Oracle® Fusion Middleware

User's Guide for Oracle Identity Analytics

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

E23367-02

March 2014

ORACLE

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

E23367-02

Primary Author: Deena Purushothaman

Contributing Author: Kevin Kessler

Contents

7 Identity Certification

8 Identity Audit

Preface

This guide describes how to use the Oracle® Identity Analytics 11gR1 software, including how to complete identity certifications, how to check for access violations, how to modify access based on changes, and how to identify, assess, and prioritize segregation of duties (SoD) violations.

Audience

This guide is written for business managers and other users in a supervisory role who need information about how to use the Oracle Identity Analytics software to grant employees and partners access to applications, check for access violations, and so on.

- Compliance officers and IT specialists who need to configure and maintain role management and compliance functionality should see the Business Administrator's section of the *Administrator's Guide for Oracle Identity Analytics*.
- System administrators, deployment engineers, and service providers who need information about how to administer the Oracle Identity Analytics software at a systems level should see the System Administrator's section of the *Administrator's Guide for Oracle Identity Analytics*.
- Deployment engineers who are responsible for integrating Oracle Identity Analytics with other IT systems should see the *System Integrator's Guide for Oracle Identity Analytics*.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents in the Oracle Identity Analytics Release 11g R1 PS1 documentation set:

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

Conventions

The following text conventions are used in this document:

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

1

Oracle Identity Analytics Overview

This chapter contains the following sections:

1.1 Introducing the Role-Based Access Control Model

With the enactment of strict compliance-related legislation, like the Sarbanes-Oxley (SOX) Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley (GLB) Act, it has become imperative for companies to secure their information and exercise control over access to mission-critical applications within the organization. Oracle understands that organizations today need a strong governance environment around access control. To establish strong governance, a robust framework around access control is necessary. This can be attained using the Role Based Access Control (RBAC) framework and an enterprise-wide role definition effort.

Role-based access control (RBAC) limits access to system applications to only authorized users within an organization. The model simplifies identity and access control compliance by managing access based on a user's roles within a company, not on an individual, user-by-user basis. Roles are created based on usage and enterprise policies. For example, new employees need access to certain system applications in order to perform their job responsibilities. Using the RBAC model, the new employees can be assigned to existing roles, which automatically give them access to the necessary set of system applications. Business managers are required to check and certify or revoke access to system applications on a regular basis.

1.2 Understanding Oracle Identity Analytics Benefits

Oracle Identity Analytics software addresses all aspects of role-based access control. The software allows organizations to streamline the access-control process, simplify attestation, and enhance audit effectiveness, thereby resulting in secure and robust role management.

Oracle Identity Analytics enables you to accomplish the following tasks:

- Simplify the assignment and management of user access
- Create and manage roles rather than users

- Achieve compliance by way of access certifications and segregation of duties (SoD)
- Align business and IT processes with a common terminology for IT access permissions
- Ensure an ongoing understanding of access: who has it, who approved it, and what access violations exist
- Reduce the risk of security violations and access control-related deficiencies
- Manage the role lifecycle through the use of workflows, versioning, consolidation, history, and ownership
- Provide complete rule lifecycle management to effectively manage the rapid on-boarding and off-boarding of users

1.3 Understanding the Oracle Identity Analytics Model

Oracle Identity Analytics is organized into the following modules: Identity Warehouse, Identity Certification, Role Engineering and Management, and Identity Auditing.

1.3.1 Identity Warehouse

The Identity Warehouse is a central repository that contains data on user entitlements. This data is imported from one or more databases within your organization on a scheduled basis. The Oracle Identity Analytics import engine supports complex entitlement feeds saved as either text or XML files. Extract, Transform, and Load (ETL) processing capabilities are also available. Imported data is then correlated or mapped to various roles during the certification phase. A glossary description of each entitlement is also captured during the import process.

1.3.2 Identity Certification

Managing and auditing enterprise-wide attestations is a major challenge to companies with a large number of employees. Because individual users may have access to a multitude of platforms, systems, and applications, organizations need an easy-to-use tool that managers can use to review user entitlements on a regular basis. Moreover, federal requirements require time-based certifications, granular entitlements, and so on.

The Oracle Identity Analytics identity certification module makes user entitlements easy to monitor and distribute. Managers can easily communicate with IT administrators to monitor, authorize, add, or revoke application access based on changes. The Oracle Identity Analytics identity certification module allows managers to collect, manage, and distribute user entitlements. In addition, these certifications can be scheduled depending upon the compliance requirements of the entitlement certification.

The identity certification module can perform four types of certifications:

- **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.

- **Data Owner Certification**. Allows data owners to certify users.

Each certification addresses different audience types and ensures stringency at every step of the access management process.

1.3.3 Role Engineering and Management

Role-based access control is one of the complex and challenging efforts carried out in security administration. RBAC restricts access of the systems to authorized users by using predefined and approved roles. Within an organization, roles are seldom stationary. With a dynamic business environment, role management is also in a constant state of flux. New roles need to be created while old ones need to upgraded or managed on a regular basis.

Oracle Identity Analytics offers an end-to-end solution to define roles based on existing user entitlements. Roles can also be generated using the software's role mining module. The Oracle Identity Analytics role mining interface uses sophisticated algorithms to create new roles based on user entitlements, and cuts the role definition time by about fifty percent. Multiple rules and a combination of attributes (such as job codes, department, and location) can be used to assign role-based access to new and existing users.

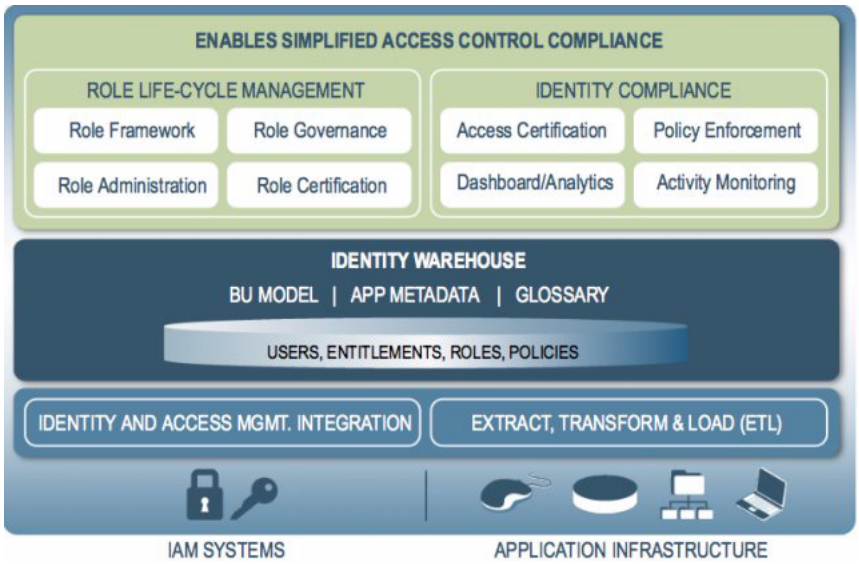
The Oracle Identity Analytics software is a good alternative to manual access control methodologies because its superior framework facilitates easy management of users and their access to roles in a controlled and effective manner. Oracle Identity Analytics provides a complete setup of security, workflow, and auditing features to manage the lifecycle of roles. The built-in workflow engine provides the ability to configure the best suited workflow processes depending on the business requirements and allows stakeholders to call external functions from the workflows. This functionality enables greater efficiencies from a role-based access control model. Additionally, multiple rules and a combination of attributes (such as job codes, department, and location) can be used to assign role-based access to new and existing users.

1.3.4 Identity Auditing

Today, organizations need to manage continuous exception monitoring, segregation of duties (SoD) violations, detective scanning, inter and -intra-application SoD enforcement, actual vs. assigned exceptions, exception lifecycle management, and so on. Organizations also tend to have numerous exceptions related to the access users have to target systems.

Close monitoring is an integral part of Oracle Identity Analytics. The identity auditing module has a detective mechanism that monitors users' actual access to resources and captures any violations on a continuous basis. The software can also be programmed to conform to audit policies and to report exceptions. It provides a summary of all exceptions, which helps security analysts, executives, or auditors accept or mitigate the exceptions.

Figure 1–1 Oracle Identity Auditing Dashboard



1.4 Understanding Oracle Identity Analytics Components and Terminology

This section introduces Oracle Identity Analytics components and defines terminology that you need to know in order to be successful with the software.

1.4.1 Understanding Users

A *user* is defined as a discrete, identifiable entity that has a business need to access or modify enterprise information assets. Typically a user is an individual, but a user can also be a program, a process, or a piece of computer hardware.

Users are associated with business structures in various ways. A user can be assigned to several business structures based on access level and other details within an organization. A business user has a *manager* or an *application approver* who is tasked with carrying out various user- and role-management functions on the user.

1.4.2 Understanding Resources and Resource Types

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

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

Note: In older releases, the term *endpoint* was used to denote a resource, while the term *namespace* was used to denote a resource type.

1.4.3 Understanding Business Structures

A *business structure* in Oracle Identity Analytics is defined as a department or sub-department within an organization. An organization can be segregated into as many business structures, with as many levels of hierarchy as is required to represent teams and sub-teams within the organization. There is no limit to the number of users that can be assigned to a business structure. All operations in Oracle Identity Analytics such as identity auditing and identity certification are performed on the basis of a business structure.

1.4.4 Understanding the User Store

The *user store* is the central platform or database or directory where user records are stored. Commonly used user stores include Active Directory, Exchange, ORACLE, SAP, UNIX, and RDBMS Tables.

Initially, an organization in Oracle Identity Analytics is populated with users using a feed from an HR system. The HR system is used to create all the global identities in Oracle Identity Analytics. Alternatively, the global identities can be created from a provisioning system such as Oracle Waveset (Sun Identity Manager).

The entitlements from the various applications are stored in a centralized user store in Oracle Identity Analytics. The user store can be a relational database that handles the various user entitlements. Once the entitlements are in the user store, the role engineering and management, identity certification, and identity auditing pieces can be carried out on them.

A user is a global identity to which various accounts are associated. A user can have multiple accounts, but all of the accounts are associated with a single global identity in Oracle Identity Analytics. This global identity is defined under the Users View, which shows the entire list of users that belong to the organization.

A naming convention for all users needs to be established. A common naming convention is a combination of a user's name in lowercase letters and a set of numbers. For example, John Smith's user name might be josmit01. User names must be unique.

1.4.5 Understanding Roles

A *role* represents a job function. Roles contain policies that describe the access that individuals have on a directory. Roles represent unique job functions performed by users in the domain. For example, a person can function as a manager, a developer, and a trainer. In this case, there are three roles that represent each job function because each requires different privileges and access to different *resources*.

Roles give you the flexibility and power to enforce enterprise standards, so that you can do the following:

- Manage users who perform the same tasks the same way no matter where they are located in the enterprise.
- Perform less work when managing users because you do not have to manually specify privileges every time a change is made to a person's job function.

A role can be embedded inside a role as a nested role. Role hierarchy can be defined to any level required in an organization.

1.4.6 Understanding Policies

Policies define account attributes and privileges that users have on different platforms or applications. In OIA, a policy represents a specific privilege on a specific data resource. Policies are assigned to roles, and roles are assigned to users. Policies provide consistent directory permissions and user rights across and within the organization for all of the users in a role.

1.4.7 Understanding Orphan Accounts

An *orphan account* is an account that is no longer associated with any user entry. (The user may have left the organization or shifted departments, but the account was not deactivated when the user left or moved.)

2

Using the Oracle Identity Analytics User Interface

This chapter contains the following sections:

2.1 Logging In to Oracle Identity Analytics

To open the Oracle Identity Analytics user interface, you need a supported browser. For a list of supported browsers, see the "Compatibility Matrix" chapter in the *Installation & Upgrade Guide for Oracle Identity Analytics*.

2.1.1 To Log In to the User Interface

1. Open the Oracle Identity Analytics login page by typing the URL into your browser, or by clicking the Oracle Identity Analytics icon (if available).

   The login page opens.

2. Enter your user name and password.

   If your user name and password are accepted, the Oracle Identity Analytics home page opens.

2.2 Using the Oracle Identity Analytics User Interface Menu

The Oracle Identity Analytics user interface features two menus:

- The "Home" menu in the top-right corner of the screen provides **Home**, **Logout**, **Help**, and **About** links
- The main application menu organizes the interface into multiple modules, including **My Settings**, **My Requests**, **Identity Warehouse**, **Identity Certification**, and so on.

The following table describes the menu links in the top-right corner of the screen.

Table 2–1 The Links in the "Home" Menu

Link	Description
Home	Click to view a dashboard that summarizes whether you have any requests or identity certifications to approve, complete, or dismiss. This screen is displayed upon logging in to Oracle Identity Analytics. For help, including information on how to open the Home page, see Chapter 3, "The Home Page."
Logout	Click to log out of Oracle Identity Analytics.
Help	Click to open a window that contains Oracle Identity Analytics help topics. The information available from the Help menu is the same information available in the *Oracle Identity Analytics User's Guide*.
About	Click to open a window that contains the version number for your installation of Oracle Identity Analytics.

The following table describes the top-level tabs that are available in the main application menu. Most modules have a secondary row of tabs (or views) that further organize Oracle Identity Analytics functionality. Depending on your role and entitlements, only some tabs may be visible to you.

Table 2–2 The Tabs in the Main Menu

Tab	Description
My Settings	Click to view information about your Oracle Identity Analytics account, including your name, password, and e-mail address, as well as information about your proxy assignments. Proxy assignments enable you to delegate certifications to another user while you are away from the office.
My Requests	Click to view and either approve or reject pending requests, such as role change requests and membership change requests. You can also view completed requests on a separate subtab.
Identity Warehouse	Click to create, view, and manage business structures, users, roles, policies, and resources.
Identity Certification	Click to view the certification dashboard. Additional tabs allow you to create, view, search, manage, and complete certifications. Identity certifications are conducted periodically to verify that users have access only to the proper entitlements on the assigned systems.
Role Management	Click to perform role mining and identity correlation tasks, including role discovery, role consolidation, entitlements discovery, and rules-for-role-assignments discovery. This module is primarily intended for use by administrators.
Identity Audit	Click to create audit rules and audit policies, and to scan for audit violations.
Reports	Click to access various reports, including business unit reports, system reports, audit reports, and custom reports.
Administration	Click to configure and maintain Oracle Identity Analytics. This module is primarily intended for use by administrators.

3

The Home Page

This chapter contains the following section:

- Section 3.1, "Home Page"

3.1 Home Page

The home page contains a dashboard with five charts or graphs that represent important data related to workflow requests, certifications, approvals, and policy violations. You can select whether the dashboard displays vertical charts, horizontal charts, or pie charts.

Figure 3–1 Oracle Identity Analytics Home Page

3.1.1 To Open the Home Page

1. Log in to Oracle Identity Analytics.

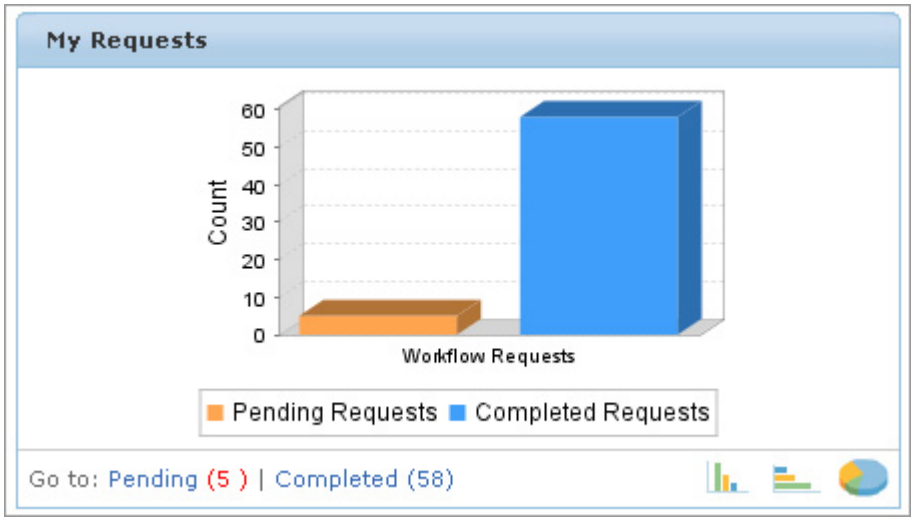
2. Click **Home** in the upper right corner of the screen.

   The Home page opens.

3.1.2 My Requests

The My Requests chart shows how many workflow requests are completed and how many are awaiting action from the user. Click the Pending and Completed links to open the requests approval page. Click the "three charts" icon in the bottom-right part of the panel to view a different chart type.

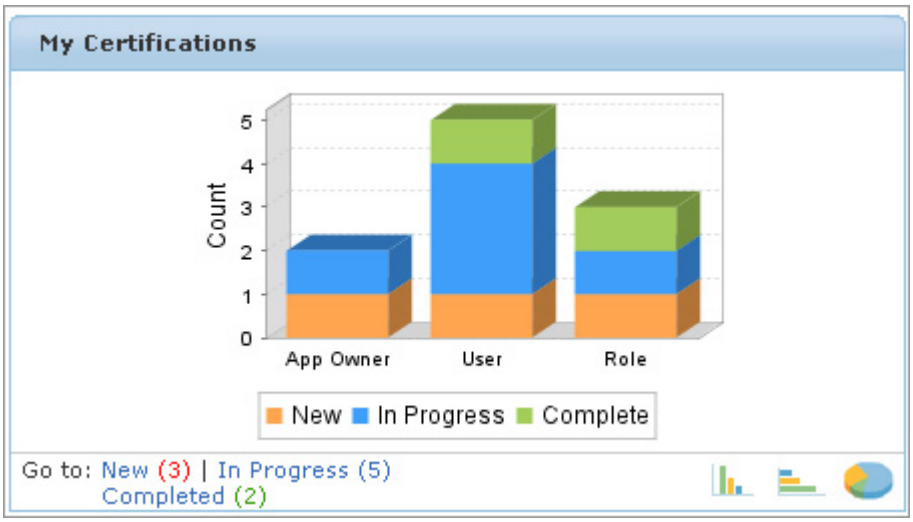
Figure 3–2 My Requests



3.1.3 My Certifications

The My Certifications chart displays information about New, In Progress, and Completed certifications. Click the **Pending**, **In Progress**, or **Completed** links to open the Certification inbox that contains the appropriate certifications. Click the "three charts" icon in the bottom-right part of the panel to view a different chart type.

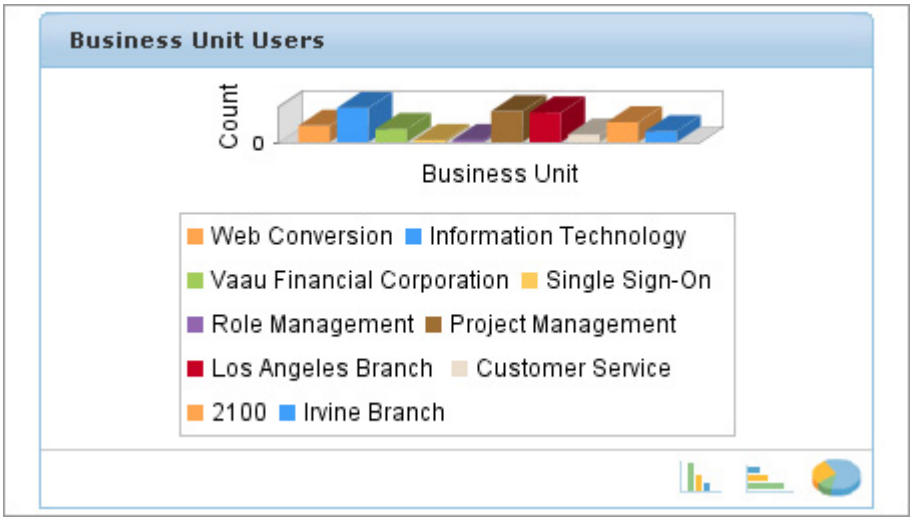
Figure 3–3 My Certifications



3.1.4 Business Structure Users

The Business Structure Users chart displays the number of users that belong to each business unit. Click the "three charts" icon in the bottom-right part of the panel to view a different chart type.

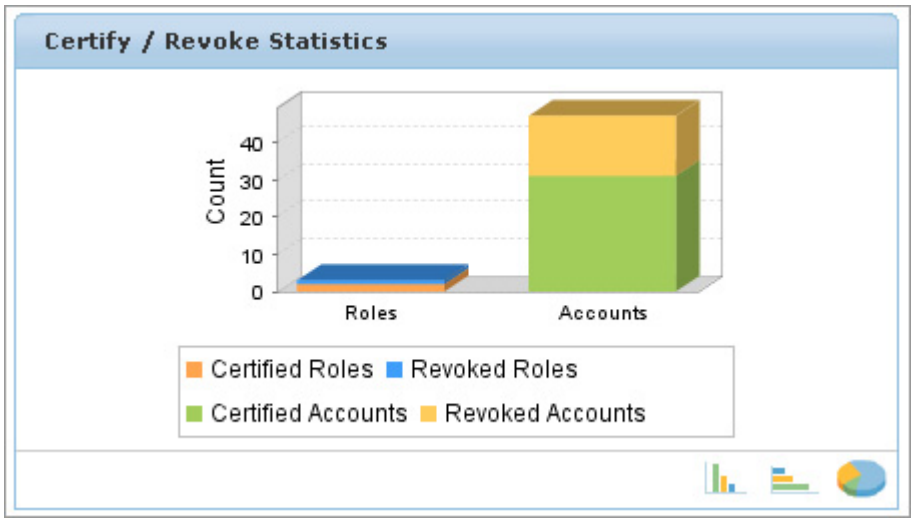
Figure 3–4 Business Structure Users



3.1.5 Certify/Revoke Statistics

The Certify/Revoke Statistics chart displays the number of roles and accounts that are certified and revoked during a certification process. Click the "three charts" icon in the bottom-right part of the panel to view a different chart type.

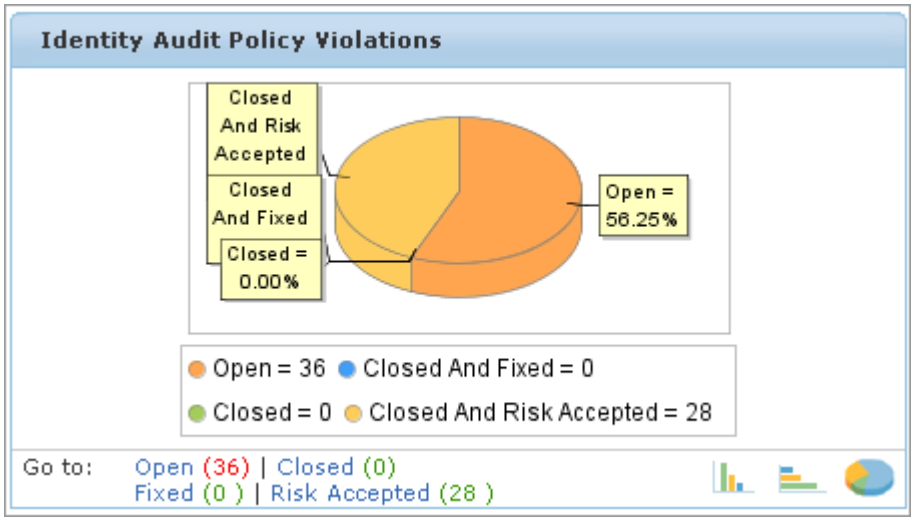
Figure 3–5 Certify / Revoke Statistics



3.1.6 Identity Audit Policy Violations

This chart displays the number of open, closed, and risk-accepted identity audit policy violations. Click the links to view the corresponding violations. Click the "three charts" icon in the bottom-right part of the panel to view a different chart type.

Figure 3–6 Identity Audit Policy Violations



4

My Settings

This chapter contains the following section:

- Section 4.1, "My Settings Tab"

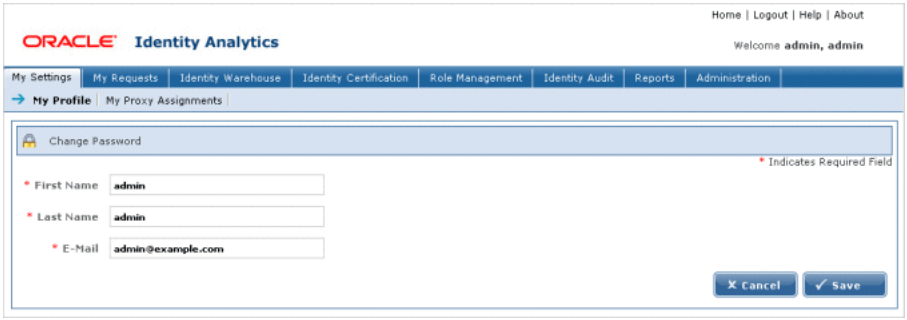
4.1 My Settings Tab

Use the My Settings Tab to manage your Oracle Identity Analytics user account and to manage your delegations while you are out of the office.

4.1.1 My Profile

Click **My Profile** to change your first and last name and e-mail address.

Figure 4–1 My Profile Page



4.1.1.1 To Change Your User Name and Email Address

1. Log in to Oracle Identity Analytics.
2. Choose **My Settings** > **My Profile**.
3. Edit the **First Name**, **Last Name**, and **E-Mail** fields and click Save.

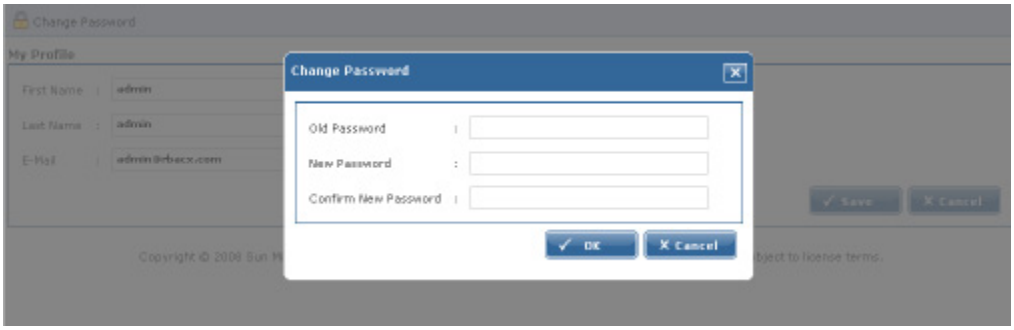
4.1.1.2 To Change Your Password

1. Log in to Oracle Identity Analytics.
2. Choose **My Settings** > **My Profile**.
3. Click **Change Password**.

   The Change Password pop-up window opens.

4. Complete the form and click OK.
5. Click Save.

Figure 4–2 Change Password



4.1.2 My Proxy Assignments

Click My Proxy Assignments to delegate certification-related duties to another user while on vacation or out of the office. Delegations cannot be set for more than 30 days.

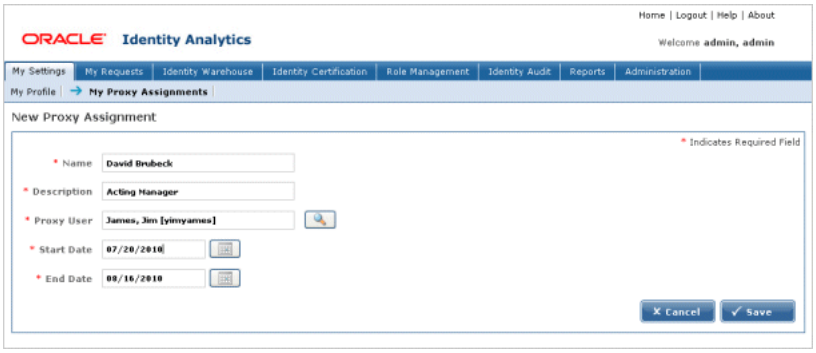
4.1.2.1 To Delegate Certification-Related Duties to Another User

1. Log in to Oracle Identity Analytics.
2. Choose **My Settings** > **My Proxy Assignments**.
3. Click **New Proxy Assignment**.

   The New Proxy Assignment page opens.
4. Complete the form.
   - The **Start Date** should be set to the date that you will leave.
   - The **End Date** should be set to the date that you will return. Proxy users will not be able to delegate on your behalf on the end date.
   - Delegations cannot be set for more than 30 days.
5. Click Save.

   A new Proxy Assignment will be created. As of the start date, the designated proxy can log in to Oracle Identity Analytics and perform the tasks that you designated up until the specified end date.

Figure 4–3 Enter Proxy Details



5

My Requests

This chapter contains the following section:

5.1 My Requests Tab

Use the My Requests Tab to view and either approve or reject pending requests, such as role change requests and membership change requests. You can also view completed requests on a separate subtab.

5.1.1 To Approve Pending Requests

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

   The requests are listed.
3. Click **View** to view a request in detail.
4. Click either **Approve** or **Reject**, as desired.

   The object is listed in the **Completed Requests** tab.

5.1.2 To View Completed Requests

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

   The completed requests are listed.
3. Click **View** to review the details of a request.

> **Note:** - If a role or policy owner is not assigned, then Oracle Identity Analytics automatically approves any changes made.

6

Identity Warehouse

This chapter contains the following sections:

6.1 What Is the Identity Warehouse?

The Identity Warehouse is a central repository that contains all of the important entitlement data for your organization, including Users, Roles, Policies, Resources, and Business Structures. This data is imported from your organization's databases on a regular, scheduled basis. The Oracle Identity Analytics software has an import engine that supports complex entitlement feeds. The engine accepts either text or XML files, and includes Extract, Transform, and Load (ETL) processing capabilities. The engine also captures the glossary description of each entitlement.

6.2 Understanding the Identity Warehouse User Interface

This section provides help using the Identity Warehouse portion of the user interface.

6.2.1 The Identity Warehouse > Business Structures Page

To open the Identity Warehouse - Business Structures page, choose **Identity Warehouse** > **Business Structures** from the main menu.

The Identity Warehouse - Business Structures page has four subtabs, which are described in the following section.

6.2.1.1 Tabs on the Identity Warehouse - Business Structures Page

This section describes the pages that open when you click the tabs on the **Identity Warehouse > Business Structures** page.

General Tab

This page displays basic information about the business structure, including Type, Division, and Owner. Also provides information about the status of the business structure. Actions can only be taken on a business structure if it is in the active state.

Users Tab

This page displays all users who are part of the selected business structure.

Roles Tab

This page displays all the roles associated with the selected business structure.

Policies Tab

This page displays all the policies associated with the selected business structure.

6.2.2 The Identity Warehouse > Users Page

To open the Identity Warehouse - Users page, choose **Identity Warehouse** > **Users** from the main menu.

This page displays user name, first name, last name, primary e-mail, and risk summary information. Quick search and advanced search are provided.

You can get detailed information about a user by clicking the user name link. This will open a page in a new window that contains the user's roles, business structures, accounts, general details, custom properties, and relationship map. See Section 6.3.5, "Viewing User Details" for additional information.

Orphan Accounts

An *orphan account* is an account that is no longer associated with any user entry. (The user may have left the organization or shifted departments, but the account was not deactivated when the user left or moved.)

The Orphan Accounts page is documented in the "Identity Warehouse" chapter in the Oracle Identity Analytics Administration Guide.

6.2.2.1 Tabs on the Identity Warehouse - Users - *User* Detail Page

Upon selecting a user, a page with tabs opens. This section describes the pages that open when you click the tabs on the selected user page.

General Tab

This page displays basic information about user.

- **Risk Summary** - The user's overall risk (*high*, *medium*, or *low*), as calculated by Oracle Identity Analytics based on the user's Item Risk and any related risk factors. In OIA, three bars signifies high risk, two bars signifies medium risk, one bar signifies low risk.

To better understand Risk Summary values, see "Understanding How Risk Summaries are Calculated" in the "Oracle Identity Analytics Identity Warehouse" chapter of the *Administrator's Guide for Oracle Identity Analytics*.

Accounts Tab

Displays information about the user's accounts.

Roles Tab

Displays information about the user's assigned roles.

Business Structures Tab

Displays information about the business structures that the user is assigned to.

Workflow Tab (Optional)

Displays three approver fields that are populated with data if OIA has been integrated with the CA Identity Manager provisioning server. The three approver fields are **Business Approver**, **Technical Approver,** and **Delegate**.

Note: The Workflow tab is hidden by default. To enable it, see "To Enable the Workflow Tab on the Identity Warehouse Pages" in the *System Integrator's Guide for Oracle Identity Analytics*, "Customizing the OIA User Interface" chapter.

Custom Properties

Displays custom information about the user. For more information about custom properties, see "Working With Extended User Custom Properties" in the "Oracle Identity Analytics Identity Warehouse" chapter, in the *Administrator's Guide for Oracle Identity Analytics*.

Relationship Map

Displays the user's relationship to other objects in the system hierarchy

6.2.3 The Identity Warehouse > Roles Page

To open the Identity Warehouse - Roles page, choose **Identity Warehouse** > **Roles** from the main menu.

The Roles page is divided into the following sections:

- The left side displays the following subtabs:
  - The **Hierarchy** subtab displays roles in the organization
  - The **Search** subtab displays the search feature
- The right side displays ten tabs that are described in the following section.

6.2.3.1 Tabs on the Identity Warehouse - Roles Page

This section describes the pages that open when you click the tabs on the **Identity Warehouse > Roles** page.

General Tab

Use this page to view or enter basic information about the role, such as the name of the role, the role type, the Item Risk level, the status (Active, Inactive, Decommissioned), and so on.

- **Type** - A role can be one of the following types:
  - **Provisioning role** - Entitlement roles used in Oracle Identity Manager or other provisioning solutions.
  - **Access Control role** - Roles that capture policies for products that are integrated with Oracle Identity Analytics, like Siteminder and Open SSO.
  - **Organizational role** - Roles that are based on job function, such as Consultant, Analyst, Contractor, and so on.
- **Risk Level** - The assigned Item-Risk level (*high*, *medium*, or *low*) for this role. In OIA, three bars signifies high risk, two bars signifies medium risk, one bar signifies low risk.

  For more information about Risk Levels and how they are used to calculate Risk Summaries, see "Understanding How Risk Summaries are Calculated," in the "Oracle Identity Analytics Identity Warehouse" chapter, in the *Administrator's Guide for Oracle Identity Analytics*.
- **Status** - A role can exist in one of the following states:
  - **Active** - Applies to roles that have been approved by the role owner. Only active roles can be acted upon.
  - **Inactive** - Applies to old roles.
  - **Composing** - Applies to roles that are in the process of being created. Roles in a composing state have not yet been sent by an administrator for approval.
  - **Pending Approval** - Applies to roles that have been sent by an administrator for approval.
  - **Decommissioned** - Applies to roles that no longer exist. All information regarding the role, however, is retained in Oracle Identity Analytics.
- **Service Desk / Service Desk Ticket#** - The helpdesk system reference number for the role, if relevant to your organization.

Business Structures Tab

Use this page to view, add, and remove the business structures associated with the role.

Policies Tab

Use this page to view, add, and remove the policies that make up the role.

Users Tab

Use this page to (1) view the users who are assigned to the role, (2) add additional users to the role, and (3) remove users who are assigned to the role.

The page is divided into the following sections.

Composing	Applies to user-role assignments that are in the process of being created. Assignments in a composing state have not yet sent by an administrator for approval. ■ **Add Users** -Assign one or more users to a role by clicking **Add Users**. To assign a user to a role indefinitely, set the **End Date** to be the same as the **Start Date** in the **User-Role** Association pop-up. ■ **Remove Users** - Remove one or more users from a role.
Pending Approval	Applies to user-role assignments that have been sent by an administrator for approval.
Active	Applies to user-role assignments that have been approved by the role owner and are active. ■ **Add Users** -Assign one or more users to a role by clicking **Add Users**. To assign a user to a role indefinitely, set the **End Date** to be the same as the **Start Date** in the **User-Role** Association pop-up. *Note:* Users added from the **Active** section will still appear in the **Composing** section until they are approved. ■ **Remove Users** - Remove one or more users from a role.
Pending Activation	Applies to user-role assignment that have been approved by the role owner but are not yet active.
Modified	Applies to user-role assignment that have been modified.

Exclusion Roles Tab (Optional)

Note: The Exclusion Roles tab is hidden by default. To enable it, see the steps in the *System Integrator's Guide for Oracle Identity Analytics*, "Customizing the Oracle Identity Analytics User Interface" chapter, "Enabling Hidden Pages in the UI" section.

The Exclusion Roles page displays conflicting roles. This information defines segregation of duties at the role level. See Section 6.7, "Setting the Segregation of Duties at the Policy and Role Levels" for more information.

- Click **Add Exclusion Roles** and add the roles that need to be excluded to define segregation of duties at the role level.
- Select one or more roles and click **Remove Exclusion Roles** to remove the role(s) from the Exclusion Roles list.

Ownership Tab

This page displays the owner(s) of the role.

Workflow Tab (Optional)

Displays three approver fields that are populated with data if OIA has been integrated with the CA Identity Manager provisioning server. The three approver fields are **Business Approver**, **Technical Approver,** and **Delegate**.

Note: The Workflow tab is hidden by default. To enable it, see "To Enable the Workflow Tab on the Identity Warehouse Pages" in the *System Integrator's Guide for Oracle Identity Analytics*, "Customizing the OIA User Interface" chapter.

Custom Properties Tab

This page displays the custom properties associated with the role.

Versions Tab

This page displays all versions of the role. This section allows you compare two versions and revert to an older version of the role.

History Tab

This page displays the role's history. Role history is divided into four sections: *Role Membership History*, *Owner History*, *Policy History*, and *Attribute History*.

6.2.4 The Identity Warehouse > Policies Page

To open the Identity Warehouse - Policies page, choose **Identity Warehouse** > **Policies** from the main menu.

The left side of the Policies page displays the following subtabs:

- The **Hierarchy** subtab displays resource types. Policies are displayed below each resource type. The bottom section displays policies that have been revised, but not approved.
- The **Search** subtab displays the search feature.

The right side displays eight tabs that are described in the following section.

6.2.4.1 Tabs on the Identity Warehouse - Policies Page

This section describes the pages that open when you click the tabs on the **Identity Warehouse** > **Policies** page.

General Tab

Use this page to view or change the policy name, status (Active, Inactive, Decommissioned), and Item Risk level. You can also enter comments about the policy, and add a Service Desk Ticket number.

Business Structures Tab

This page displays the business structures associated with the policy.

Roles Tab

This page displays the roles associated with the policy.

Resources Tab

This page displays the resources that are part of the policy.

Exclusion Policies Tab

This page displays conflicting policies. This information defines segregation of duties at the policy level. See Section 6.7, "Setting the Segregation of Duties at the Policy and Role Levels" for more information.

Ownership Tab

Use this page to view the current policy owner(s) and add or remove policy owners.

Workflow Tab (Optional)

Displays three approver fields that are populated with data if OIA has been integrated with the CA Identity Manager provisioning server. The three approver fields are **Business Approver**, **Technical Approver,** and **Delegate**.

> **Note:** The Workflow tab is hidden by default. To enable it, see "To Enable the Workflow Tab on the Identity Warehouse Pages" in the *System Integrator's Guide for Oracle Identity Analytics*, "Customizing the OIA User Interface" chapter.

Version Tab

This page displays all versions of the policy.

Entitlements Tab

This page displays the resource attributes and values that make up the policy.

6.2.5 The Identity Warehouse > Applications Page

To open the Identity Warehouse - Applications page, choose **Identity Warehouse** > **Applications** from the main menu.

An *application* is a collection of multiple resource types and resources. The Applications page lists the applications that are stored in the Oracle Identity Analytics Identity Warehouse. Oracle Identity Analytics administrators define the resource types, resources, and metadata that define the application.

Click an application in the **Application Name** column to open a page with application detail. The application detail page has four tabs that are described in the next section.

> **Note:** To learn more about working with applications, see the "Working With Applications" topic in the "Oracle Identity Analytics Identity Warehouse" chapter of the *Administrator's Guide for Oracle Identity Analytics*.

6.2.5.1 Tabs on the Identity Warehouse - Application - Application Detail Page

This section describes the pages that open when you click the tabs on the **Identity Warehouse** > **Application** > **Application Details** page.

General Tab

Displays basic information about the application, including Name, Version, Description, Environment, Comments, and Status (Active or Inactive).

Users

Lists all the users that are associated with the application.

Ownership

Lists the assigned owner(s) of the application. Application owners are responsible for reviewing user access on the applications that they own.

The following actions are available to Oracle Identity Analytics administrators:

- Click **Add Owner** to add one or more additional users as owners for this application.
- Select one or more users and click **Remove Owner** to remove the users from the owners list for this application.

Conditions

Lists the resource type, resource, attribute name, and attribute value associated with the application.

- Click **Add Condition** to open the Add Conditions dialog box.

  Create a condition that includes either a **Resource Type** and **Resource**, or a condition that includes a **Resource Type**, a **Resource**, an **Attribute Name**, and an **Attribute Value**. (You do not have to select from all four columns.)

  Click OK.

- Select one or more conditions and click **Remove Condition** to remove the conditions from the list for this application.

6.2.6 The Identity Warehouse > Resources Page

To open the Identity Warehouse - Resources page, choose **Identity Warehouse** > **Resources** from the main menu.

The Resources page lists all the resources in Oracle Identity Analytics and the Item-Risk Level for each resource.

Click in the **Resource** column to open a page showing resource detail. The resource detail page has three tabs that are described in the next section.

To learn more about working with resources, refer to the "Working With Resources" section in the *Administrator's Guide for Oracle Identity Analytics*.

6.2.6.1 Tabs on the Identity Warehouse - Resources Page

General Tab

Displays basic information about the resource, including Resource Name, Host Name, Host IP Address, Description, Comments, and Item-Risk Level. The **Risk Level** is the assigned Item-Risk level (high, medium, or low) for this resource. In OIA, three bars signifies high risk, two bars signifies medium risk, one bar signifies low risk.

Data Management Tab

Displays the resource-attribute values (also referred to as *entitlements*) for the selected resource.

Use the **Search** box to filter the attribute values displayed in the table. Choose whether to search in the Attribute Value, Glossary, or Description columns, then type your search string. The system returns all matching results, including substring matches. (So for example, typing "ar" in the Attribute Value search box, might return `qcfar` and `warpdev`.)

The table displays the following information for each resource-attribute value:

- **Glossary** - A user-friendly descriptive name for the attribute value (entitlement). During identity certification, if a glossary entry is available, OIA displays the glossary entry instead of the actual attribute-value name.

- **Description** - A brief description of the attribute value.
- **Data Owner** - The person responsible for the attribute value (entitlement). In a Data Owner Certification, data owners certify the user accounts that have a specific attribute value assigned.
- **Classification** - A classification value for the attribute.
- **Risk Level** - The Item Risk level associated with the resource-attribute value. In OIA, three bars signifies high risk, two bars signifies medium risk, one bar signifies low risk.

Administrators can click a resource-attribute value and edit these settings. The data entered here is made available to certifiers during the certification process.

Remediation Tab

Displays remediation settings and information for the resource. To define the remediation process, first select the provisioning mode used for this 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 this resource.

6.3 Working With Users

This section contains instructions on how to perform common user tasks in Oracle Identity Analytics.

> **Tip:** For help with the **Identity Warehouse > Users** user interface, see Section 6.2.2, "The Identity Warehouse > Users Page."

6.3.1 Searching for a User

Oracle Identity Analytics provides quick search and advanced search options for user searches. Quick search enables searching for users on any of the commonly populated user fields (for example, User Name, First Name, Last Name, Business Unit, Department, Manager). Advanced Search should be used to conduct a narrower search and to create complex searches.

6.3.1.1 To Search for a User (Quick Search)

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. To perform a quick search, choose a field from the drop-down menu.

   All the commonly populated fields are available to search on.
4. Enter a value to search for.

   Wildcards are accepted, for example, `a*` or `j*n*`.
5. To search on the selected field for the entered value, click **Search**. The results for the search are displayed.

6.3.1.2 To Search for a User (Advanced Search)

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

4. Create a condition by selecting values for **Attribute**, **Condition**, and **Value**. Attributes can be selected over an extensive range including Resources, Business Units, and any other commonly populated user field. The **Value** field supports wildcards, for example, `a*` or `j*n*`.
5. To create more conditions, click **Add**.
6. To remove conditions, select the condition by selecting its corresponding checkbox and click **Remove**. In the case of multiple conditions, set **Operation** to AND or OR to specify the logical operation between the conditions.
7. To group two conditions together, select them and click **Group**. Groupings are displayed by a different color coding for each group. In the case of nested groups, the outermost grouping will have one color code with each component group having its own color code.
8. To ungroup a grouped conditional, select the grouped conditional by selecting its corresponding checkbox, and click **Ungroup**. The created search condition is dynamically displayed in a highlighted line under the Group and Ungroup tags as a single logical condition.
9. To search on the created condition, click **Search**.

6.3.2 To Create a User

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. To add a new user, click the **New User** button on the top panel.

   The Create User pop-up window opens.
4. Complete the form and click OK to create the user.

6.3.3 To Rename a User

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. Search for the user.

   For help using Search, see Section 6.3.1, "Searching for a User."
4. Click the user's link in the **User Name** column.
5. Type a new name for the user and click Save.

6.3.4 To Delete a User

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. Search for the user. For help using Search, see Section 6.3.1, "Searching for a User."
4. Select the user name for the user that you want to delete, and click the **Delete User** button.

6.3.5 Viewing User Details

This section describes how to view a user's account and account type details.

6.3.5.1 To View User Accounts (Entitlements)

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. Search for the required user.

   For help using Search, see Section 6.3.1, "Searching for a User."
4. Click to select the User, and click the **Accounts** tab.
5. Click the required account to view account details.

6.3.5.2 To View a User's Account Type

Account Types help describe accounts. Knowing the *type* associated with an account can be helpful when making decisions during remediation and access certification, and when performing a role engineering wave. To designate an account type while importing accounts using the Oracle Identity Analytics automated import process, a type attribute should be provided in the `.rbx` schema file. This predefined account type can then be leveraged while performing identity certifications, role engineering, and remediations, allowing the different Oracle Identity Analytics actors to make educated decisions.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. Search for a user.

   For help using Search, see Section 6.3.1, "Searching for a User."
4. Click to select the user.
5. Click the **Accounts** tab.

   The account type is listed in the **Account Type** column.

6.3.6 Setting User Status

User status can be set to either *active* or *inactive*. If a user is scheduled to leave the company, an *End Date* for the user can be specified in Oracle Identity Analytics.

6.3.6.1 To Set User Status

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. Search for the user. For help using Search, see Section 6.3.1, "Searching for a User."
4. Select the user.
5. On the **General** tab, scroll down to the **Suspension** section.
6. In the **Status** field, set the status to **Active** or **Inactive** in the drop-down menu.

   If you set the user to *Inactive*, the **End Date** for the user is automatically changed to today's date.

   If you set the user to *Active*, specify an **End Date** for the user.

> **Note:** To make an *inactive* user *active*, you must set the user's status to Active and specify a new **End Date** for the user.

6.3.7 To Assign a Role to a User

To temporarily assign a role to a user, see Section 6.6.5, "To Assign a User to a Role."

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. Search for the user. For help using Search, see Section 6.3.1, "Searching for a User."
4. Select the user and then click the **Roles** tab.
5. Click **Add Roles**.
6. Search for the role. For help using Search, see Section 6.6.2, "To Search for a Role."
7. Select the role.

   Once one or more roles are assigned to the user, an approval process needs to be completed before they are displayed. For more information, see Section 6.6.1, "Understanding the Role Approval Process."

6.3.8 To Associate a User With a Business Structure

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Users**.
3. Search for the user that you want to associate with a business unit. For help using Search, see Section 6.3.1, "Searching for a User."
4. Select the user and then click the **Business Unit** tab.
5. Click the **Add Business Unit(s)** button, and assign one or more business unit(s) to the user.

6.4 Working With Business Structures

This section describes how to delete and create Business Structures in the Identity Warehouse.

> **Tip:** For help with the **Identity Warehouse > Business Structures** user interface, see Section 6.2.1, "The Identity Warehouse > Business Structures Page."

6.4.1 To Delete a Business Structure

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Business Structures**.
3. Click to select the business structure that you want to delete.
4. Click **Delete Business Structures**.

   A Delete Business Structures confirmation window opens.
5. Click **Yes** to delete.

   The business structure is deleted.

6.4.2 To Create a Business Structure Hierarchy

An *n*-level business structure hierarchy can be defined in Oracle Identity Analytics. A business structure can have various child business structures under it.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Business Structures**.
3. Click **New Business Structure** to create a business structure.

   The Create Business Structure window opens.
4. Complete the form as follows:
   - **Name** - Type the name of the business structure.
   - **Parent** - Select the parent business structure from the drop-down menu.
   - **Enter the Service Desk Tick #** - Each business structure can be associated with a unique service desk ticket number if an integration between Oracle Identity Analytics and a ticketing system is used in your organization.
5. Click OK.

6.5 Working With Policies

Policies are templates that define the various access levels that a user has on the target systems. Policies are individually defined for each resource. Roles are made up of policies.

The polices component displays all available policies that exist for the organization categorized according to Resource Type. Resources are depicted using a round globe icon. The available policies are shown under each resource type.

> **Tip:** For help with the **Identity Warehouse > Policies** user interface, see Section 6.2.4, "The Identity Warehouse > Policies Page."

6.5.1 Understanding the Policy Approval Process

The lifecycle of a policy is managed by out-of-the-box workflows. Workflows are step-by-step explanations (flowcharts) that Oracle Identity Analytics follows to complete a selected set of tasks. The workflows can be modified to suit the requirements of your organization.

Workflows only show active information when a Policy is going through the approval process, for example during the "Pending Approval" state. In the "Active" state, workflows do not convey much information.

Oracle Identity Analytics has the following policy workflows:

- Policy creation workflow
- Policy modification workflow

The default policy creation and policy modification workflows each have three steps:

- **Start workflow** - This steps kicks-off once a policy is created or modified.
- **Policy Owner Approval** - If a policy owner approves the request, the workflow proceeds to the next step. Otherwise, the policy is discarded.
- **Finish** - The policy is created.

To understand or change policy workflows, refer to the Oracle Identity Analytics Workflows chapter in the *Administrator's Guide*.

6.5.1.1 Approving Policy Change Requests

Modifications to a policy are activated only after the approval of the policy owner.

To approve a policy change request, see Section 5.1.1, "To Approve Pending Requests."

6.5.2 To Create a Policy

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Policies**.
3. Click **New Policy**.

   The Policy Wizard window opens.
4. Select the resource type for which you are creating the policy and click **Next**.
5. Select the resource for which access needs to be defined and click **Next**.
6. Click **Add Owner** to search for the owners for this policy and click **Next**. For help using Search, see Section 6.3.1, "Searching for a User."

   Note: Depending on how the system is configured, only users who have the permissions required to manage the policy will be listed.

7. When the Policy Property window opens up, complete the form:
   - **Name** - Type the name of the policy.
   - **Comments** - Type any additional comments about the policy.
   - **Service Desk Ticket #** - Add the helpdesk system reference number, if relevant to your organization.
8. Click the Entitlements tab and complete the form:
   - **Value** - Enter the value of the attribute defined for the resource.
   - **Required** - Selecting this means the value is mandatory and needs to be assigned to the role. This value cannot be excluded.
   - **Risk Level** - This policy attribute is not currently used and is deprecated.

     Note: Only the policy Risk Level attribute is deprecated. For more information about Risk attributes in OIA, see the *Administrator's Guide for Oracle Identity Analytics*, "Oracle Identity Analytics Identity Warehouse" chapter, "Understanding How Risk Summaries are Calculated" section.

   - **+ / -** - Use these to add or delete an attribute value.
9. Click Finish.

The new policy is displayed under the resource type on the Policies page.

6.5.3 To Delete or Rename Policies

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

- To rename a policy, do the following:
  a. Select the policy by clicking on the policy name.

b. Change the name of the policy and click **Save**.

- To delete a policy, do the following:
  a. Select the policy by clicking on the policy name.
  b. Click the **Delete Policy** button.

6.5.4 To Associate Policies With Resources

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

   Policies are listed by resource type on the left side of the page.
3. Click to select the desired policy.
4. Click the **Resources** tab in the panel on the right.
5. Click the **Add Resources** button.
6. Select one or more resources from the list and click **OK**. (Hold down the Control key while clicking to select multiple items. Click an item again while holding down Control to clear that item.)
7. Click **Save**.

   The resource will not be associated with the policy until it has been approved by the policy owner.
8. Click **Send For Approval**.

Once the policy owner approves it, the resource is associated with the policy.

6.5.5 To Add Policies To Roles

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**.
3. Select a role and click the **Policies** tab on the right side of the page to add policies to (or remove policies from) the role.
4. Choose one of the following tasks:
   - Click **Add Policies** to assign the selected policies to the role.
   - Click **Remove Policies** to remove the selected policies from the role.
5. Click **Save**.

   The policies associated with a role will display on the **Policies** tab for the role.

6.5.6 To Associate Policy Owners With Policies

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

   Policies are listed by resource type on the left side of the page.
3. Click a policy and click the **Ownership** tab on the right side of the page.
4. Click **Add Owner** and search for the user (or users) to add.

   For help using Search, see Section 6.3.1, "Searching for a User."

Note: Depending on how the system is configured, only users who have the permissions required to manage the policy will be listed.

5. Click **Save**.

6.6 Working With Roles

Oracle Identity Analytics administers role-based access controls. Roles make it easier to assign access levels to users and to audit those assignments on an ongoing basis. Rather than assigning access levels to users directly, access levels are assigned to a role. Roles are assigned to users, and a user's access level is determined by the roles assigned to that user.

Role-based administration typically grows and expands as new situations occur. The main advantage of using this approach is ease of implementation. Role-based administration can be established in a centralized fashion, distributed throughout your network, or hybridized. Oracle Identity Analytics can be configured to match the unique structure and needs of your organization. Roles can be defined in a hierarchical format, and segregation of duties (SoD) can be administered through a role.

Tip: For help with the **Identity Warehouse > Roles** user interface, see Section 6.2.3, "The Identity Warehouse > Roles Page."

6.6.1 Understanding the Role Approval Process

The lifecycle of a role is managed by out-of-the-box workflows. Workflows are step-by-step explanations (flowcharts) that Oracle Identity Analytics follows to complete a selected set of tasks. The workflows can be modified to suit the requirements of your organization.

Workflows only show active information when a role is going through the approval process, for example during the "Pending Approval" state. In the "Active" state, workflows do not convey much information.

Oracle Identity Analytics has the following role workflows:

- Role creation workflow
- Role modification workflow
- Role membership workflow
- Mass modification workflow

The mass modification workflow enables you to bulk modify roles.

The default role creation, role modification, and role membership workflows each have four steps:

1. Start workflow: This step starts once a role is created, modified, or a member is added or removed.
2. Policy Owner Approval: If a policy owner approves the request, the workflow proceeds to the next step. Otherwise, the role is rejected.
3. Role Owner Approval: If a role owner approves the request, the workflow proceeds to the next step. Otherwise, the role is rejected.
4. Finish: The role is created or modified.

To understand or change role workflows, refer to the Oracle Identity Analytics Workflows chapter in the *Administrator's Guide*.

6.6.1.1 Approving Role Change Requests

Modifications to a role are activated only after the approval of the role owner.

To approve a role change request, see Section 5.1.1, "To Approve Pending Requests."

6.6.2 To Search for a Role

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**.
3. To use quick search, click the **Search** tab on the left side of the page and choose an option from the drop-down menu. Commonly populated fields are available to be searched on.
4. Enter a value to search for. Wildcards can be used (for example, `a*` or `j*n*`).
5. Click **Search** to search the selected field for the value specified. Search results are displayed in the Search panel on the left side of the screen.
6. Click a role to select it.

6.6.3 Creating Roles

There are three ways to create roles in Oracle Identity Analytics:

- Manually
- From existing roles
- From an existing user

When a role is created, it is placed into the **Composing** state until the system sends it for approval. After the role is sent for approval, the role moves into the **Active** state.

6.6.3.1 To Create Roles Manually

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**.
3. Choose **New Role** > **Create Role Manually**.

   The Create New Role pop-up window opens.
4. Complete the form:
   - **Name** - Type a name for the role.
   - **Parent Role** - Click the button to open the Select Role window, select the role that you want to designate as the parent role for the role you are creating, and click OK.
   - **Risk Level** - The Item-Risk level for the role. Select High, Medium, or Low from the menu.
   - **Status** - When a role is created, it is placed into the **Composing** state until the system sends it for approval. After the role is sent for approval, the role moves into the **Active** state.
   - **Start Date** - Enter the start date. The role will be active on this date.

- **End Date** - (Optional) Leave this field blank to make the role active indefinitely, or enter an end date to schedule the last date that the role should be active.
- **Service Desk Ticket** - Add the helpdesk system reference number, if relevant to your organization.

5. Click **Next**.

   The **Select Owners** page opens.

6. Click **Add Owners** to select one or more owners for this role. For help using Search, see Section 6.3.1, "Searching for a User."

   Depending on how the system is configured, the list of users to choose from may only include users who have sufficient privileges to perform the Role Owner job.

7. Click **Next**.

   The **Select Users** page opens.

8. Click **Add Users** to select one or more users that you want to assign this role to. For help using Search, see Section 6.3.1, "Searching for a User."

9. Click **Next**.

   The **Select Policies** page opens.

10. Click **Add Policies** to select one or more policies to assign to this role.

11. Click **Finish** to create the role.

    The role is available in the **Roles** view under the **Identity Warehouse** tab.

6.6.3.2 To Create Roles From Existing Roles

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**.
3. Choose **New Role** > **Create Role Using an Existing Role as Template**.

   The Create Role pop-up window opens.

4. Complete the form:
   - **Name** - Type a name for the role.
   - **Template Role** - Click **Select Template Role**, search for the role that you want to use as a template for the new role, select the role, and click OK.
5. Click **Save** to create the role.

   The role is available in the **Roles** view under the **Identity Warehouse** tab.

6.6.3.3 To Create Roles Based On an Existing User

You can create a role based on an existing user. All of the entitlements that the selected user has are used to create corresponding policies that are assigned to the new role.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**.
3. Choose **New Role** > **Create Role From Existing User**.

   The Create New Role pop-up window opens.

4. Type a name for the role and click **Select User**.

The Search window opens.

5. Use either the user *quick search* or *advanced search* feature to search for the user whose entitlements will be used to create policies for the new role.

   For help using the search feature, see Section 6.3.1, "Searching for a User."

6. Select the user and click **OK**.

7. Click **Save** to create the role.

   The role is available in the **Roles** view under the **Identity Warehouse** tab.

6.6.4 To Rename, Modify, or Decommission (Delete) a Role

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**.
3. Search for a role, or select a role from the **Roles** panel on the left side of the screen. For help using the search feature, see Section 6.3.1, "Searching for a User."
4. Do one of the following tasks:
   - *To rename a role*, click the **General** tab, type the new role name in the **Name** field, and click **Save**. Or, *to modify a role*, type or select the new role properties, and click **Save**.

     Select the new version that was created for the role and click **Send for Approval**. See Section 6.6.1, "Understanding the Role Approval Process" for more information.
   - To delete a role, click the **Decommission Role** button. Decommissioning a role removes all role-user associations. The role itself, however, is not truly deleted. Instead, the role is made inactive and stored in Oracle Identity Analytics. The role cannot be made active again, and it cannot be modified in any way or assigned to users.

6.6.5 To Assign a User to a Role

Also see Section 6.3.7, "To Assign a Role to a User."

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**.
3. Click a role and click the **Users** tab.
4. Click to expand the **Composing** panel.
5. Click **Add Users** and add one or more users.
6. (Optional) To temporarily assign the role to the user, enter an **End Date** in the User-Role Association pop-up.

   To assign a user to a role indefinitely, leave the **End Date** blank.
7. Click **OK**.

6.6.6 To Associate Roles With Business Units

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**.
3. Click a role and click the **Business Structures** tab.

4. Click the **Add Business Structures** button and select the desired business units.
5. Click **Save**.

6.6.7 To Associate Role Owners With Roles

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**.
3. Click a role and click the **Ownership** tab.
4. Click the **Add Owners** button and search for the user (or users) to add.

   For help searching for users, see Section 6.3.1, "Searching for a User."

   Note: Depending on how the system is configured, only users who have the permissions required to manage the role will be listed.

5. Select one or more users.
6. Click **Save**.

   A new version of the role is created.
7. Select the new version of the role (the role should be in the Composing state) and click **Send for Approval**.

6.6.8 To Create a Role Hierarchy

Similar to a business unit hierarchy, an *n*-level role hierarchy can be defined in Oracle Identity Analytics. A role can have various "child roles" under it. To define a role hierarchy, add a new child role to it. When a child role is added to a user, the parent role is also automatically assigned to the user. The role hierarchy defines an organized structure of roles. Roles defined in an organization may have a hierarchy associated with them. In addition, enterprise-level roles and application-level roles can be defined.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**. The role hierarchy is defined when a new Role is created manually.

- To change a role hierarchy, follow these steps:
  a. Select the role and click the button located next to the **Parent Role** field on the **General** tab.
  b. From the list of roles that appear, select the role that you want to designate as the parent role.
- To select the child role for a user, follow these steps:
  a. Choose **Identity Warehouse** > **Users** and search for the user that you want to assign to a role.
  b. Select the user and click the **Role** tab.
  c. Click the **Add Roles** button. The parent Role is automatically assigned to the user. If the parent role is removed, the child role is automatically removed from the user.

6.7 Setting the Segregation of Duties at the Policy and Role Levels

The reason you define segregation of duties (SoD) is to separate certain duties or areas of responsibility so that they cannot be assigned to the same person. By defining segregation of duties, you reduce opportunities for unauthorized modification or misuse of data or services. Segregation of duties is a primary internal control intended to decrease the risk of errors or irregularities, identify problems, and ensure that corrective action is taken. This is done by assuring that no single individual has control over all phases of a transaction. Oracle Identity Analytics performs SoD at the policy level and, if enabled, the role level.

6.7.1 To Define Segregation of Duties at the Policy Level

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Policies**.
3. Click a policy to select it and go to the **Exclusion Policies** tab.
4. Click **Add Exclusion Policies**.
5. Add the policies to be excluded.
6. Click **Save**.

   A new version of the policy is created.
7. Select the new version of the policy (the policy should be in the Composing state) and click **Send for Approval**.

When a policy is added to a role, the excluded policies both cannot be assigned to the role.

6.7.2 To Define Segregation of Duties at the Role Level (Optional)

Note: The Exclusion Roles tab is hidden by default. To enable it, see the steps in the *System Integrator's Guide for Oracle Identity Analytics*, "Customizing the Oracle Identity Analytics User Interface" chapter, "Enabling Hidden Pages in the UI" section.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Warehouse** > **Roles**.
3. Click a role, then click the **Exclusion Roles** tab.
4. Click **Add Exclusion Roles**.
5. Add the roles that need to be excluded.
6. Click **Save**.

   A new version of the role is created.
7. Select the new version of the role (the role should be in the Composing state) and click **Send for Approval**.

7

Identity Certification

This chapter describes the identity certification user interface pages and includes information about how to complete identity certifications. An overview of identity certification is presented first.

This chapter contains the following sections:

7.1 Identity Certification Overview

This section describes what, why, and how identity certifications are conducted. It also discusses who is typically involved in the identity certification process.

7.1.1 What Is Identity Certification?

Identity certification is the process of reviewing user entitlements to ensure that users have not acquired entitlements that they are not authorized to have. Certifications can be scheduled to run on a regular basis to meet compliance requirements. Managers use the Oracle Identity Analytics (OIA) Identity Certification module to review their employees' entitlements to access applications and data. Based on changes reported by Oracle Identity Analytics, managers can authorize or revoke employee access, as needed.

The following table lists the four types of identity certification that are possible in Oracle Identity Analytics.

Table 7–1 The Four Types of Identity Certification

Identity Certification Type	Description
User Entitlement Certification	Allows managers to certify employee access to roles, accounts, and entitlements. This is the most common and most sweeping type of certification. Typically, each manager in an organization reviews the access-privileges of the people who report directly to that manager. Each reviewer in a certification of this type is focused on his or her direct-reports, but is expected to review all of the access-privileges for each of those people.

Table 7–1 (Cont.) The Four Types of Identity Certification

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

Business administrators are tasked with creating certifications for their organizations. For information about creating certifications, see the "Oracle Identity Analytics Identity Certifications" chapter in the *Administrator's Guide for Oracle Identity Analytics*.

7.1.2 What is Closed-Loop Remediation?

Closed-loop remediation is a feature that utilizes a separate provisioning system to automatically revoke roles and entitlements based on the results of the Oracle Identity Analytics certification process. Closed-loop remediation is only available if the provisioning solution is either Oracle Identity Manager or Oracle Waveset (Sun Identity Manager).

For non-managed applications, you can manually revoke roles and entitlements by using the information stored in the remediation configuration module.

For information about how to de-provision accounts during a certification process, see Section 7.4.7, "To De-provision Accounts During The Certification Process." Because OIA is the authoritative source for roles, when roles are revoked, Oracle Identity Analytics directly de-provisions them.

7.1.3 Who Is Involved in Completing Identity Certifications?

The identity certification module in Oracle Identity Analytics allows personnel in an organization to review and certify user entitlement data, role content data, and application access data. Following are descriptions of the types of users that are typically involved in the identity certification process, as well as the certifications that each user type can authorize or revoke. In Oracle Identity Analytics, personnel who participate in the identity certification process are called *actors*.

Table 7–2 Identity Certification Actors

Actor Name	Description	Certification Types That Can Be Accessed
Certifier	A generic term that signifies a person who is responsible for reviewing and completing any kind of certification.	■ User entitlement certification ■ Role entitlement certification ■ Resource entitlement certification ■ Data owner certification
User manager	A manager with direct reports. Users report to a user manager.	■ User entitlement
Access reviewer	Designated personnel responsible for reviewing user access.	■ User entitlement ■ Resource entitlement
Application owner	Designated personnel responsible for reviewing user access on a particular target system.	■ User entitlement ■ Resource entitlement
Role owner	Designated personnel responsible for reviewing role and its content.	■ Role entitlement
Data owner	Designated personnel responsible for reviewing access to an attribute value.	■ Data owner
Oracle Identity Analytics administrator	An administrator with full access to the Oracle Identity Analytics application and who can create and view the progress of all certifications.	■ User entitlement ■ Role entitlement ■ Resource entitlement ■ Data owner
Auditor or Audit analyst	Designated personnel who can view the Identity Certification Dashboard to view the progress of each certification. Can view reports from completed certifications.	■ Identity certification dashboard ■ Certification reports
Certification administrator	Administrator with limited access to the Oracle Identity Analytics application and who can only create and view the progress of certifications.	■ User entitlement ■ Role entitlement ■ Resource entitlement ■ Data owner

7.2 Understanding the Identity Certification User Interface

This section provides help using the identity certification portion of the user interface, which you access by clicking **Identity Certification** on the main menu.

7.2.1 The Dashboard

To open the identity certification dashboard, choose **Identity Certification > Dashboard** from the main menu.

The identity certification dashboard summarizes status information for certifications in progress. The information presented is customized based on your user access. For example, if you are logged in as an administrator with global access, the dashboard presents certification data for the entire organization. If you are logged in as a manager, however, the dashboard only presents information relevant to your particular business units.

The identity certification dashboard presents the following information.

Table 7–3 Certification Dashboard UI Descriptions

Dashboard Panel	Description
Certifications by Status	This bar graph compares certification statuses (new, in progress, complete, and expired) for each of the four certification types (user, role, resource, and data owner).
Summary	Provides the total number of users, accounts, resource types, and resources that are defined in Oracle Identity Analytics for your organization.
User Accounts Certification Status	This pie chart shows how many user accounts are marked as certified, revoked, and incomplete.
Notifications Issued in Last Week	This bar graph shows how many reminders have been sent in the last week to managers, senior managers, and the IT security department.
Statistics	Provides the average number of certifications per business structure, the average number of roles per user, the average number of accounts per user, and the average number of users in the average business structure.
User Roles Certification Status	This pie chart shows how many user roles are marked as certified, revoked, or incomplete.

7.2.2 Remediation Tracking

This page is visible only to administrators. To open the Remediation Tracking page, choose **Identity Certification > Remediation Tracking** from the main menu.

Use the Remediation Tracking page to track the remediation status of revoked accounts, access within accounts, or roles.

For details and instructions about using the Remediation Tracking page, see the Understanding Remediation Tracking section in the "Oracle Identity Analytics Identity Certifications" chapter in the *Oracle Identity Analytics 11gR1 Business Administrations Guide*.

7.2.3 Certification Jobs

This page is visible only to administrators. To open the Certifications Jobs page, choose **Identity Certification > Certification Jobs** from the main menu.

Use the Certification Jobs page to view the status of certification jobs and delete certification jobs.

For details and instructions about using the Certification Jobs page, see "Scheduling Certifications" in the "Oracle Identity Analytics Identity Certifications" chapter in the *Administrator's Guide for Oracle Identity Analytics*.

7.2.4 My Certifications

To open the My Certifications page, choose **Identity Certification > My Certifications** on the main menu.

Use the My Certifications page to view and search for certifications. If you are an administrator, you can create new access certifications from this page by clicking **New Certification** at the top of the page.

The My Certifications page displays new and in-progress certifications. Filters are provided to view all certifications, or any combination of new, in-progress, complete, or expired certifications. Click any column header to sort the table by the column type. Click again to reverse-sort the table.

In the **Certification Name** column, click a certification to view progress and to conduct employee verification on the selected certification.

- Click **Complete Certification** to complete a certification process.
- Click **View Reports** to view a report of a completed certification.
- Click **View Reminder Logs** to view notifications sent for a particular certification.

7.3 Understanding the Certification Pages

The following help topics document the pages that you use when completing a certification.

This section includes the following topics:

7.3.1 Certification Pages Overview

When you open a certification, a summary page displays that lists the certification items needing review. From the summary page you can navigate deeper into the certification and get a detailed view of each certification item. Both the summary and the detail pages include controls for filtering which certification items are displayed.

This section describes the user interface elements that are common to the certification pages.

The Certification Name

The top of the page displays the certification name. Certifications use the following naming convention:

Name-of-the-certification_Certifier's-last name_Certifier's-first-name

The Status Bar and More Info Icon

If the certification page is open to a summary page, a status bar and a certification details More Info icon also display.

- The **Completed** bar shows the percentage of the certification that is complete.
- Click the More Info icon to open a pop-up window that contains detailed information about the certification. See the topic for more information about the Certification Details pop-up window.

The Export-To Section

The **Export To** options enable you to work on the certification offline. You have to return to Oracle Identity Analytics, however, to complete the certification. You can export the certification to PDF or .xls formats.

> **Note:** The **Export To** options are only available on certification summary pages, not certification detail pages.

The Filter-Data-By Menu

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

> **Note:** Filter expressions with multiple criteria are evaluated using the "AND" operator.

The following filter controls may be available:

+ and **-**	Click to add and remove additional filter criteria.
Apply	Click to apply the filter and refresh the page.
Reset	Click **Reset** to remove all filtering and refresh the page.

If a filter is active, use the **First**, **Previous**, **Next**, and **Last** buttons to navigate from one record to the next.

Risk Level

In OIA, three red bars signifies high risk, two yellow bars signifies medium risk, one green bar signifies low risk.

7.3.2 User Entitlement Certification Help

User entitlement certification enables managers to certify employee access to roles, accounts, and entitlements. For step-by-step instructions about how to complete a user entitlement certification, see To Complete a User Entitlement Certification.

User Entitlement Certification Help is organized as follows:

- User Entitlement Certification - Summary Page
- User Entitlement Certification - Roles Detail Page
- User Entitlement Certification - Entitlements Detail Page

7.3.2.1 User Entitlement Certification - Summary Page

Filter-Data-By Menu (User Entitlement Certification - Summary Page)

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

Filter expressions with multiple criteria are evaluated using the "AND" operator.

All	Display all users.
Risk Summary	Display users by High, Medium, or Low risk levels. Risk Summary levels are based on the combined risk level of the roles, accounts, and entitlements that the user holds.
Entitlement Summary Risk	Display all users where the highest contributing Item-Risk or Risk-Factor level for any entitlement assigned to the user is High, Medium, or Low.
Role Summary Risk	Display all users where the highest contributing Item-Risk or Risk-Factor level for any role assigned to the user is High, Medium, or Low. **Note** - Filtering by Low Role-Summary Risk could return users who do not have any assigned roles. This is because the Low Role-Summary Risk filter excludes all users who have High-risk and/or Medium-risk roles assigned. Users who have only Low-risk roles assigned, and users who have no roles assigned, are returned.
Account Summary Risk	Display all users where the highest contributing Item-Risk or Risk-Factor level for any account assigned to the user is High, Medium, or Low.
Role Name	Display users with the role name that matches the search string provided. The asterisk (*) can be used as a wildcard.
Resource Name	Display users with a resource name that matches the search string provided. The asterisk (*) can be used as a wildcard.
Status	Display users by Claim, Decline, Delegate, or Disclaim status.**Note** - Status terminology is configurable. The terminology in use at your organization may differ from the terms listed here. ■ **Claim** - The user works for you and you are the correct person to complete the certification ■ **Decline** - The user does not work for you and you are not responsible for verifying his or her assigned roles and entitlements. ■ **Delegate** - The user reports to another manager who is responsible for verifying this user's assigned roles and entitlements. You will not approve or revoke roles and entitlements for this user. ■ **Disclaim** - The user is no longer part of the organization. The user is removed from the certification process and you will not approve or revoke roles and entitlements for this user.
User Attribute	Display users who meet the attribute criteria that you supply.

The Actions Menu (User Entitlement Certification - Summary Page)

Use the **Actions** menu to change status, reset status, or edit a comment for one or more entries in the certification.

Claim	The user works for you and you are the correct person to complete the certification.
Decline	The user does not work for you and you are not responsible for verifying his or her assigned roles and entitlements.
Delegate	The user reports to another manager. Select the manager who is responsible for verifying this user's assigned roles and entitlements. You will not approve or revoke roles and entitlements for this user.
Disclaim	The user is no longer part of the organization. The user is removed from the certification process and you will not approve or revoke roles and entitlements for this user.
Complete User	The users are valid for this certification.
Reset Status	Clear the decision column for the selected entries to indicate that no action has been taken.
Edit Comment	Modify the comment for the selected entries.

Summary Table (User Entitlement Certification - Summary Page)

The table on the summary page lists the certification items needing review.

User Name	The user's user ID. This is a unique value that identifies the user in your IT environment.
First Name	The user's first name.
Last Name	The user's surname.
Primary Email	The user's e-mail address.
Status	Displays *Decline*, *Delegate*, or *Disclaim* if that status was selected for the user. Otherwise, this field shows the percentage of the certification that is complete for this user. **Note** - Status terminology is configurable. The terminology in use at your organization may differ from the terms listed here. **Decline** - The user does not work for you and you are not responsible for verifying his or her assigned roles and entitlements **Delegate** - The user reports to another manager and you are not responsible for approving or revoking roles and entitlements for this user. **Disclaim Worker** - The user is no longer part of the organization. The user will be removed from the certification process and you will not approve or revoke roles and entitlements for this user.

Risk Summary	The risk level (High, Medium, or Low) assigned to the user based on the combined risk level of the roles and entitlements that the user holds. ■ **High-risk** users hold one or more high-risk roles/entitlements. ■ **Medium-risk** users hold one or more medium-risk roles/entitlements, and no high-risk roles/entitlements. ■ **Low-risk** users do not hold any high-risk or medium-risk roles/entitlements.
Roles	The total number of roles that the user holds.
Accounts	The total number of accounts that the user holds.
Entitlements	The total number of entitlements that the user holds.
Certification Comments	Reviewer comments entered about the user certification.

7.3.2.2 User Entitlement Certification - Roles Detail Page

The role detail page lists a user's assigned roles. To open the Roles Detail page, open a user entitlement certification and click the **Roles** tab.

Filter-Data-By Menu (User Entitlement Certification - Roles Detail Page)

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

Filter expressions with multiple criteria are evaluated using the "AND" operator.

Risk Summary	Display a user's roles based on the value recorded in the Risk Summary column.
Item Risk	Display the user's roles that have a matching risk value recorded in the Item Risk column.
Policy Violation	Display the user's roles that have a policy violation.
Last Certification	Display the user's roles based on the previous certification status.
Provisioning Methods	Display the user's roles based on the provisioned-by information returned by Oracle Identity Manger if OIM and OIA have been configured to work together.
Role Name	Display the user's roles that match the search string provided. The asterisk (*) character can be used as a wildcard.

The Actions Menu (User Entitlement Certification - Roles Detail Page)

Use the **Actions** menu to change status, reset status, or edit a comment for one or more entries in the certification.

Certify	The role is valid for this user for this certification.

Revoke	The role is not valid for this user for this certification.
Abstain	The user does not work for you and you are not responsible for verifying his or her assigned roles and entitlements.
Certify Conditionally	You temporarily certify the role even though the role might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
Reset Status	Clear the decision column for the selected entries to indicate that no action has been taken.
Edit Comment	Modify the comment for the selected entries.

Roles Detail Table (User Entitlement Certification - Roles Detail Page)

The table on the roles detail page lists a user's assigned roles.

Role Name	The name of the assigned role being certified.
Description	A description of the role.
Decision	One of the following: ■ **Certify** - The role is valid for this user for this certification. ■ **Revoke** - The role is not valid for this user for this certification. ■ **Certify Conditionally** - You temporarily certify the role even though the role might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
Risk Summary	The overall risk level for the role. This value is determined by choosing the highest risk level across the next four columns.
Item Risk	The risk level associated with the role as determined by an Oracle Identity Analytics administrator during the role configuration process.
Policy Violations	**Yes** if one or more policy violations result from this role assignment, otherwise **No**. One or more violations is considered to be high risk, and no policy violations is low risk.
Last Certification	The status of the previous certification of this role assignment. One of the following: **Certify**, **Revoke**, **Decline**, **Certify Conditionally**, or **New**.
Provisioning Method	The provisioned-by information returned by Oracle Identity Manger if OIM and OIA have been configured to work together.

Comments	Comments entered about this role by a reviewer.

7.3.2.3 User Entitlement Certification - Entitlements Detail Page

The entitlements detail page lists a user's accounts and entitlements that are assigned outside of any assigned roles. To open the Entitlements Detail page, open a user entitlement certification and click the **Entitlements** tab.

Filter-Data-By Menu (User Entitlement Certification - Entitlements Detail Page)

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

Filter expressions with multiple criteria are evaluated using the "AND" operator.

Risk Summary	Display a user's accounts and entitlements based on the value recorded in the Risk Summary column.
Item Risk	Display the user's roles that have a matching risk value recorded in the Item Risk column.
Policy Violation	Display the user's accounts and entitlements that have a policy violation.
Last Certification	Display the user's accounts and entitlements based on the previous certification status.
Provisioning Methods	Display the user's accounts and entitlements based on the provisioned-by information returned by Oracle Identity Manger if OIM and OIA have been configured to work together.
Resource Name	Display the user's accounts and entitlements by resource name. The asterisk (*) character can be used as a wildcard.
Resource Type	Display the user's accounts and entitlements by resource category.
Attribute	Display the user's entitlements by attribute name. The asterisk (*) character can be used as a wildcard.
Attribute Value	Display the user's entitlements by attribute value. The asterisk (*) character can be used as a wildcard.

The Actions Menu (User Entitlement Certification - Entitlements Detail Page)

Use the **Actions** menu to change status, reset status, or edit a comment for one or more entries in the certification.

Certify	The entitlement is valid for this user for this certification.
Revoke	The entitlement is not valid for this user for this certification.
Abstain	The user does not work for you and you are not responsible for verifying his or her assigned roles and entitlements.

Certify Conditionally	You temporarily certify the entitlement even though the entitlement might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
Reset Status	Clear the decision column for the selected entries to indicate that no action has been taken.
Edit Comment	Modify the comment for the selected entries.

Note: If you select all of the listed roles and entitlements when you choose an action, the system asks you to confirm if you want to "Select only entitlements that are displayed on the current page," or if you want to "Select all entitlements from this certification." Note that the "Select all entitlements from this certification" option applies only to the selection of roles and entitlements for the current user only. It does not apply to all of the roles and entitlements assigned to all of the users in the certification.

Entitlements Detail Table (User Entitlement Certification - Entitlements Detail Page)

The table on the entitlements detail page lists a user's assigned accounts and entitlements.

Note: Rows representing accounts are labeled (Account Only) in the Attribute Name column.

Resource Name	The name of the resource that has the accounts and entitlements that are being certified. (A resource is an application or some other enterprise information asset that users need to do their jobs.)
Resource Type	The resource category that the resource belongs to.
Account Name	The name of the user's account on the resource. Click the More-Info icon to see additional account details.
Attribute	Attributes are entitlements that map to different objects on a resource type. For example, *database name* is an attribute of MySQL™, *UID* is a UNIX attribute, and so on. **Note** - (Account Only) rows represent accounts.
Attribute Value	The value of the attribute listed. **Note** - Account rows do not have attribute values.

Decision	One of the following: ■ **Certify** - The entitlement is valid for this user. ■ **Revoke** - The entitlement is not valid for this user. ■ **Certify Conditionally** - You temporarily certify the entitlement even though the entitlement might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates. ■ **Abstain** - The user does not work for you and you are not responsible for verifying his or her assigned roles and entitlements.
Risk Summary	The overall risk level for the account or entitlement. This value is determined by choosing the highest risk level across the next four columns.
Item Risk	The assigned attribute-value risk or entitlement risk. The risk level is determined by an Oracle Identity Analytics administrator during the resource configuration process.
Policy Violations	**Yes** if one or more policy violations result from this role assignment, otherwise **No**. One or more violations is considered to be high risk, and no policy violations is low risk.
Last Certification	The status of the previous certification of this entitlement. One of the following: Certify, Revoke, Decline, Certify Conditionally, or New.
Provisioning Method	The provisioned-by information returned by Oracle Identity Manger if OIM and OIA have been configured to work together.
Comments	Comments entered about the account or entitlement by a reviewer.

7.3.3 Role Entitlement Certification Help

A role entitlement certification enables role owners to certify roles and role content, such as polices, entitlements, and users assigned to roles. For step-by-step instructions about how to complete a role certification, see To Complete a Role Entitlement Certification.

Role Entitlement Certification Help is organized as follows:

- Role Entitlement Certification - Summary Page
- Role Entitlement Certification - Policies Detail Page
- Role Entitlement Certification - Members Detail Page

7.3.3.1 Role Entitlement Certification - Summary Page

Filter-Data-By Menu (Role Entitlement Certification - Summary Page)

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

Filter expressions with multiple criteria are evaluated using the "AND" operator.

All	Display all roles.
Risk Level	Display the user's roles that have a matching role risk value recorded in the Risk Level column.
Role Name	Display roles that match the search string provided. The asterisk (*) character can be used as a wildcard.
Status	Display roles by Claim or Decline status. ■ **Claim** - The role belongs to you and you are the correct person to certify the content of the role. ■ **Decline** - The role does not belong to you and you are not responsible for verifying the content of the role.
Policy Violations	Display roles that have open identity auditing violations.

Actions Menu (Role Entitlement Certification - Summary Page)

Use the **Actions** menu to change status, reset status, or edit a comment for one or more entries in the certification.

Claim	The role belongs to you and you are the correct person to complete the certification.
Decline	The role does not belong to you and you are not responsible for verifying it.
Complete Roles	The remaining roles are valid for this certification.
Reset Status	Clear the decision column for the selected entries to indicate that no action has been taken.
Edit Comment	Modify the comment for the selected entries.

Summary Table (Role Entitlement Certification - Summary Page)

The table on the summary page lists the certification items needing review.

Role Name	The name of the role being certified.
Description	A description of the role.
Status	Either shows the percentage of the certification that is complete for this role, or *Decline*.
Risk Level	The risk level associated with the role as determined by an administrator during the role configuration process.

Policy Violations	Indicates if any open identity auditing violations are caused by this role. The identity audit component checks for identity relationships that go against policy, including segregation of duties (SoD) violations.
Policies	Shows the number of policies assigned to the role. Policies define account attributes and privileges that users have on different platforms or applications. A policy has a specific privilege on a specific data resource. Policies are assigned to roles, and roles are assigned to users.
Comments	Comments entered about this role certification by a reviewer.

7.3.3.2 Role Entitlement Certification - Policies Detail Page

The policies detail page shows policies that belong to this role, as well as attributes of the policy. To open this page, open a role entitlement certification and click the **Policies** tab.

Filter-Data-By Menu (Role Entitlement Certification - Policies Detail Page)

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

Filter expressions with multiple criteria are evaluated using the "AND" operator.

Resource Name	Display policies and attributes that have resource names that match the search string provided. The asterisk (*) character can be used as a wildcard.
Resource Type	Display policies and attributes that match the selected resource category.
Policy Name	Display policies and attributes that match the selected policy name.
Attribute Name	Display the attributes that match the attribute name search string provided. The asterisk (*) character can be used as a wildcard.
Attribute Value	Display the attributes that match the attribute value search string provided. The asterisk (*) character can be used as a wildcard.
Risk Summary	Display policies and attributes based on combined risk levels.
Item Risk	Display policies based on resource risk, and display attributes based on either the assigned attribute value risk or the entitlement risk.
Last Certification	Display policies and attributes based on the previous certification status.

Actions Menu (Role Entitlement Certification - Policies Detail Page)

Use the **Actions** menu to change status, reset status, or edit a comment for one or more entries in the certification.

Certify	The policy, entitlement, or user assigned to this role is valid for this certification.

Revoke	The policy, entitlement, or user assigned to this role is not valid for this certification.
Abstain	The policy, entitlement, or user does not belong to you and you are not responsible for verifying it.
Certify Conditionally	You temporarily certify the policy, entitlement, or user assigned to this role even though it might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
Reset Status	Clear the decision column for the selected entries to indicate that no action has been taken.
Edit Comment	Modify the comment for the selected entries.

Note: If you select all of the listed policies and entitlements when you choose an action, the system asks you to confirm if you want to "Select only policies that are displayed on the current page," or if you want to "Select all policies from this certification." Note that the "Select all policies from this certification" option applies only to the policies and entitlements assigned to the current role. It does not apply to all of the policies and entitlements assigned to all of the roles in the certification.

Policies Detail Table (Role Entitlement Certification - Policies Detail Page)

Note - Rows representing policies are labeled (Policy Only) in the Attribute Name column.

Resource Name	The name of the resource that the policy or the policy attribute relates to.
Resource Type	The resource category that the resource belongs to.
Policy Name	The name of the policy or the policy attribute that belongs to the role.
Attribute Name	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. Rows representing policies display as (Policy Only).
Attribute Value	The value of the attribute listed. Rows representing policies do not have attribute values.

Decision	One of the following: ■ **Abstain** - The policy or policy attribute does not belong to you and you are not responsible for verifying it ■ **Certify** - The policy or policy attribute is valid for this certification. ■ **Revoke** - The policy or policy attribute is not valid for this certification. ■ **Certify Conditionally** - You temporarily certify the policy or policy attribute even though it might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
Last Certification	The status of the previous certification of this policy or attribute. One of the following: **Certify**, **Revoke**, **Decline**, **Certify Conditionally**, or **New**.
Comments	Comments entered about this policy or policy attribute by a reviewer.

7.3.3.3 Role Entitlement Certification - Members Detail Page

The members detail tab shows all of the members that belong to this role. To open this page, open a role entitlement certification and click the **Members** tab.

Filter-Data-By Menu (Role Entitlement Certification - Members Detail Page)

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

Filter expressions with multiple criteria are evaluated using the "AND" operator.

User ID	Display role members who have account names that match the search string provided. The asterisk (*) character can be used as a wildcard.
Risk Summary	Display role members by High, Medium, or Low risk level. The Risk Summary level is based on the combined risk level of the roles, accounts, and entitlements that the user holds.
Policy Violation	Display role members who have one or more policy violations resulting from this role assignment.
Provisioning Method	Display role members based on the provisioned-by information returned by Oracle Identity Manger if OIM and OIA have been configured to work together.
Last Certification	Display role members based on the previous certification status.

Actions Menu (Role Entitlement Certification - Members Detail Page)

Use the **Actions** menu to change status, reset status, or edit a comment for one or more entries in the certification.

Certify	The policy, entitlement, or user assigned to this role is valid for this certification.
Revoke	The policy, entitlement, or user assigned to this role is not valid for this certification.
Abstain	The role does not belong to you and you are not responsible for verifying it.
Certify Conditionally	You temporarily certify the policy, entitlement, or user even though it might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
Reset Status	Clear the decision column for the selected entries to indicate that no action has been taken.
Edit Comment	Modify the comment for the selected entries.

Members Detail Table (Role Entitlement Certification - Members Detail Page)

User ID	The employee's user ID. This is a unique value that identifies the employee in your IT environment.
First Name	The user's first name.
Last Name	The user's surname.
Primary Email	The user's e-mail address.
Decision	One of the following: ■ **Abstain** - The role does not belong to you and you are not responsible for verifying it. ■ **Certify** - The user is valid for this role for this certification. ■ **Revoke** - The user is not valid for this role for this certification. ■ **Certify Conditionally** - You temporarily certify the user even though the user assignment might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
Risk Summary	The overall risk level for the user for this role. This value is determined by choosing the highest risk level across the next three columns.
Policy Violations	**Yes** if one or more policy violations result from this role assignment, otherwise **No**. One or more violations is considered to be high risk, and no policy violations is low risk.
Last Certification	The status of the previous certification of the user for this role. One of the following: **Certify**, **Revoke**, **Decline**, **Certify Conditionally**, or **New**.

Provisioning Method	The provisioned-by information returned by Oracle Identity Manger if OIM and OIA have been configured to work together.
Comments	Comments entered about this role user by a reviewer.

7.3.4 Resource Entitlement Certification Help

Resource entitlement certification involves certifying or revoking employee entitlements on one or more resources. Resource entitlements are entitlements that are assigned directly to an employee and are not assigned to an employee as part of a role. For step-by-step instructions about how to complete a resource certification, see Section 7.4.5, "To Complete a Resource Entitlement Certification."

Resource Entitlement Certification Help is organized as follows:

- Resource Entitlement Certification - Summary Page
- Resource Entitlement Certification - Accounts and Entitlements Detail Page

7.3.4.1 Resource Entitlement Certification - Summary Page

Filter-Data-By Menu (Resource Entitlement Certification - Summary Page)

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

Filter expressions with multiple criteria are evaluated using the "AND" operator.

All	Display all users.
Risk Level	Display resources by High, Medium, or Low risk level.
Resource Name	Display resources that match the search string provided. The asterisk (*) can be used as a wildcard.
Status	Display resources by Claim or Decline status. **Note** - Status terminology is configurable. The terminology in use at your organization may differ from the terms listed here. ■ **Claim** - The resource belongs to you and you are the correct person to complete the certification ■ **Decline** - The resource does not belong to you and you are not responsible for completing the certification.

Actions Menu (Resource Entitlement Certification - Summary Page)

Use the **Actions** menu to change status, reset status, or edit a comment for one or more entries in the certification.

Claim	Restores a disclaimed user, role, resource, or data source to your verification queue for certification.

Decline	Either the user does not work for you and you are not responsible for verifying his or her assigned roles and entitlements, or the role, resource, or data source does not belong to you and you are not responsible for verifying it.
Complete Resource	The remaining open accounts and entitlements for this resource are valid.
Reset Status	Clear the decision column for the selected entries to indicate that no action has been taken.
Edit Comment	Modify the comment for the selected entries.

Summary Table (Resource Entitlement Certification - Summary Page)

The table on the summary page lists the certification items needing review.

Resource Type	The resource category that the resource belongs to.
Resource Name	The name of the resource for which accounts and entitlements are being certified. Click the Resource Name link to open the Accounts and Entitlements Detail page.
Status	Shows Certify or Revoke if this resource certification is complete. Otherwise, this field shows the percentage of the certification that is complete for this resource.
Risk Level	The risk level of the named resource as determined by an Oracle Identity Analytics administrator during the resource configuration process.
Accounts	The total number of accounts that the named resource has.
Entitlements	The total number of entitlements that the named resource has.
Certification Comments	Comments entered about the resource certification by a reviewer.

7.3.4.2 Resource Entitlement Certification - Accounts and Entitlements Detail Page

The accounts and entitlements detail page shows the accounts and entitlements on the named resource. Click a Resource name on the Resource Entitlement Certification page to open this detail page.

Note - The rows representing accounts have *Attribute Name* labeled as *(Account Only)*.

Filter-Data-By Menu (Resource Entitlement Certification - Accounts and Entitlements Detail Page)

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

Filter expressions with multiple criteria are evaluated using the "AND" operator.

Attribute name	Display the entitlements that match the entitlement (attribute) name search string provided. The asterisk (*) character can be used as a wildcard.

Attribute Value	Display the entitlements that match the entitlement (attribute) value search string provided. The asterisk (*) character can be used as a wildcard.
Risk Summary	Display accounts and entitlements based on combined risk levels.
Item Risk	Display accounts based on resource risk, and display entitlements based on attribute value risk or entitlement risk.
Policy Violation	Display the accounts and entitlements that have a policy violation.
Last Certification	Display accounts and entitlements based on the previous certification status.
Provisioning Methods	Display role members based on the provisioned-by information returned by Oracle Identity Manger if OIM and OIA have been configured to work together.

Actions Menu (Resource Entitlement Certification - Summary Page)

Use the **Actions** menu to change status, reset status, or edit a comment for one or more entries in the certification.

Claim	The attribute or account is valid for this resource for this certification.
Decline	The attribute or account is not valid for this resource for this certification.
Reset Status	Clear the decision column for the selected entries to indicate that no action has been taken.
Edit Comment	Modify the comment for the selected entries.

Note: If you select all of the listed accounts and entitlements when you choose an action, the system asks you to confirm whether the action should be applied to "Items on this page only" or "All remaining items." Note that the "All remaining items" option applies only to the accounts and entitlements assigned to the current resource. It does not apply to all of the remaining accounts and entitlements in the certification.

Accounts and Entitlements Detail Table (Resource Entitlement Certification - Accounts and Entitlements Detail Page)

This table lists the accounts and entitlements on the named resource.

Account Name	The employee's user ID. This is a unique value that identifies the employee in your IT environment.
First Name	The user's first name.
Last Name	The user's surname.

Attribute Name	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. Rows representing policies display as (Policy Only).
Attribute Value	The value of the attribute listed.
Decision	One of the following: ■ **Abstain** - You are not responsible for verifying this entitlement. ■ **Certify** - The entitlement is valid for this user for this certification. ■ **Revoke** - The entitlement is not valid for this user for this certification. ■ **Certify Conditionally** - You temporarily certify the entitlement even though it might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
Risk Summary	The overall risk level for the account or attribute. This value is determined by choosing the highest risk level across the next four columns.
Item Risk	The assigned account risk or entitlement risk.
Policy Violations	**Yes** if one or more policy violations result from this role assignment, otherwise **No**. One or more violations is considered to be high risk, and no policy violations is low risk.
Last Certification	The status of the previous certification of this resource account or entitlement. One of the following: **Certify**, **Revoke**, **Decline**, **Certify Conditionally**, or **New**.
Provisioning Method	The provisioned-by information returned by Oracle Identity Manger if OIM and OIA have been configured to work together.
Comments	Comments entered about this account or entitlement by a reviewer.

7.3.5 Data Owner Certification Help

A data owner certification enables data owners to certify whether employees should be able to access data. For step-by-step instructions about how to complete a data owner certification, see Section 7.4.6, "To Complete a Data Owner Certification."

Data Owner Certification Help is organized as follows:

- Data Owner Certification - Summary Page
- Data Owner Certification - Entitlement Detail Page

7.3.5.1 Data Owner Certification - Summary Page

Filter-Data-By Menu (Data Owner Certification - Summary Page)

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

Filter expressions with multiple criteria are evaluated using the "AND" operator.

All	Display all users.
Status	Display certification items by Claim or Decline status.**Note** - Status terminology is configurable. The terminology in use at your organization may differ from the terms listed here. ■ **Claim** - The data source belongs to you and you are the correct person to complete the certification ■ **Decline** - The data source does not belong to you and you are not responsible for completing the certification.
Risk Level	Display data sources by High, Medium, or Low role risk level.
Resource	Display resources that match the search string provided. The asterisk (*) can be used as a wildcard.
Attribute	Display the entitlements that match the entitlement (attribute) name search string provided. The asterisk (*) character can be used as a wildcard.
Attribute Value	Display the entitlements that match the entitlement (attribute) value search string provided. The asterisk (*) character can be used as a wildcard.

Actions Menu (Data Owner Certification - Summary Page)

Use the **Actions** menu to change status, reset status, or edit a comment for one or more entries in the certification.

Claim	The data source belongs to you and you are responsible for verifying it.
Decline	The data source does not belong to you and you are not responsible for verifying it.
Reset Status	Clear the decision column for the selected entries to indicate that no action has been taken.
Edit Comment	Modify the comment for the selected entries.
Complete Value	The remaining users are valid for this certification.

Summary Table (Data Owner Certification - Summary Page)

The table on the summary page lists the certification items needing review.

Attribute	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.
Attribute Value	The value of the attribute listed.
Resource	The name of the resource where the data being certified resides.
Resource Type	The resource category that the resource belongs to.
Status	Shows **Declined** if you clicked the **Decline** button for the data source. Otherwise, this field shows the percentage of the certification that is complete for this data source.
Risk Level	The risk level (High, Medium, or Low) assigned to the entitlement / attribute-value on that row.
Users	Shows the number of users that have this entitlement.
Classification	Show the classification value for the attribute value.
Comments	Comments about this certification added by the certifier during the certification process.

7.3.5.2 Data Owner Certification - Entitlement Detail Page

The entitlement detail page shows users who have the entitlement. To open this detail page, click an entitlement in the **Attribute Value** column on the data owner certification page.

Filter-Data-By Menu (Data Owner Certification - Entitlement Detail Page)

The **Filter data by** menu allows you to filter items within a certification by various criteria, such as risk level, certification status, and so on.

Filter expressions with multiple criteria are evaluated using the "AND" operator.

Decision	.Display users whose Decision status matches the value selected. Select **All** to display all users
By User Attribute	Display users with attributes such as *User Name*, *First Name*, *City*, *Country* and so on that match the supplied value. The asterisk (*) character can be used as a wildcard.
Risk Summary	Display users by High, Medium, or Low risk level. Aggregated risk is based on the combined risk level of the roles, accounts, and entitlements that the user holds.
Last Certification	Display users based on the previous certification status.
Policy Violations	Display users who have one or more policy violations.
Provisioning Method	Display users based on the provisioned-by information returned by Oracle Identity Manger if OIM and OIA have been configured to work together.

Actions Menu (Data Owner Certification - Entitlement Detail Page)

Use the **Actions** menu to change status, reset status, or edit a comment for one or more entries in the certification.

Certify	The user entitlement is valid for this resource for this certification.
Revoke	The user entitlement is not valid for this resource for this certification.
Abstain	You are not responsible for verifying the user entitlement for this resource.
Certify Conditionally	You temporarily certify the user entitlement even though it might not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.
Reset Status	Clear the decision column for the selected entries to indicate that no action has been taken.
Edit Comment	Modify the comment for the selected entries.

Note: If you select all of the listed accounts when you choose an action, the system asks you to confirm whether the action should be applied to "Items on this page only" or "All remaining items." Note that the "All remaining items" option applies only to all of the accounts assigned the current attribute value. It does not apply to all of the accounts assigned to the remaining attribute values in the certification.

Entitlement Detail Table (Data Owner Certification - Entitlement Detail Page)

This table lists the users who have the selected entitlement.

Account Name	The name of the user's account on the resource. Click the More-Info icon to see additional account details.
First Name	The user's first name.
Last Name	The user's surname.
Decision	One of the following: ■ **Certify** - The user is valid for this entitlement for this certification. ■ **Revoke** - The user is not valid for this entitlement for this certification. ■ **Certify Conditionally** - You temporarily certify the user even though the user assigned to the entitlement may not be valid. Selecting this option requires you to enter an end date and you are prompted to annotate this record with a comment. The system includes the end date and comment when it generates reports. The system does not revoke the access or send out notices regarding expired end dates.

Risk Summary	The overall risk level for the user for this entitlement. This value is determined by choosing the highest risk level across the next three columns.
Policy Violations	**Yes** if the policy is causing a violation, otherwise **No**. A violation is considered to be high risk, and no policy violation is low risk. This value contributes to the overall risk level as shown in the Risk Summary column.
Last Certification	The status of the previous certification of this policy or attribute. One of the following: Certify, Revoke, Decline, Certify Conditionally, or New.
Provisioning Method	The provisioned-by information returned by Oracle Identity Manger if OIM and OIA have been configured to work together.
Comments	Comments entered about this user by a reviewer.

7.3.6 Certification Details Help

The certification details pop-up can be displayed by clicking the information icon found next to the certification name in the summary view for each type of certification.

The Certification Details pop-up window opens and displays information in the following sections:

- Certification Overview
- Certification History

Use the certification details page to view detailed information about a certification.

Note - The details displayed in the certification overview section varies based on the type of certification you have open.

7.3.6.1 Certification Overview

Table 7–4 Screen elements in the Certification Overview section of the Certification Details page

Details	Description
Certification	Displays the name of the certification. Certifications use the following naming convention: *Name-of-the-certification_Certifier's-last name_Certifier's-first-name*
Business structure	Displays the business structure selected for the certification.
Completed	Displays the progress (in percentage) of the certification completion.
Number of users	Displays the number of users that are part of the certification.
Number of roles	Displays the number of roles that are part of the certification.
Number of accounts	Displays the number of accounts that are part of the certification.
Number of resources	Displays the number of resources that are part of the certification.
Number of attribute values	Displays the number of attribute values that are part of the certification.
Certifier	Displays the name of the certifier.

Table 7–4 (Cont.) Screen elements in the Certification Overview section of the Certification Details page

Details	Description
Search button	Option to delegate the certification to another manager.

Note - The details displayed in the Certification Overview section varies depending on the certification page that you have open.

7.3.6.2 Certification History

Table 7–5 Screen elements in the Certification History section of the Certification Details page

Details	Description
Start Date	The suggested start date to perform the certification.
End Date	The date when the certification expires. Managers cannot review certifications after the expiration date.
Incremental	If a certification is marked as incremental, then certifiers are required to certify only the changes made to a certification after the last time it was certified. Otherwise, certifiers are required to complete the entire certification again.
Created By	Displays the name of the creator of the certification.
Creation Date	Displays the date of creation.
Last Updated By	Displays the name of the user who updated the certification.
Last Update Date	Displays the date of the last update.

7.3.7 Help for More-Info Pop-Up Pages

During the certification process you can view additional details about roles, accounts, attributes, and policies by clicking a More-Info link. When you click a More-Info link, one of four Meta Information pages opens. The following sections provide details about the Meta Information pages.

- "Role Meta-Information Pop-Up Help"
- "Accounts Meta-Information Pop-Up Help"
- "Attribute Meta-Information Pop-Up Help"
- "Policy Meta-Information Pop-Up Help"

7.3.7.1 Role Meta-Information Pop-Up Help

The Role Meta-Information Pop-Up consists of four sections:

- **General** - This section includes information about the role.
  - **General tab** - Displays basic information about the role.
  - **Business Structures tab** - Displays business structures associated with the role.
  - **Users tab** - Displays users assigned to the role.
  - **Exclusion Roles tab** - Displays conflicting roles. This helps define segregation of duties at the role level.
  - **Ownership tab** - Displays the role owner.

    - **Custom Properties tab** - Displays the custom properties associated with the role.
- **Rules** - This section displays rules associated with the role.
- **Certification History** - This section shows the certification history of the role. Information includes last date of action, the nature of the action, and comments, if any.
- **Policy Entitlements** - This section displays all the policies that are part of the role. All policy-related information, such as business structures, roles, resources, exclusion policies, ownership information, and entitlements, are displayed.
- **Provisioning Method** - (This section is available if the Oracle Identity Manager provisioning solution is enabled.) Provisioning Method provides information about how the item was provisioned to the system.
- **Open Audit Exception** - This section shows if the role is part of an open-audit exception. An open-audit exception is a violation that has not been fixed.

7.3.7.2 Accounts Meta-Information Pop-Up Help

The Accounts Meta-Information Pop-Up consists of four sections:

- **General** - This provides information about the account and its entitlements.
    - **Account** - This lists account information such as name, resource, and domain.
    - **Entitlement** - This lists information about the account's entitlements.
- **Open Audit Exception** - This section shows if the account is part of an open-audit exception. An open-audit exception is a violation that has not been fixed.
- **Certification History** - This section shows the certification history of the account. The information provided here includes a description of the action taken, the date that the action was taken, and comments, if any.
- **Provisioning Method** - (This section is available if the Oracle Identity Manager provisioning solution is enabled.) Provisioning Method provides information about how the item was provisioned to the system.
- **User Activity** - This section displays the user's recent account activity. The section is divided into two subtabs:
    - **Alerts -** Displays the alerts raised by the Intellitactics Security Information and Event Monitoring (SIEM) solution when it detects event violations based on the SIEM solution's internally defined rule set. The tab displays the alert title, description, time range, score, and status. These fields display the value captured by the SIEM solution.
    - **All Events -** Displays user activity events, which are collected by monitored endpoints by the Intellitactics SIEM system and reported in Oracle Identity Analytics as daily summarized data. The tab displays the event ID, event type, time range, count, and user ID. These fields display the value captured by the SIEM solution.

  Note - The User Activity section will be displayed if Oracle Identity Analytics is integrated with Intellitactics Security Manager, a security information and event monitoring solution. To learn more about Intellitactics Security Manager, see "Integrating with Intellitactics Security Manager" in the *Administrator's Guide for Oracle Identity Analytics*.

7.3.7.3 Attribute Meta-Information Pop-Up Help

The Attribute Meta-Information Pop-Up consists of the following sections:

- **General** - This section lists the attribute name, value, and glossary information. It also lists the attribute hierarchy, if any.
- **Certification History** - This section shows the certification history of the attribute. The information provided includes a description of the action taken, the date the action was taken, and comments, if any.
- **Provisioning Method** - (This section is available if the Oracle Identity Manager provisioning solution is enabled.) Provisioning Method provides information about how the item was provisioned to the system.

7.3.7.4 Policy Meta-Information Pop-Up Help

The Policy Meta-Information Pop-Up consists of three sections:

- **General** - This section includes information about the policy.
  - **General tab** - Displays basic information about the policy.
  - **Business Structures tab** - Displays the business structures associated with the policy.
  - **Ownership tab** - Displays the policy owner.
  - **Resources tab** - Displays all the resources associated with the policy.
  - **Exclusion Policies tab** - Displays conflicting policies. This helps define segregation of duties at the policy level.
  - **Roles tab** - Displays the roles associated with the policy.
  - **Entitlements tab** - Displays the attribute and the corresponding attributes values.
- **Open Audit Exception** - This section shows if the account is part of an open audit exception. An open audit exception is a violation, which is not fixed.
- **Certification History** - This section shows the certification history of the account. Information includes a description of the action taken, the date the action was taken, and comments, if any.

7.4 Completing Certifications

This section describes how to complete certifications in Oracle Identity Analytics. It includes the following topics:

7.4.1 To Find and Open Your Certifications

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Certifications > My Certifications**.
3. To search for specific certifications, use the **Show Me** drop-down menu, or click the expand icon on the left side of the page to open the Search panel.
   - The Show Me drop-down menu displays the following options: New & In Progress, All, New, In Progress, Complete, and Expired.
   - The search panel enables you to search for a certification using the following fields: Certification Name, Business Structure, Created By, Updated By.
   - Certifications use the following naming convention: *Name-of-the-certification_Certifier's-last name_Certifier's-first-name*.

   Note: - During certification, to obtain additional information about users, roles, attributes, and policies, click the More Info link.
4. Click a certification to open it.

   The Certification Details page opens.

7.4.2 To Delegate a Certification to Another User

Use the steps in this section if you want to delegate a particular certification to someone else.

Note: If you will be unable to complete certifications for an extended period of time, you can delegate certifications to another user to complete. Refer to Section 4.1.2.1, "To Delegate Certification-Related Duties to Another User" to delegate all certification completion tasks to another manager.

Before You Begin - Open your list of assigned certifications by following the steps in the Section 7.4.1, "To Find and Open Your Certifications" section.

1. Click to open the certification that you want to delegate.

   The Certification page opens.
2. Click the More Info icon next to the certification name on the summary page.

   Your name will be displayed as the certifier in the Certification Overview box.
3. Click the Search icon to search for a user to delegate the certification to. For help using Search, see Section 6.3.1, "Searching for a User."
4. Click Close.

7.4.3 To Complete a User Entitlement Certification

User Entitlement Certification enables managers to certify employee access to roles and related entitlements. To complete a user entitlement certification, follow these steps:

Before You Begin - Open your user entitlement certification. See Section 7.4.1, "To Find and Open Your Certifications" for instructions.

1. Reassign users who do not work for you.

   See Section 7.4.3.1, "Step One: Re-Assign Users Who do not Work for You"for more information.

2. Review users' roles and entitlements. Revoke the roles and entitlements that are no longer applicable and certify the rest.

   See Section 7.4.3.2, "Step Two: Review Roles and Entitlements and Revoke Those That No Longer Apply"for more information.

3. (Optional) Bulk certify multiple users with low risk levels.

   See Section 7.4.3.3, "Step Three: Bulk Certify Low-Risk Users (Optional)" for more information.

4. Complete the user entitlement certification.

   See Section 7.4.3.4, "Step Four: Complete the User Entitlement Certification" for more information.

7.4.3.1 Step One: Re-Assign Users Who do not Work for You

1. Review the certification and verify that the listed employees work for you and also that you are responsible for verifying their assigned roles and entitlements.
2. Remove users who do not belong in your verification queue by selecting the check box next to each user name and clicking one of the following buttons:
   - **Decline** - The employee does not work for you and you are not responsible for verifying his or her assigned roles and entitlements.
   - **Delegate** - The employee reports to another manager. Select the manager who is responsible for verifying this employee's assigned roles and entitlements. You will not approve or revoke roles and entitlements for this employee.
   - **Disclaim Worker** - The employee is no longer part of the organization. The employee is removed from the certification process and you will not approve or revoke roles and entitlements for this employee. To return a user to your verification queue, select the check box next to the user name and click the following button:
   - **Claim** - Restores a user to your verification queue for certification.

     Tip: For a description of the fields on the User Entitlement Certification user interface pages, see Section 7.3.2, "User Entitlement Certification Help."

7.4.3.2 Step Two: Review Roles and Entitlements and Revoke Those That No Longer Apply

Before You Begin - Complete the steps in Section 7.4.3.1, "Step One: Re-Assign Users Who do not Work for You."

1. Filter the users in your certification queue by risk level or assignment status by choosing an option from the **Filter Users By** menu.
   - **Show All** - Displays all users.
   - **Risk Level** - Display users by High, Medium, or Low risk level. Click **+** to add an additional filter option; click **-** to remove the filter option. Click **Apply** to apply the filter and refresh the page.
   - **Status** - Display users by Claim, Decline, Delegate, or Disclaim status.

Note: Status terminology is configurable. The terminology in use at your organization may differ from the terms listed here.

2. Click a user to review the employee's assigned roles.

   Tip: If the user has a large number of roles, use the **Filter Roles By** menu to view only High, Medium, or Low risk-level roles. For a description of the fields on the user entitlement user interface pages, see Section 7.3.2, "User Entitlement Certification Help."

3. Carry out the following actions as required:

   - **Revoke** - To revoke a role if the entitlement is not valid, select the applicable check boxes and click **Revoke**. Type a note in the Comments pop-up and click OK. If closed-loop remediation is configured, the accounts and entitlements that make up the revoked roles will be automatically de-provisioned.
   - **Certify Conditionally** - To temporarily certify one or more entitlements, even though the entitlements might not be valid, select the applicable check boxes and click **Certify Conditionally**. Use the **End Date** box to specify the date when the certification will expire, type a note in the **Comments** box, and click OK.
   - **Certify** - To certify one or more roles if they are valid for this user, select the applicable check boxes and click **Certify**. Type a note in the Comments pop-up and click OK.
   - **Decline** - Select the applicable check boxes and click **Decline** if you do not know if the employee's access is valid. The employee's access is neither certified nor revoked. The employee's access details appear in the certification report for post-certification action. When selecting Decline, you are prompted to annotate this record with a comment.

4. Click the Entitlements tab to review the user's entitlements that have been assigned outside of a role. Revoke, Certify Conditionally, Certify, and/or Decline the user's entitlements as needed.
5. Click **Back to Search Results** to review the next employee's assigned roles and entitlements and to revoke those that are no longer applicable.

7.4.3.3 Step Three: Bulk Certify Low-Risk Users (Optional)

The bulk certify action will certify the selected users and set the status to 100%. Any blank status on a role, an account, or an entitlement for the selected users will be set to Certify.

Before You Begin - For employees who do not have low risk levels, complete the steps in Section 7.4.3.2, "Step Two: Review Roles and Entitlements and Revoke Those That No Longer Apply."

1. To bulk certify multiple users, select the check box next to each user name and click the **Certify User** button.

   Note: Use the global check box at the top of the column to select all of the employees listed. In the dialog box, choose whether you want to certify only the users who are displayed on the current page, or if you want to certify all of the users in the certification.

2. Type a comment in the box and click OK.

7.4.3.4 Step Four: Complete the User Entitlement Certification

When all of the users are certified, the Complete Certification dialog box opens.

Note - To be complete, the Certification Details page should show 100% complete for all users.

1. Do one of the following:
   - To complete the certification, select **Yes**, type your password, and click **Submit**.
   - To edit the certification or return to the certifications page, select **Not right now**.

7.4.4 To Complete a Role Entitlement Certification

Role Entitlement Certification enables role owners to certify roles and role content. To complete a role entitlement certification, follow these steps:

Before You Begin - Open your role entitlement certification. See Section 7.4.1, "To Find and Open Your Certifications" for instructions.

1. Decline the roles that do not belong to you. See Section 7.4.4.1, "Step One: Decline the Roles That do not Belong to You" for more information.
2. Review the content of your roles. Revoke the policies, entitlements, and role members that are no longer correct and certify the rest. See Section 7.4.4.2, "Step Two: Review the Contents of Your Roles" for more information.
3. (Optional) Bulk certify roles with low risk levels. See Section 7.4.4.3, "Step Three: Bulk Certify Low-Risk Roles (Optional)" for more information.
4. Complete the role entitlement certification. See Section 7.4.4.4, "Step Four: Complete the Role Entitlement Certification" for more information.

7.4.4.1 Step One: Decline the Roles That do not Belong to You

1. Review the certification and verify that the listed roles belong to you and that you are responsible for verifying the roles and the role content.
2. Decline the roles that do not belong in your verification queue by selecting the check box next to each role name and clicking one of the following buttons:
   - **Decline** - The role does not belong to you and you are not responsible for verifying the role and its content.
   - **Claim** - The role belongs to you and you are responsible for verifying the role and its content.

     Tip: For a description of the fields on the Role Entitlement Certification user interface pages, see Section 7.3.3, "Role Entitlement Certification Help."

7.4.4.2 Step Two: Review the Contents of Your Roles

Before You Begin - Complete the steps in Section 7.4.4.1, "Step One: Decline the Roles That do not Belong to You."

1. Filter the roles in your certification queue by risk level by choosing an option from the **Filter Data By** menu.

2. Click a role to open the policies detail page. The policies detail page shows the policies that belong to this role, as well as the attributes (or entitlements) that make up each policy.
3. Review the role's policies and attributes.

   Tip: If the role has a large number of policies and attributes, use the **Filter Data By** menu to view only High, Medium, or Low risk-level items.

   For a description of the fields on the role entitlement user interface pages, see Section 7.3.3, "Role Entitlement Certification Help."

4. Carry out the following actions as required:
   - **Revoke** - To revoke a policy or attribute if it is not valid, select the applicable check boxes and click **Revoke**. Type a note in the Comments pop-up and click OK. If closed-loop remediation is configured, the policy or attribute will be automatically de-provisioned.
   - **Certify Conditionally** - To temporarily certify a policy or attribute, even though the policy or attribute may not be valid, select the applicable check boxes and click **Certify Conditionally**. Use the **End Date** box to specify the date when the certification will expire, type a note in the **Comments** box, and click OK.
   - **Certify** - To certify a policy or attribute if it is valid for this user, select the applicable check boxes and click **Certify**. Type a note in the Comments pop-up and click OK.
   - **Decline** - Select the applicable check box and click **Decline** if you do not know if the policy or attribute is valid. The policy or attribute is neither certified nor revoked. The role's details appear in the certification report for post-certification action. When selecting Decline, you are prompted to annotate this record with a comment.
5. Click the Members tab to review the users who have this role assigned. Revoke, Certify Conditionally, Certify, and/or Decline the role's members as needed.
6. Click **Back to Search Results** to review the next role's assigned policies and attributes and to revoke those that are no longer applicable.

7.4.4.3 Step Three: Bulk Certify Low-Risk Roles (Optional)

The **Complete Roles** action will certify the selected roles and set the status to 100%. Any blank status on a policy, attribute, or role member for the selected roles will be set to Certify.

Before You Begin - For roles that do not have low risk levels, complete the steps in Section 7.4.4.2, "Step Two: Review the Contents of Your Roles."

1. To bulk certify multiple roles, select the check box next to each role name and click the **Complete Roles** button.**Note** - Use the global check box at the top of the column to select all of the roles listed. In the dialog box, choose whether you want to certify only the roles that are displayed on the current page, or if you want to certify all of the roles in the certification.
2. Type a comment in the box and click OK.

7.4.4.4 Step Four: Complete the Role Entitlement Certification

When all of the roles are certified, the Complete Certification dialog box opens.

Note - To be complete, the Certification Details page should show 100% complete for all roles.

1. Do one of the following:
   - To complete the certification, select **Yes**, type your password, and click **Submit**.
   - To edit the certification or return to the certifications page, select **Not right now**.

7.4.5 To Complete a Resource Entitlement Certification

Resource Entitlement Certification involves certifying or revoking employee entitlements on one or more resources. Resource entitlements are entitlements that are assigned directly to an employee and are not assigned to an employee as part of a role. To complete a resource entitlement certification, follow these steps:

Before You Begin - Open your resource entitlement certification. See Section 7.4.1, "To Find and Open Your Certifications" for instructions.

1. Decline the resources that do not belong to you. See Section 7.4.5.1, "Step One: Decline the Resources That do not Belong to You" for more information.
2. Review the accounts and attributes (entitlements) that are assigned to users. Revoke the accounts and attributes that are no longer correct and certify the rest. See Section 7.4.5.2, "Step Two: Review Your Account and Attribute Assignments" for more information.
3. (Optional) Bulk certify resources with low risk levels. See Section 7.4.5.3, "Step Three: Bulk Certify Resources With Low-Risk Assignments (Optional)" for more information.
4. Complete the resource entitlement certification. See Section 7.4.5.4, "Step Four: Complete the Resource Entitlement Certification" for more information.

7.4.5.1 Step One: Decline the Resources That do not Belong to You

1. Review the certification and verify that the listed resource belongs to you and that you are responsible for verifying the resource accounts and attributes (entitlements) that are assigned to users.
2. Decline the resources that do not belong in your verification queue by selecting the check box next to each resource name and clicking one of the following buttons:
   - **Decline** - The resource does not belong to you and you are not responsible for verifying the users with accounts and entitlements on the resource.
   - **Claim** - The resource belongs to you and you are responsible for verifying the users with accounts and entitlements on the resource.

     Tip: For a description of the fields on the Resource Entitlement Certification user interface pages, see Section 7.3.4, "Resource Entitlement Certification Help."

7.4.5.2 Step Two: Review Your Account and Attribute Assignments

Before You Begin - Complete the steps in Section 7.4.5.1, "Step One: Decline the Resources That do not Belong to You."

1. Filter the resources in your certification queue by risk level by choosing an option from the **Filter Data By** menu.
2. Click a resource name to open the resource detail page. The resource detail page shows the accounts and attributes (entitlements) that are assigned to users.
3. Review the assigned accounts and attributes.

   Tip: If the resource has a large number of assigned accounts and attributes, use the **Filter Data By** menu to view only High, Medium, or Low risk-level items.

   For a description of the fields on the resource entitlement user interface pages, see Section 7.3.4, "Resource Entitlement Certification Help."

4. Carry out the following actions as required:
   - **Revoke** - To revoke an assigned account or entitlement if it is not valid, select the applicable check boxes and click **Revoke**. Type a note in the Comments pop-up and click OK. If closed-loop remediation is configured, the account or attribute will be automatically de-provisioned.
   - **Certify Conditionally** - To temporarily certify an assigned account or entitlement, even though the account or entitlement may not be valid, select the applicable check boxes and click **Certify Conditionally**. Use the **End Date** box to specify the date when the certification will expire, type a note in the **Comments** box, and click OK.
   - **Certify** - To certify an assigned account or entitlement, select the applicable check boxes and click **Certify**. Type a note in the Comments pop-up and click OK.
   - **Decline** - Select the applicable check box and click **Decline** if you do not know if the assigned account or entitlement is valid. The assigned account or entitlement is neither certified nor revoked. The resource's details appear in the certification report for post-certification action. When selecting Decline, you are prompted to annotate this record with a comment.
5. Click **Back to Search Results** to review the next role's assigned policies and attributes and to revoke those that are no longer applicable.

7.4.5.3 Step Three: Bulk Certify Resources With Low-Risk Assignments (Optional)

The **Complete Resource** action will certify the selected resources and set the status to 100%. Any blank status on an account or attribute (entitlement) for the selected resources will be set to Certify.

Before You Begin - For resources that do not have low risk levels, complete the steps in Section 7.4.5.2, "Step Two: Review Your Account and Attribute Assignments."

1. To bulk certify multiple resources, select the check box next to each resource name and click the **Complete Resource** button.

   Tip: Use the global check box at the top of the column to select all of the resources listed. In the dialog box, choose whether you want to certify only the resources that are displayed on the current page, or if you want to certify all of the resources in the certification.

2. Type a comment in the box and click OK.

7.4.5.4 Step Four: Complete the Resource Entitlement Certification

When all of the resources are certified, the Complete Certification dialog box opens.

Note - To be complete, the Certification Details page should show 100% complete for all resources.

1. Do one of the following:
   - To complete the certification, select **Yes**, type your password, and click **Submit**.
   - To edit the certification or return to the certifications page, select **Not right now**.

7.4.6 To Complete a Data Owner Certification

Data Owner Certification enables data owners to certify whether employees should be able to access data. To complete a data owner certification, follow these steps:

Before You Begin - Open your data owner certification. See Section 7.4.1, "To Find and Open Your Certifications" for instructions.

1. Decline any data sources that do not belong to you. See Section 7.4.6.1, "Step One: Decline the Data Sources That do not Belong to You" for more information.
2. Review the list of users who are assigned to the data source. Revoke the user accounts that should not have access and certify the rest. See Section 7.4.6.2, "Step Two: Review Your User Assignments" for more information.
3. (Optional) Bulk certify items with low risk levels. See Section 7.4.6.3, "Step Three: Bulk Certify Data Sources With Low-Risk Assignments (Optional)" for more information.
4. Complete the data owner certification. See Section 7.4.6.4, "Step Four: Complete the Data Owner Certification" for more information.

7.4.6.1 Step One: Decline the Data Sources That do not Belong to You

1. Review the certification and verify that the listed data sources belong to you and that you are responsible for verifying user access to the data.
2. Decline the data sources that do not belong in your verification queue by selecting the check box next to each Attribute/Attribute-Value name and clicking one of the following buttons:
   - **Decline** - The data source does not belong to you and you are not responsible for verifying the users with access privileges to the data.
   - **Claim** - The data source belongs to you and you are responsible for verifying the users with access privileges to the data.

     Tip: For a description of the fields on the Data Owner Certification user interface pages, see Section 7.3.5, "Data Owner Certification Help."

7.4.6.2 Step Two: Review Your User Assignments

Before You Begin - Complete the steps in Section 7.4.6.1, "Step One: Decline the Data Sources That do not Belong to You."

1. Filter the data sources in your certification queue by risk level by choosing an option from the **Filter Data By** menu.

2. Click an attribute value to open the entitlement detail page. The entitlement detail page shows the users who are assigned to the data source.
3. Review the list of assigned users.

   Tip: If the data source has a large number of assigned accounts and attributes, use the **Filter Data By** menu to view only High, Medium, or Low risk-level items.

   For a description of the fields on the resource entitlement user interface pages, see Section 7.3.5, "Data Owner Certification Help."

4. Carry out the following actions as required:
   - **Revoke** - To revoke a user account if it is not valid, select the applicable check boxes and click **Revoke**. Type a note in the Comments pop-up and click OK. If closed-loop remediation is configured, the account will be automatically de-provisioned.
   - **Certify Conditionally** - To temporarily certify a user, even though the user access may not be valid, select the applicable check boxes and click **Certify Conditionally**. Use the **End Date** box to specify the date when the certification will expire, type a note in the **Comments** box, and click OK.
   - **Certify** - To certify a user, select the applicable check boxes and click **Certify**. Type a note in the Comments pop-up and click OK.
   - **Decline** - Select the applicable check box and click **Decline** if you do not know if the user access is valid. The user access is neither certified nor revoked. The details appear in the certification report for post-certification action. When selecting Decline, you are prompted to annotate this record with a comment.
5. Click **Back to Search Results** to review the next role's assigned policies and attributes and to revoke those that are no longer applicable.

7.4.6.3 Step Three: Bulk Certify Data Sources With Low-Risk Assignments (Optional)

The **Complete User Access** action will certify the selected data sources and set the status to 100%. Any blank status on a user account for the selected data sources will be set to Certify.

Before You Begin - For data sources that do not have low risk levels, complete the steps in Section 7.4.6.2, "Step Two: Review Your User Assignments."

1. To bulk certify multiple data sources, select the check box next to each attribute-name/attribute-value and click the **Complete User Access** button.**Note** - Use the global check box at the top of the column to select all of the data sources listed. In the dialog box, choose whether you want to certify only the data sources that are displayed on the current page, or if you want to certify all of the data sources in the certification.
2. Type a comment in the box and click OK.

7.4.6.4 Step Four: Complete the Data Owner Certification

When all of the data sources are certified, the Complete Certification dialog box opens.

Note - To be complete, the Certification Details page should show 100% complete for all data sources.

1. Do one of the following:

- To complete the certification, select **Yes**, type your password, and click **Submit**.
- To edit the certification or return to the certifications page, select **Not right now**.

7.4.7 To De-provision Accounts During The Certification Process

As a certifier, you can directly de-provision the accounts or roles you revoke during the certification process. Please check with your Oracle Identity Analytics administrator if this feature is configured.

To check and de-provision accounts, do the following:

1. Review and certify or revoke access to accounts, attributes, roles, policies and entitlements.
2. Select 'revoke' from the drop-down menu against an account, attribute, role or policy.
3. Click the hyperlinked resource name under the resource column.
4. Follow the steps.

Note - If Oracle Identity Analytics is integrated with Oracle Waveset (Sun Identity Manager), then revoked accounts will be de-provisioned automatically.

7.5 Viewing Certification Reports

Managers can view or export reports of completed certifications. Various reports are available for each certification type.

7.5.1 To View a Certification Report

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Certifications** > **My Certifications**.
3. Choose **Complete** from the **Show Me** drop-down menu.

   A list of completed certifications is displayed.
4. Click the certification that you want to view.
5. Select the type of report you want to view and click OK.

   The report is displayed.
6. Click **Actions** to either print or export the report.

7.5.2 Certification Reports Available in Oracle Identity Analytics

This section details the various certification reports that are available in Oracle Identity Analytics.

Table 7–6 User Entitlement Certification Reports

Reports Available	Description
Revoked access report	Lists access marked as revoked.
Certified access report	Lists access marked as certified.
Terminated users report	Lists employees that were marked as terminated.

Table 7–6 (Cont.) User Entitlement Certification Reports

Reports Available	Description
Completed certification report	Comprehensive report of a user entitlement certification. This report includes a list of all employees and their access.
Abstain report	Lists certification items that the certifier declined to complete because the certifier is not responsible for verifying the user's assigned roles and entitlements.
Certify conditionally report	Lists access that the certifier temporarily certified, even though the access may not be valid. Certifiers are required to enter an end date, which are included in this report, however, the system does not revoke the access or send out notices regarding expired end dates.

Table 7–7 Role Entitlement Certification Reports

Reports Available	Description
Revoked entitlement report	Lists entitlements marked as revoked.
Certified entitlement report	Lists entitlements marked as certified.
Complete certification report	Comprehensive report of a role entitlement certification.

Table 7–8 Resource Entitlement Certification Reports

Reports Available	Description
Revoked entitlement report	Lists entitlements marked as revoked.
Certified entitlement report	Lists entitlements marked as certified.
Completion certification report	Comprehensive report of a resource entitlement certification.

Table 7–9 Data Owner Certification Reports

Reports Available	Description
Certify Access report	Lists access marked as certified.
Revoked access report	Lists access marked as revoked.
Declined report	Lists access that the certifier declined to review because the data source does not belong to the certifier
Complete data ownership report	Comprehensive report of a data owner certification including revoked and certified access.

8 Identity Audit

This chapter describes the identity audit user interface pages and includes information about how to complete an identity audit.

This chapter contains the following sections:

8.1 Identity Audit Overview

The Identity Audit module is designed to detect segregation of duties (SoD) violations. A *segregation of duties violation* is a violation whereby a user account, a user attribute, or a role has been assigned two entitlements that should not be held in combination.

While the identity certification module enables managers to certify or revoke access of users, the identity audit module has a detection mechanism that monitors users' actual access to resources and captures any violations on a continuous basis. The software can also be programmed to conform to audit policies and report exceptions. It provides a summary of all exceptions, which helps security analysts, executives, or auditors accept or mitigate the exceptions.

In Oracle Identity Analytics, audit rules define violations. Audit rules are collected together to create an audit policy. User accounts and business structures are then scanned for audit policy violations. User accounts, user attributes, and roles that violate an identity audit policy are flagged and tracked until the violation is resolved.

Use the Identity Audit module to create and track audit rules, audit policies, and audit policy violations throughout the audit lifecycle. The module maintains a history of audit scans.

8.2 Understanding the Identity Audit User Interface

This section provides help using the Identity Audit portion of the user interface.

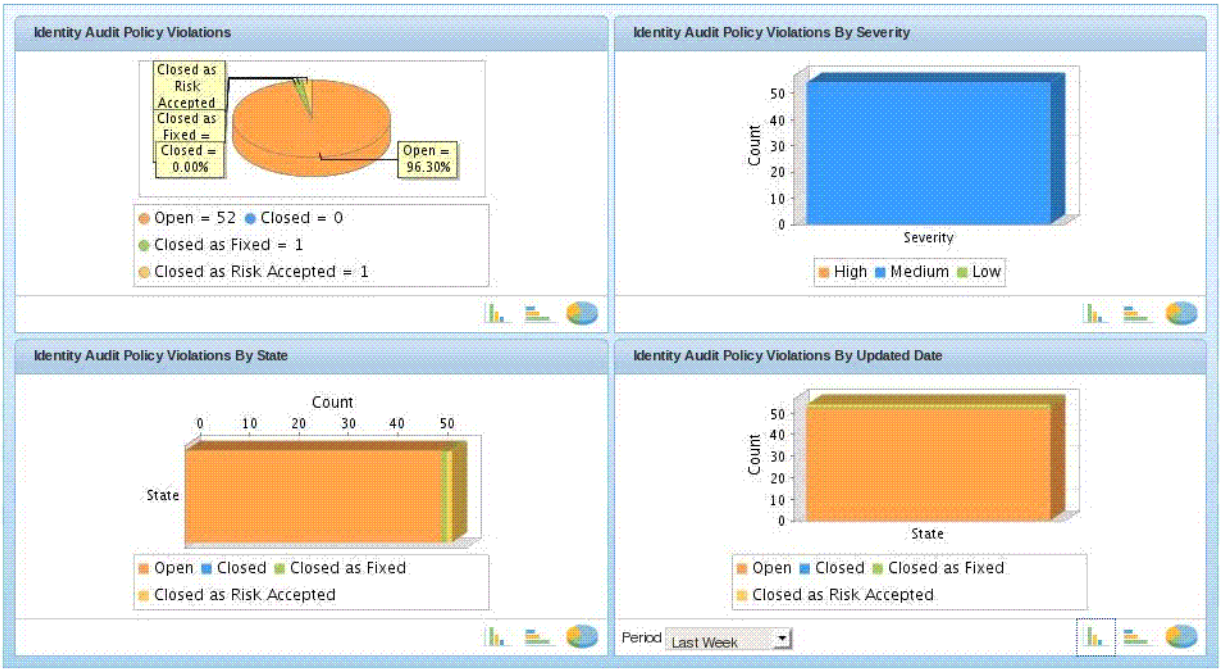
8.2.1 The Dashboard

To open the identity audit dashboard, choose **Identity Audit** > **Dashboard** from the main menu.

The identity audit dashboard summarizes identity audit policy violation status information. It displays graphs that enumerate the number of violations, and lists violations by state, priority, and date-of-last-update. The following four graphs are displayed:

- Identity Audit Policy Violations
- Identity Audit Policy Violations By State
- Identity Audit Violation By Severity
- Identity Audit Policy Violations By Updated Date

Figure 8–1 The Identity Audit Dashboard



To change the view of the graphs, click the "three graphs" icon in the lower right corner of each panel.

To change the time period that the Dashboard reports on, click the **Period** drop-down menu at the bottom-right of the screen.

8.2.2 Policies

To open the identity audit Policies page, choose **Identity Audit** > **Policies** from the main menu.

Use the Identity Audit Policies page to edit and run audit policies, as well as to preview audit policies and view the results of completed audit policy scans. Click the **New Policy** button to create a new audit policy.

8.2.3 Rules

To open the identity audit Rules page, choose **Identity Audit** > **Rules** from the main menu.

Use the identity audit Rules page to create and edit audit rules.

8.2.4 Policy Violations

To open the identity audit Policy Violations page, choose **Identity Audit** > **Policy Violations** from the main menu.

The audit Policy Violations page has the following subtabs.

Open Violations Tab

This page displays all the violations that are not yet fixed by the remediator. You can view the open violations by clicking them.

Closed Violations Tab

Displays all violations that have been addressed by a remediator and closed.

8.3 Understanding Audit Policy Violations

An audit policy violation occurs if one or more rules associated with a policy is broken by a user account, a user attribute, or a user role. Oracle Identity Analytics tracks the violation until it is resolved.

Audit policies have designated remediators who are responsible for taking action when violations are discovered.

The following three actors can be remediators:

- Rbacxadmin
- Policy Owner
- Remediator (designated person assigned during policy creation)

A remediator can reassign violations to another user so that action can be taken to resolve the violation. The remediator is mentioned in the audit trail of every violation, thereby making the remediator accountable for the action.

Each broken rule, as well as the user, account, role, and membership details that caused the violation are recorded. Each Identity Audit Violation contains at least one cause. When more than one rule in the policy matches, then the violation will have multiple causes. Violation causes are displayed on the Violation Details page under three different categories:

- Account Causes
- Role Causes
- HR Attribute Causes

For more information about the Audit Violation Details page, see Section 8.4.3, "Audit Violation Details Help.".

8.4 Acting on Audit Policy Violations

The following procedures describe how to take action on audit policy violations.

8.4.1 To Assign an Audit Policy Violation to Another User

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Audit** > **Policy Violations**.

   A list of open violations is displayed.

3. Click a violation in the **Exception** column.

   The Policy Violation Details page opens.

4. To reassign the violation to another user, click **Reassign To** in the **Violation Details** section.

   A page asking you to select another remediator opens.

5. Use search to choose another user. For help using search, see Section 6.3.1, "Searching for a User."

6. Click OK.

8.4.2 To View and Take Action on Audit Policy Violations

1. Log in to Oracle Identity Analytics.

2. Choose **Identity Audit** > **Policy Violations**.

   A list of open violations is displayed.

   Audit policy violations can be sorted by four different states:

   - **Open** - The remediator has not yet taken any action on the violation.
   - **Closed** - The remediator has closed the violation.
   - **Closed and Fixed** - The remediator has fixed the violation and therefore it should not appear in the next policy scan.
   - **Closed as Risk Accepted** - The remediator has acknowledged the violation and opted to allow the access for a certain time period.

3. Click a violation in the **Exception** column.

   The Policy Violations Details page opens.

4. To take action on the violation, review the user's access.

   To understand the Audit Violations page, see Section 8.4.3, "Audit Violation Details Help."

   - If you click **Close Violation** or **Close as Fixed**, a comment box opens.

     Enter a comment for future reference and click OK.

   - If you click **Close as Risk Accepted**, enter a comment and an end date, after which time the exemption will expire, then click OK.

8.4.3 Audit Violation Details Help

When taking action on an open violation (see Section 8.4.2, "To View and Take Action on Audit Policy Violations"), the Policy Violation Details page displays the following information.

Violation Details Section

Table 8–1 Violation Details Section of the Policy Violation Details Page

Field	Description
Policy	Displays the name of the policy
Assigned To	Displays the remediator's name.
Reassign To	Allows you to reassign the violation to another user.

Table 8–1 (Cont.) Violation Details Section of the Policy Violation Details Page

Field	Description
Assigned Date	The date when the policy was assigned to the remediator.
State	Displays the state of the violation.
Detection Count	The number of scans in which the violation was detected.
Last Detected	Last time the violation was found in an identity audit scan.
Expiration Date	Displays the expiration date of a "Close as Risk Accepted" violation.
Close Date	The date a remediation action was taken and the violation was moved to one of the "Closed" states.
Comments	Displays any comments added by the remediator.

User Details Section

Table 8–2 Users Details Section of the Policy Violation Details Page

Field	Description
Name	Displays the name of the user.
Department	Displays the user's department.
E-mail	Displays the user's e-mail ID.
User Name	Displays the user name.
Manager	Displays the name of the manager.
Job Title	Displays the user's job title.

Accounts Section

The accounts section displays the user account that resulted in an identity audit violation.

Table 8–3 Accounts Section of the Policy Violation Details Page

Field	Description
Name	Displays the name of the account under violation.
Resource Type	Displays the resource type under violation.
Resource	Displays the resource under violation.
Rule	Displays the identity audit rule.
Condition	Displays the identity audit rule condition.
Status	Displays the state of the rule.

Roles Section

The Roles section displays the name of the user role that resulted in the identity audit violation.

Table 8–4 Roles Section of the Policy Violation Details Page

Field	Description
Name	Displays the role under violation.

Table 8–4 (Cont.) Roles Section of the Policy Violation Details Page

Field	Description
Rule	Displays the identity audit rule.
Condition	Displays the identity audit rule condition.
Status	Displays the state of the rule.

HR Attributes Section

The HR Attributes section displays the user attributes and values that resulted in the violation. If the violation occurred due to a business structure membership, the name of the business structure is displayed.

Table 8–5 HR Attributes Section of the Policy Violation Details Page

Field	Description
Attributes	Displays the HR attribute under violation.
Rule	Displays the identity audit rule.
Condition	Displays the identity audit rule condition.
Status	Displays the state of the rule.

8.4.4 To View Audit Trails

An audit trail is a permanent history of every audit violation identified by Oracle Identity Analytics as well as all subsequent actions taken to resolve the violation.

The audit trail is updated whenever a violation is updated or modified. The audit trail tracks date information (when actions were taken), as well as any changes that affect the user, state, remediator, and comments fields.

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Audit** > **Policy Violations**.
3. To view the audit trail of a violation, do the following:
   a. Click **Open Violations** in the submenu bar to view the audit trail of an open violation, or click **Closed Violations** in the submenu bar to view the audit trail of a closed violation.
   b. Select the violation.

      The Violations Details page opens.
   c. Click the **Audit Trail** page option.

      The audit trail for the violation is displayed.
   d. Use the **Search** feature to search by name in the **Assigned To** field.

      Note: You can only search the **Assigned To** field. The Audit Trail Search feature does not search any of the other fields on the Audit Trail page.

8.4.5 To Export A Violation

1. Log in to Oracle Identity Analytics.
2. Choose **Identity Audit** > **Policies**.

All the identity audit polices are listed.

3. Select the desired policy whose violations you want to export.
4. Click **Export Violations**.
5. Select the options to generate your report:
   - **Report Format** - Select the report format. Formats include PDF, CSV, XML, HTML, or XLS.
   - **Violations to be exported** - Select from the options listed.
6. Click Ok.

9 Reports

This chapter contains the following sections:

9.1 Overview

This chapter describes the various reports that can be generated in Oracle Identity Analytics. Reports are valuable tools that auditors and end-user managers can use to evaluate, analyze, and review access controls in the organization.

Reports are broadly classified as follows:

- *Business structure reports*: Out-of-the-box reports that run on selected business structures.
- *System reports*: Out-of-the-box reports that are run on all users, roles, or policies in Oracle Identity Analytics.
- *Identity Audit reports*: Open-audit exception reports based on audit policy scans.
- *Custom reports*: Reports customized according to the requirements of your organization.

9.2 Understanding the Reports User Interface

This section provides help using the Reports portion of the user interface.

9.2.1 The Dashboard

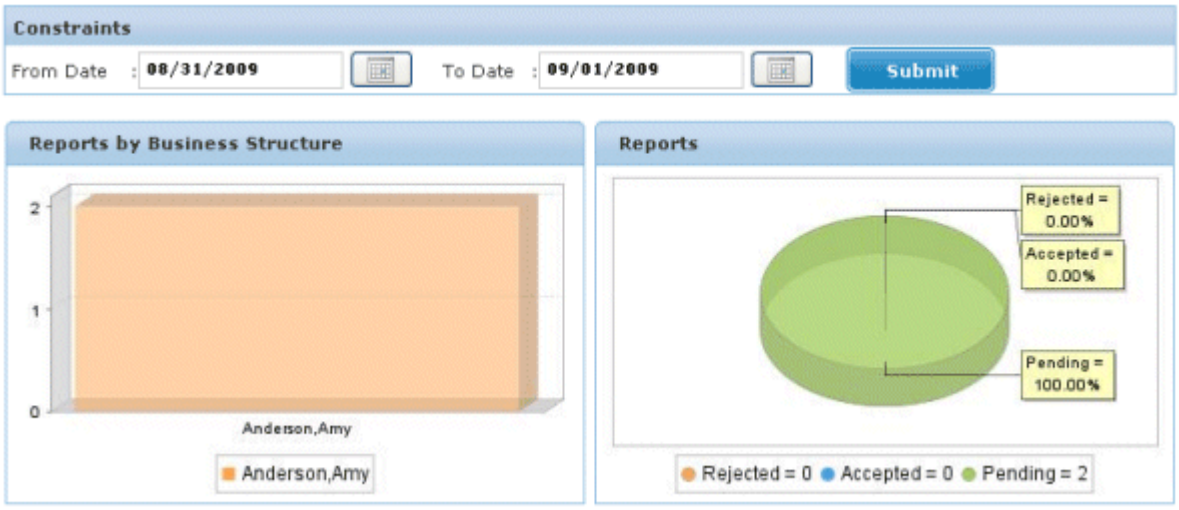
To open the reports dashboard, choose **Reports** > **Dashboard** from the main menu.

The reports dashboard summarizes status information for reports. The two graphs are the following:

- Reports by Business Structure.

- Reports which are pending, accepted or rejected by the managers.

Figure 9–1 The Reports Dashboard



9.2.2 Sign Off Reports

To open the Sign Off Reports page, choose **Reports** > **Sign Off Reports** from the main menu.

Use the Sign Off Reports page to sign off on pending reports and to view completed reports.

9.2.3 Ad Hoc Reports

To open the Ad Hoc Reports page, choose **Reports** > **Ad Hoc Reports** from the main menu.

The Ad Hoc Reports page has four subtabs: **Business Structure Reports**, **System Reports**, **Identity Audit Reports**, and **Custom Reports**. These reports can be run at any given time.

Use this page to run these reports and to download them.

9.2.4 Schedule Reports

To open the Schedule Reports page, choose **Reports** > **Schedule Reports** from the main menu.

Use the Schedule Reports page to generate specific reports at regular intervals.

9.2.5 Custom Reports

To open the Custom Reports page, choose **Reports** > **Custom Reports** from the main menu.

The Custom Reports page helps you to create customized reports based on the needs of your organization. Creating custom reports is an administrative function. See the "Oracle Identity Analytics Reports" chapter in the *Administrator's Guide for Oracle Identity Analytics* to create a custom report.

9.3 Working With Reports

This section describes how to schedule and approve reports.

9.3.1 To Schedule Reports

1. Log in to Oracle Identity Analytics.
2. Choose **Reports** > **Schedule Reports**.
3. Click **New Report Job**.
4. Complete the form:
   - **Name**: Enter the name of the report.
   - **Description**: Enter a description for the report.
   - **Report Name**: Choose a report from the drop-down menu.

     All out-of-the-box reports and custom reports are listed.
   - For a one-time-only report, set the date and time to schedule the report.

     For a recurring report, set the time to schedule the report.

     Note: When scheduling a *one-time-only* report, the report runs at the scheduled date and time in your local time zone (that is, the *client computer* time zone).

     When scheduling a *recurring* report, the report will run at the scheduled time in the time zone configured on the server (the *server computer* time zone).
5. Click **Create**.

9.3.2 To Sign Off on Reports

1. Log in to Oracle Identity Analytics.
2. Choose **Reports** > **Sign Off Reports**.
3. Select the report that you want to sign-off on from the **Pending Reports** section.
4. Review the contents of the report. Select one of the following:
   - **Accept**
   - **Reject**
5. After signing off, the report is displayed in the **Completed Reports** section.

9.4 Defining Business Structure Reports

The following table describes the different business structure reports that Oracle Identity Analytics can generate.

Table 9–1 Business Structure Reports in Oracle Identity Analytics

Report	Description
Business structure roles report	Lists all the roles under each business structure.

Table 9–1 (Cont.) Business Structure Reports in Oracle Identity Analytics

Report	Description
Business structure role users report	Lists all the roles and the assigned users under each business structure.
Business structure user roles report	Lists all the users and their assigned roles under each business structure.
Business structure users report	Lists all the users under each business structure.
Business structure user entitlements report	Lists all the users, under each business structure, with their entitlements.
User certification report	Lists all the users, under selected business structure, their roles and associated entitlements.
Business structure role policies report	Lists all the roles and associated policies under each business structure.
Data owner report	Lists all the entitlements and its owner.
Business structure resource type entitlement report	Lists all the users, under selected business structure, their associated resource types and entitlements.

9.4.1 To Generate Business Structure Reports

1. Log in to Oracle Identity Analytics.
2. Choose **Reports** > **Ad Hoc Reports**.
3. Select **Business Structure Reports** to view a report under this section.
4. Select the report that you want to view and click **Run**.

   A window opens.
5. Select the Business Structure and click **OK**.

   The report is displayed.
6. Click the **Actions** drop-down menu for options to export the report in other formats. Formats 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.

9.5 Defining System Reports

System reports are further classified as follows:

- Roles reports
- Policy reports
- User reports
- Exception reports
- Forecast reports

The different system reports that can be generated are described in the following tables.

Table 9–2 "Role" System Reports in Oracle Identity Analytics

Report	Description
Role Policies Report	Lists the roles and associated policies of different applications within those roles.
Roles Users Report	Lists all roles and assigned users.

Table 9–3 "Policy" System Reports in Oracle Identity Analytics

Report	Description
Policy Roles Report	Lists the roles in a policy.
Policy Resource Types Report	Lists policies by resource type.
Policy Attributes Report	Lists the attributes in a policy.

Table 9–4 "User" System Reports in Oracle Identity Analytics

Report	Description
Policies Attribute Report	Lists the attributes in a policy.
User Business Unit Report	Lists the business units under a user.
User Role Report	Lists the roles under a user.
User Role Business Structure Report	Lists the business structures under a role, which is under a user.
User Application Report	Lists the applications under a user.
User Account Report	Lists the accounts under a user.
User Role-Based Access Report	Lists the attributes under a policy in a resource type under a user.

Table 9–5 "Exception" System Reports in Oracle Identity Analytics

Report	Description
Operational Exception Report	Reports the missing data required for correlations in Oracle Identity Analytics.
Import Validation Report	A set of reports displaying the data that has not been imported into Oracle Identity Analytics from the daily scheduled dumps.

Table 9–6 "Forecast" System Reports in Oracle Identity Analytics

Report	Description
Expiration Forecast Report	The report contains three subreports: User expiration, Role expiration, and User-Role Association expiration. It provides a list of all the expirations occurring in the current week.

9.5.1 To Generate System Reports

1. Log in to Oracle Identity Analytics.
2. Choose **Reports** > **Ad Hoc Reports**.
3. Click **System Reports** and refer to the previous tables to determine the section.

4. Click the section and click **Run** against the Report Name that you want to view. The report is displayed.
5. Click the Actions drop-down menu for options to export the file in other formats. Formats include PDF, XLS, CSV, HTML, XML, and print.
6. (Optional) To download the report, click **Download** in either the **Download PDF Report** column or the **Download CSV Report** column.

9.6 Defining Identity Audit Reports

The different identity audit reports that can be generated are described here.

Table 9–7 Identity Audit Reports in Oracle Identity Analytics

Report	Description
All Open Audit Exceptions Report	Provides a list of audit-related exceptions, including Segregation of Duties, Assigned vs. Actual Rights Violation, and Terminated User reports.
Latest Open Audit Exceptions Report	Provides a list of audit-related exceptions, including Segregation of Duties, Assigned vs. Actual Rights Violation, and Terminated User reports. This report lists all exceptions for the current day.

9.6.1 To Generate Identity Audit Reports

1. Log in to Oracle Identity Analytics.
2. Choose **Reports** > **Ad Hoc Reports**.
3. Click **Identity Audit Reports**.
4. Select the report name and click **Run**.

   The report is displayed.
5. Click the **Actions** drop-down menu for options to export the file in other formats. Formats include PDF, XLS, CSV, HTML, XML, and print.
6. (Optional) To download the report, click **Download** in either the **Download PDF Report** column or the **Download CSV Report** column.

9.7 Defining Custom Reports

You can create and run custom reports in Oracle Identity Analytics. To create a custom report, see "Working With Custom Reports" in the *Administrator's Guide for Oracle Identity Analytics*.

9.7.1 To Run Custom Reports

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. Click the **Actions** drop-down menu for options to export the file in other formats. Formats include PDF, XLS, CSV, HTML, XML, and print.
6. (Optional) To download the report, click **Download** in either the **Download PDF Report** column or the **Download CSV Report** column.