mail being sent to the user. |
| Identity Audit Policy Owner Name | Used to display the full name of the identity audit policy owner associated with the violation. |
| Identity Audit Policy Owner Email | Used to display the e-mail address of the identity audit policy owner associated with the violation. |
| Identity Audit Violation Remediator Name | Used to display the full name of the identity audit violation remediator associated with the violation. |
| Identity Audit Violation Remediator Email | Used to display the e-mail address of the identity audit violation remediator associated with the violation. |
| Identity Audit Violation Old Remediator Name | 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. |
| Identity Audit Violation Old Remediator Email | 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. |
| Identity Audit Violation Remediator Manager Email | Used to display the e-mail address associated with the manager of a user who is currently the remediator of a violation. |

Import/Export

You can import the following in Oracle Identity Analytics:

- Users
- Business Structures
- Roles
- Policies
- Glossary
- Accounts
- Resource Metadata

- Resources

Details about importing are discussed in the *Oracle Identity Analytics Importing Chapter*.

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 nine workflows:

- Role creation
- Role modification
- Role membership
- Role membership activation
- Mass modification
- Policy creation
- Policy modification
- Role membership rule creation
- Role membership rule modification.

Details about understanding and designing workflows are discussed in the *Oracle Identity Analytics Workflows Chapter*.

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.

To Create a New Event Listener

1. Log in to Oracle Identity Analytics.
2. Choose Administration > Configuration.
3. Click Events.
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:
 - **User to Business Structure Rule Scan** - Runs selected user-to-business structure rules.
 - **Role Membership Rules** - Runs the selected role membership rules on users.
 - **IDA Policy Scan** - Run selected identity audit policies on users based on a condition.
 - **User Entitlement Certification Creation** - Creates a user entitlement certification.
8. Use the following table to configure this form, then click Finish.

Table 11-9 - Add Event Listener Form Properties

| Listener Action Properties | Description |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status | Must be enabled for execution. The status of the action can be active or inactive. Inactive actions will not be executed. |
| Event count | 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. |
| Time interval | Defines the interval after which the action will be executed repeatedly. |
| Action configuration | Includes items such as the list of rules to be executed, or certification configuration in case of certification action. |

Oracle Identity Analytics Access Control

Oracle Identity Analytics Access Control Introduction

This chapter describes how to assign privileges to Oracle Identity Analytics users.

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.

| Role Name | Description | System 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 |
| 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 |

| Role Name | Description | System Privileges |
|-------------------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 e-mail template, and access the Configuration system sub-tab |

System Privileges

| Privileges | 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 subtab |
| Access Resource type view | Allows a user to access Resource Type view |
| Configure Resource type definitions | Allows a user to configure Resource Type definitions |

| Privileges | Description |
|----------------------------------------------------|---------------------------------------------------------------------|
| Configure Identity Certification | Allows a user to configure identity certifications |
| Configure Email Templates | Allows a user to configure e-mail 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 |
| 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 |

| Privileges | Description |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 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 subtab 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 |
| 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 |

Business Privileges

| Privileges | Description |
|---------------------------|----------------------------------------------------|
| Access Business Structure | Allows a user to access Business Structure details |

| Privileges | Description |
|----------------------------------------------------|--------------------------------------------------|
| 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 |
| Sign off Reports | Allows a user to sign off on reports |
| Certify Entitlements | Allows a user to certify associated entitlements |

Working With Oracle Identity Analytics Users And Roles

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.

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.
 - 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.
 - a. Complete the user information form and click Next.
 - b. 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.
 - c. Select the desired Business Role by using the arrow keys and click Finish.
 - d. 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.

Password Quality Settings

Password Quality Settings consists of two options:

- Quality check
- Dictionary check

Enabling these options lets the administrator create guidelines to select a password.

| Quality Settings | Description |
|----------------------------------|--------------------------------------------------------------------------------------------------|
| Minimum Password Length | Set the minimum password length |
| Minimum Alphabetic 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 |
| Minimum Alpha Numeric Characters | Set the minimum alpha numeric characters required in the password |
| Password Interval | Set the number of days after which the password expires |
| Grace Period Days | Set the number of days users have to select a new password after their original password expires |

To Modify User Password

1. Log in to Oracle Identity Analytics.
2. Choose Administration > Access Control.

3. Click OIA Users.
4. Find the user and click Change Password in the Action column.
5. Type a new password and click OK.

Audit Event Log and Import-Export Log

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.

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.

| 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 |

| 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 |

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.

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.

- Click Export to save audit event log records as a CSV file that you can open using a spreadsheet application.

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 this table.

| Function | 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.

| Function | Description |
|-------------------------|---------------------------------------------------------------|
| Total number of records | Total number of records in the feed file |
| Records Imported | Total number of records imported by Oracle Identity Analytics |
| Number of Errors | Number of errors encountered during the feed import |

The details captured by the export logs are described in the table below:

| Function | 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). |

| Function | Description |
|---------------|-----------------------------------------------------------------------------------------------|
| 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.

| Function | 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 |

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.

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 [“Import-Export Log” on page 145](#).

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.

