Oracle

Securing Incentive Compensation
Sales Cloud

Release 12
# Contents

## Preface

### 1 About This Guide

- Audience and Scope
- Related Guides

### 2 Introduction to Oracle Sales Cloud Security

- Securing Oracle Incentive Compensation: Overview
- Authentication and Identity Management: Explained
- Single Sign-On Authentication: Explained

### 3 Authorization with Role-Based Access Control

- Role-Based Access Control in Incentive Compensation: Explained
- Incentive Compensation Role Types: Explained
- Security Policies: Explained
- Role Inheritance for Incentive Compensation: Explained
- Predefined Incentive Compensation Roles: Explained
- Incentive Compensation Work Area Duties: Explained
- Reviewing Predefined Roles for Incentive Compensation: Explained
- Customizing Security: Points to Consider
- Oracle Fusion Applications Security Console: Explained

### 4 Data Sharing Mechanisms and Visibility

- Data Sharing and Visibility in Incentive Compensation

### 5 About Incentive Compensation Users

- About Creating Users for Incentive Compensation
- Creating Setup Users for Oracle Incentive Compensation: Worked Example
## 6 Getting Ready to Create Application Users

- Creating Rules to Automatically Provision Job Roles to Incentive Compensation Users
- Role Provisioning and Deprovisioning: Explained
- Assigning Security Profiles to Abstract Roles: Worked Example
- FAQs for Preparing for Application Users

## 7 Creating Application Users

- User Setup Options: Critical Choices
- Setting the Default User Name Format: Procedure
- Managing Data Access for Users: Explained
- Creating Application Users for Oracle Incentive Compensation Cloud
- Assigning Data Access to Users: Worked Example

## 8 Managing Application Users

- Resetting User Passwords
- Inactive Users Report

## 9 Using the Security Console

- Security Console Visualizations: Explained
- Simulating Navigator Menus in the Security Console: Procedure
- Security Console Analytics: Explained

## 10 Reviewing Roles and Role Assignments

- Reviewing Role Assignments: Procedure
- Reviewing Role Hierarchies: Explained
- Comparing Roles: Procedure
- Reviewing Roles and Role Assignments in Identity Manager: Procedure
- Viewing the Duties of a Predefined Job Role in Authorization Policy Manager: Procedure
- User and Role Access Audit Report

## 11 Certificate Management

- Managing Certificates: Explained
- Generating Certificates: Explained
- Generating a Signing Request: Procedure
- Importing and Exporting X.509 Certificates: Procedure
- Importing and Exporting PGP Certificates: Procedure
- Deleting Certificates: Procedure
12 **Customizing Security**  
- Security Customization: Overview  
- Customizing Security: Points to Consider  
- Creating Job or Abstract Roles from Scratch: Procedure  
- Copying and Editing Duty Roles: Procedure  
- Role Optimization Report  
- Managing Database Resources: Procedure  

13 **Synchronizing with Oracle Identity Management**  
- Synchronizing User and Role Information: Procedure  
- Scheduling the Send Pending LDAP Requests Process: Procedure  
- Send Pending LDAP Requests: Explained  

14 **Security and Reporting**  
- Security for Incentive Compensation Analytics and Reports: Overview  
- Displaying Direct Report Data in Participant Manager Reports: Procedure  
- Business Intelligence Roles Used by Incentive Compensation: Explained  
- Customizing Security for Oracle Transactional Business Intelligence: Explained  
- Viewing Reporting Security Roles: Procedure  
- How can I customize Oracle Transactional Business Intelligence duty roles?  

15 **Advanced Data Security**  
- Advanced Data Security: Explained
Preface

This preface introduces information sources that can help you use the application.

Oracle Applications Help

Use the help icon to access Oracle Applications Help in the application. If you don’t see any help icons on your page, click the Show Help icon in the global header. Not all pages have help icons. You can also access Oracle Applications Help at https://fusionhelp.oracle.com.

Using Applications Help

Watch: This video tutorial shows you how to find help and use help features.

Additional Resources

- **Community**: Use Oracle Applications Customer Connect to get information from experts at Oracle, the partner community, and other users.
- **Guides and Videos**: Go to the Oracle Help Center to find guides and videos.
- **Training**: Take courses on Oracle Cloud from Oracle University.

Documentation Accessibility

For information about Oracle's commitment to accessibility, see the Oracle Accessibility Program.

Comments and Suggestions

Please give us feedback about Oracle Applications Help and guides! You can send e-mail to: oracle_fusion_applications_help_ww_grp@oracle.com.
1 About This Guide

Audience and Scope

This guide provides information on how implementors and administrators can set up users, roles, and security privileges. It describes role-based access controls provided for Oracle Incentive Compensation, and the tasks required to implement these controls so that users have appropriate access to data and functions. It does not cover your initial sign in or implementation tasks other than security.

Related Guides

You can refer to the following related guides to understand more about the business flows and functionality covered in this guide.

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Sales Cloud Getting Started with Incentive Compensation</td>
<td>Describes how to get started with Oracle Incentive Compensation implementations.</td>
</tr>
<tr>
<td>Oracle Sales Cloud Implementing Incentive Compensation</td>
<td>Describes tasks to configure and set up Oracle Incentive Compensation.</td>
</tr>
<tr>
<td>Oracle Sales Cloud Using Incentive Compensation</td>
<td>Describes the user tasks for the incentive compensation business process, from creating and managing compensation plans to reviewing and monitoring incentive plans and performance data.</td>
</tr>
</tbody>
</table>

Related Topics

- Oracle Help Center
2 Introduction to Oracle Sales Cloud Security

Securing Oracle Incentive Compensation: Overview

Incentive Compensation is secure as delivered. This guide describes how to enable user access to Incentive Compensation functions and data. Some of the tasks described in this guide are performed only or mainly during implementation. Most, however, can be performed at any time and as new requirements emerge. This topic summarizes the scope of this guide and identifies the contents of each chapter.

Guide Structure

This table describes the contents of each chapter in the guide.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and Identity Management</td>
<td>Introduces authentication and identity management in Incentive Compensation applications.</td>
</tr>
<tr>
<td>Authorization with Role-Based Access Control</td>
<td>A brief overview of how role-based access control (RBAC) is implemented in Incentive Compensation.</td>
</tr>
<tr>
<td>Data Sharing Mechanisms and Visibility</td>
<td>How users gain visibility to object data.</td>
</tr>
<tr>
<td>About Incentive Compensation Users</td>
<td>How to create and manage Incentive Compensation setup users and application users, and how to provision users with roles to provide them with access to Incentive Compensation functions and data.</td>
</tr>
<tr>
<td>Getting Ready to Create Application Users</td>
<td>Introduces the tools used to manage the roles, privileges, and policies of the RBAC model.</td>
</tr>
<tr>
<td></td>
<td>How to set up, manage, and use the Security Console.</td>
</tr>
<tr>
<td>Reviewing Roles and Role Assignments</td>
<td>How to review roles and identify the users who have them on the Security Console.</td>
</tr>
<tr>
<td>Customizing Security</td>
<td>How to configure Incentive Compensation security policies, how to copy predefined roles to create roles, and how to create roles from scratch.</td>
</tr>
<tr>
<td>Synchronizing with Oracle Identity Management</td>
<td>The role of the LDAP daily processes and how to schedule them.</td>
</tr>
</tbody>
</table>
Chapter 2

Introduction to Oracle Sales Cloud Security

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and Reporting</td>
<td>How to enable users to run Oracle Transactional Business Intelligence and Business Intelligence Publisher reports.</td>
</tr>
<tr>
<td>Implementing Federated Single Sign-In</td>
<td>How to implement federated Single Sign-In.</td>
</tr>
<tr>
<td>Advanced Data Security</td>
<td>An introduction to these optional cloud services:</td>
</tr>
<tr>
<td></td>
<td>• Database Vault</td>
</tr>
<tr>
<td></td>
<td>• Transparent Data Encryption</td>
</tr>
</tbody>
</table>

During implementation, you can perform security-related tasks:

- From a functional area task list
- By selecting Setup and Maintenance on the home page and searching for the task on the All Tasks tab of the Setup and Maintenance work area

Once the implementation is complete, you can perform most security-related tasks from the Setup and Maintenance work area or the Security Console.

Authentication and Identity Management: Explained

This topic describes the authentication and identity management services provided by Oracle for Cloud Applications.

Standard Authentication for Cloud Applications

Authentication, the process of verifying that a user is who they claim to be, is applied to all users, automated agents, or Web services that access an Oracle Cloud application. User credentials are checked at login and access is then granted or denied. In the standard method of authentication provided for Oracle Cloud environments, authentication providers validate user and application access based on a user name-password combination. Authentication providers also make user identity information available to other Cloud components when needed.

Identity Store

The Oracle Cloud authentication providers access the LDAP identity store, which is a logical repository of enterprise user identity data. Your LDAP directory stores definitions of LDAP user accounts.

In general, changes you make to user accounts are automatically synchronized between Oracle Sales Cloud and your LDAP directory server. However, you must also run processes on a daily basis to manage information exchange between your application and your LDAP directory server. For information, see the chapter about setting up application security.

Single Sign-On Authentication: Explained

Single Sign-On authentication, which enables users to sign in once but access multiple applications, is optionally available for Oracle Sales Cloud user authentication.
If your enterprise has moved from a traditional on-premises environment to an Oracle Cloud implementation, you might want to use your existing identity management solution for authenticating your employees in Oracle Sales Cloud, and might also want to provide a Single Sign-On experience. Implementing federated Single Sign-On allows you to provide users with Single Sign-On access to applications and systems located across organizational boundaries. For additional information, see Oracle Applications Cloud Service Entitlements (2004494.1) on My Oracle Support at https://support.oracle.com.

**Note:** Single Sign-On authentication is available on all platforms used to access the Sales Cloud application, including Oracle Mobile platforms, and is also available for Web services.
Introduction to Oracle Sales Cloud Security
3 Authorization with Role-Based Access Control

Role-Based Access Control in Incentive Compensation: Explained

When you receive your Incentive Compensation application, access to its functionality and data is secured using the industry-standard framework for authorization, role-based access control (RBAC). You must implement the RBAC controls provided so that users have appropriate access to Incentive Compensation data and functions.

In a RBAC model, users are assigned roles, and roles are assigned access privileges to protected system resources. The relationship between users, roles, and privileges is shown in the following figure.

Users gain access to application data and functions when you assign them roles, which correspond to the job functions in your organization.

Users can have any number of different roles concurrently, and this combination of roles determines the user’s level of access to protected system resources. For example, a user might be assigned the Incentive Compensation Manager role and the Employee role. In this case, the user has the following access:

- As an employee, the user can access employee functions and data.
- As an Incentive compensation manager, the user can access compensation functions and data.

When the user signs in to Incentive Compensation and is successfully authenticated, a user session is established and all the roles assigned to the user are loaded into the session repository. Incentive Compensation determines the set of privileges to system resources that are provided by the roles, then grants the user the most permissive level of access.

You can assign roles to a user manually, when you create the user, or automatically, by creating role provisioning rules.

Incentive Compensation Role Types: Explained

This topic describes the roles provided by Incentive Compensation and explains how they work together to provide users with permissions to application resources. Incentive Compensation provides the following types of roles:

- Job roles
• Abstract roles
• Duty roles

The permissions each role provides are described in security reference manuals available on http://docs.oracle.com.

Job Roles

Job roles represent the job functions in your organization. Incentive Compensation Manager and Incentive Compensation Plan Administrator are examples of predefined job roles. You can also create custom job roles.

Job roles provide users with the permissions they need to perform activities specific to their jobs. For example, providing a user with the Incentive Compensation Manager job role permits the user to manage incentive compensation participant information and assignments, manage credits and earnings, and manage incentive payment processing. You can assign job roles directly to users.

Abstract Roles

Abstract roles represent a worker's functions in the enterprise independently of the job they do. The following are examples of abstract roles used in Oracle:

• Employee
• Participant
• Participant Manager

Abstract roles permit users to perform functions that span across the different jobs in the enterprise. For example, users who are employees must be provisioned with the Employee abstract role, so they can update their employee profiles and pictures. For Incentive Compensation, you must also provision users to assign the Incentive Compensation Participant or Incentive Compensation Participant Manager abstract roles, so they can access the Sales Compensation work area and related reports. You can assign abstract roles directly to users. You can also create custom abstract roles.

Duty Roles

Duty roles permit users to carry out actions by virtue of the duty roles they include. Each predefined duty role consists of a logical grouping of privileges that represents the individual duties that users perform as part of their job. Duty roles are composed of security policies which grant access to work areas, dashboards, task flows, application pages, reports, batch programs, and so on.

Job roles and abstract roles inherit duty roles. For example, the Incentive Compensation Analyst job role inherits the Incentive Compensation Participant Assignments Duty, Incentive Compensation Credits and Earnings Duty, Incentive Compensation Participant Snapshot Management Duty, and the Incentive Compensation Payments Duty. The Compensation Participant Assignments Duty makes it possible for the analyst to assign plans, roles, pay groups, and payment plans to the participant. The Incentive Compensation Payments Duty enables payment batch assembly and paysheet management.

Duty roles can also inherit other duty roles. They're part of the security reference implementation, and are the building blocks of custom job and abstract roles. You can also create custom duty roles. You can’t assign duty roles directly to users.
Security Policies: Explained

Duty roles are associated with two types of security policies: functional security policies and data security policies. Security policies define the privileges provided by the duty role to access specific application resources. This topic describes both types of security policy.

Functional Policies

Functional policies permit an individual who is assigned a duty role to access different user interface elements, Web services, tasks flows, and other functions. For example, an incentive compensation analyst who has the Delete Incentive Compensation Paysheet functional policy can view and click the Delete button. Removing that policy removes the button from view. A functional policy is made up of the following:

- A duty role name. The name of the duty where the policy applies, for example, Incentive Compensation Payments Duty.
- A functional privilege that specifies the application features that are being secured, for example, Delete Incentive Compensation Paysheet.

In the security reference manuals, functional privileges are listed in the Privileges section.

Data Security Policies

Data security policies specify the duty roles that can perform a specified action on an object, and the conditions under which the action can be carried out. A data security policy is composed of:

- A duty role name. The name of the duty where the policy applies. For example, Incentive Compensation Credits and Earnings Duty.
- A data privilege that defines the action being performed. For example, Maintain Incentive Compensation Transaction Data.
- The condition that must be met for access to be granted. For example, users assigned a job which includes the Incentive Compensation Credits and Earnings Duty can maintain incentive compensation transactions for the business units for which they are authorized.

If the View All condition is specified, the duty role provides access to all data of the relevant type.

Each data security policy represents an underlying SQL query. The application evaluates the query at run time, and permits access to data that meets the condition. Data privileges are listed in the Data Security Policies section of the security reference manuals.

Policy Store

The policy store is the repository of all roles for Oracle Cloud Applications. The policy store is also where the security policies defined for each duty role are stored. The Security Console is a tool for managing the policy store for Oracle Cloud Applications.
Role Inheritance for Incentive Compensation: Explained

This topic describes how users inherit roles and privileges and introduces the Oracle role hierarchy.

In Incentive Compensation, each role can be linked to other roles in a parent-child format to form a hierarchy of roles. As illustrated in the following figure, users are assigned job and abstract roles, which inherit application roles of the same name. The top-level application roles in turn inherit duty roles and their associated privileges.

Role hierarchies allow privileges to be grouped to represent a feature set in Incentive Compensation, which simplifies feature management. Role hierarchies also provide privilege granularity and facilitate role reuse. For example, each role hierarchy beneath the Application Job Role represents a feature that is available through the job role to the user. Roles at lower levels of the hierarchy represent functionality that the feature requires. If this functionality is required by other features, the role that provides the functionality can be shared across roles.

>Note: Having many levels in a role hierarchy is not recommended. Deep role hierarchies are difficult to manage, and modification of the privileges in roles that are heavily reused can cause undesired behavior in other features.
Role Inheritance Rules
In Incentive Compensation, roles can be inherited according to the following rules.

- External roles (job and abstract roles) can inherit privileges from subordinate external roles.
- External roles can inherit privileges from subordinate application roles.
- Application roles can inherit privileges from subordinate application roles.
- Application roles cannot inherit privileges from external roles.

Circular references between roles are not allowed.

Role Inheritance Example
This example shows how roles and privileges are inherited for a user, Tom Green, assigned the Incentive Compensation Plan Administrator job role.

The following figure shows a few representative duty roles.
In this example, an employee is provisioned with the enterprise roles needed to do the job: the Incentive Compensation Plan Administrator job role, and the Employee abstract roles. Roles are inherited as follows:

- The Incentive Compensation Plan Administrator job role inherits Incentive Compensation Plan Administrator application role.
- The Incentive Compensation Plan Administrator application role inherits duties. These include the Incentive Compensation Credit and Earnings Duty and the Incentive Compensation Participant Assignments Duty.
- Both the application role and the duty roles are associated with functional security policies and data security policies.

Functional security policies specify which application pages and functions plan administrators can access. For example, the Incentive Compensation Plan Administrator application role has functional security policies for modeling incentive plans, such as creating and managing the plan, rate tables, and expressions. The inherited Incentive Compensation Participant Assignments Duty has functional security policies related to assigning the plan to participants. This includes creating and managing the plan terms and conditions, creating assignment roles, and assigning the roles to the plan.

Data security policies specify under what conditions the function can be performed. For example, the plan administrator can only assign roles to plans that are defined for the business units for which they have access to.

**Predefined Incentive Compensation Roles: Explained**

Many job and abstract roles are predefined. The following are the main predefined Incentive Compensation job roles:

- Incentive Compensation Manager
- Incentive Compensation Plan Administrator
- Incentive Compensation Analyst
- Incentive Compensation Application Administrator
- Incentive Compensation Integration Specialist

The following two abstract roles are predefined for users who will participate in achieving incentives:

- Incentive Compensation Participant
- Incentive Compensation Participant Manager

These predefined roles are part of the security reference implementation. The security reference implementation is a predefined set of security definitions that you can use as supplied.

You must also assign the Employee abstract role to all Oracle application users who are employees so they can carry out their work.

**Incentive Compensation Work Area Duties: Explained**

The security for incentive compensation aligns with the functional work areas and jobs. For example, one credit and earnings duty contains the privileges for the tasks included in the credit and earnings work area.

Following are the available security items and related work areas.
Following are the available security assignments to roles.

<table>
<thead>
<tr>
<th>Security</th>
<th>Work Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incentive Compensation Plan Administrator</td>
<td>Plans</td>
</tr>
<tr>
<td>Incentive Compensation Credits and Earnings Duty</td>
<td>Credit and Earnings</td>
</tr>
<tr>
<td>Incentive Compensation Participant Assignments Duty</td>
<td>Participant Assignments</td>
</tr>
<tr>
<td>Incentive Compensation Participant Snapshot Management Duty</td>
<td>Participant Snapshot</td>
</tr>
<tr>
<td>Incentive Compensation Payment Control Duty</td>
<td>Payments</td>
</tr>
<tr>
<td>Incentive Compensation Payments Duty</td>
<td>Payments</td>
</tr>
<tr>
<td>Incentive Compensation Participant</td>
<td>Sales Compensation</td>
</tr>
<tr>
<td>Incentive Compensation Participant Manager</td>
<td>Sales Compensation</td>
</tr>
<tr>
<td>Incentive Compensation Application Administrator</td>
<td>Setup and Maintenance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incentive Compensation Plan Administrator</td>
<td>Incentive Compensation Plan Administrator</td>
</tr>
</tbody>
</table>
| Incentive Compensation Credits and Earnings Duty | • Incentive Compensation Plan Administrator  
| | • Incentive Compensation Analyst  
| | • Incentive Compensation Manager |
| Incentive Compensation Participant Assignments Duty | • Incentive Compensation Plan Administrator  
| | • Incentive Compensation Analyst  
| | • Incentive Compensation Manager |
| Incentive Compensation Participant Snapshot Management Duty | • Incentive Compensation Analyst  
| | • Incentive Compensation Manager |
| Incentive Compensation Payment Control Duty | Incentive Compensation Manager |
| Incentive Compensation Payments Duty | • Incentive Compensation Analyst  
| | • Incentive Compensation Manager |
Reviewing Predefined Roles for Incentive Compensation: Explained

This topic describes the ways in which you can access information about predefined roles. This information can help you to identify which users need each role and whether to make any changes before provisioning roles.

The Security Console

On the Security Console, you can:

- Review the role hierarchy of any job, abstract, or duty role.
- Identify the function security privileges and data security policies granted to a role.
- Compare roles to identify differences.

Reports

You can run the User and Role Access Audit Report to produce an XML-format report of the function security privileges and data security policies for a specified role or all roles.

The Security Reference Manuals

Two manuals describe the security reference implementation for Oracle Sales Cloud users:

- The Security Reference for Oracle Applications Cloud includes descriptions of all predefined security data that’s common to Oracle Fusion Applications.
- The Security Reference for Oracle Incentive Compensation includes descriptions of all predefined security data for Incentive Compensation.

Both manuals contain a section for each predefined job and abstract role. For each role, you can review its:

- Duty roles
- Role hierarchy
- Function security privileges
- Data security policies
You can access the security reference manuals on cloud.oracle.com. From the menu select Resources - Discover - Documentation - Applications. Select Sales Cloud, then Books.

Customizing Security: Points to Consider

If the predefined security reference implementation doesn’t fully represent your enterprise, then you can make changes.

For example, the predefined Incentive Compensation Analyst job role includes payment duties. If some business groups in your organization have the incentive compensation manager do all payment processing, then you can create a custom Analyst role without those duties. Alternatively, if a predefined job role is too narrowly defined, then you can create a job role with a greater range of duties than its predefined equivalent.

During implementation, you evaluate the predefined roles and decide whether changes are needed. The Functional Setups User abstract role is required for any custom role intended to perform implementation tasks.

⚠️ Caution: Never edit the predefined roles. (You can identify predefined application roles by the ORA prefix in the role code.)

During each upgrade, predefined roles are updated to the specifications for that release, so any customizations would be overwritten. Instead, use one of these options:

- Copy the predefined roles and edit the copies in the Security Console.
- Create custom roles from scratch in the Security Console.

All predefined roles are granted many function security privileges and data security policies. They also inherit duty roles. To make minor changes to a role, copying the predefined role and editing the copy is the more efficient approach. Creating roles from scratch is most successful when the role has very few privileges and you can identify them easily.

Missing Enterprise Jobs

If jobs exist in your enterprise that aren’t represented in the security reference implementation, then you create custom job roles. Add duty roles to custom job roles, as appropriate.

Predefined Roles with Different Privileges

If the privileges for a predefined job role don’t match the corresponding job in your enterprise, then you create a custom version of the role. If you copy the predefined role, then you can edit the copy to add or remove duty roles, function security privileges, and data security policies, as appropriate.

Predefined Roles with Missing Privileges

If the privileges for a job aren’t defined in the security reference implementation, then you create custom duty roles.

Oracle Fusion Applications Security Console: Explained

The Security Console is an easy-to-use administrative work area where you perform most security-management tasks. This topic introduces the Security Console and describes how to access it.
Security Console Functions

Use the Security Console to:

- Review role hierarchies and role analytics.
- Create and manage custom job, abstract, and duty roles.
- Review the roles assigned to users.
- Perform user management tasks, including resetting user passwords and updating user e-mail addresses.

**Note:** You use the Manage Users work area, not the Security Console, to create users and to provision users with roles.

- Compare roles.
- Simulate the Navigator for a user or role.
- Manage the default format of user names and the enterprise password policy.
- Manage notifications for user-lifecycle events, such as password expiration.
- Manage PGP and X.509 certificates for data encryption and decryption.

**Note:** Oracle Sales Cloud does not use certificate functionality.

- Set up federation, and synchronize user and role information between Oracle Applications Security and Microsoft Active Directory, if appropriate.

Accessing the Security Console

You must have the IT Security Manager job role to access the Security Console. You open the Security Console by selecting **Tools - Security Console** from the home page or Navigator. These tasks, performed in the Setup and Maintenance work area, also open the Security Console:

- Manage Job Roles
- Manage Duties
- Manage Data Security Policies
4 Data Sharing Mechanisms and Visibility

Data Sharing and Visibility in Incentive Compensation

The conditions specified in data security policies control visibility to record-level data associated with a schema object, such as an incentive compensation plan and a paysheet.

Conditions can use the following components as mechanisms for sharing data, provided that the sharing mechanism is applicable for the object:

- Business unit
- Analyst assignment
- Person security profile

Business Unit

For incentive compensation administrators, the basis for data sharing is the business unit they have access to. Incentive compensation administrators are users assigned to the following job roles:

- Incentive Compensation Administrator
- Incentive Compensation Manager
- Incentive Compensation Plan Administrator
- Incentive Compensation Analyst

Analyst Assignment

You have the option to further limit data access for users assigned to the Incentive Compensation Analyst role. The Setup and Maintenance, Manage Parameters task allows you to limit the analyst access to the business unit or to participants who are directly assigned to the analyst.

For example, analyst Amy is directly assigned to the participants Jack and Ravi. Analyst Ryan is assigned to the participants Juan and Mary. When the Manage Parameter setting indicates analyst security is by participant, Amy cannot manage participant data for Juan and Mary because she is not the assigned analyst. This functionality applies to data within the Participant Snapshot and Payments work areas.

You can assign analysts to participants when the participants are imported, using the Participant Assignments, Manage Analyst Assignments task, and using the Participant Snapshot, Participant Details task.

Person Security Profile

The predefined person security profile types can be assigned to abstract roles, such as the employee, line manager, and contingent worker roles. You can also assign the security profile to the Incentive Compensation Participant and Incentive Compensation Participant Manager abstract roles. The person security profile, view own record option provides visibility to the participant’s own data. The person security profile, view manager hierarchy option provides the participant manager with visibility to participant data for the subordinates in their management hierarchy.
5 About Incentive Compensation Users

About Creating Users for Incentive Compensation

This topic provides information about creating users in Incentive Compensation. Review this information before you create setup and application users.

User Types

When you sign up with Incentive Compensation, you receive the user name and password for one initial user. The initial user is provisioned with the privileges necessary to perform many implementation tasks, including creating other users. The following are the different types of users that you can create when you sign in to the application as the initial user.

• Setup users

You can provision setup users with the same job roles as the initial user so that they can perform all the standard implementation setup tasks for your Incentive Compensation implementation. Setup tasks include managing security, enterprise setup, and creating other users, including other users with the same privileges. The roles assigned to the initial user are:

  o Application Implementation Consultant job role
  o IT Security Manager job role
  o Application Diagnostic Administrator job role

• Incentive compensation application administrators

Incentive compensation administrators are provisioned with the Incentive Compensation Application Administrator job role, which includes permission to manage incentive compensation parameters, calendars, and custom qualifiers.

Incentive compensation administrators cannot configure security roles or perform tasks related to enterprise setup.

To create incentive compensation administrators, follow the same procedure outlined in the topic Creating Application Users for Incentive Compensation: Worked Example.

• Application users

Application users are provisioned with job and abstract roles according to the resource role they are assigned. The provisioned job roles do not permit application users to perform implementation tasks, but they can perform a functional setup within the application, depending on their role.

Application users can be provisioned with the following roles:

  o The job roles that they require to perform their job
  o The participant or participant manager abstract role
  o The Employee or the Contingent Worker abstract role, depending on the employee type of the user
Methods of Creating Users

You can create users in either of the following ways. You can:

- Create users individually in the Manage Users work area. You can navigate to this work area using the Navigator menu from any application page.

  Use this method to create all setup users, and to create application users unless you are creating a large number of users.

- Import users from a file using the File-Based Data Import group of tasks from the Setup and Maintenance work area.

  Import users from a file only if you have a large number of users to create. To import users, you must understand how user attributes are represented in Incentive Compensation and how to map the attributes in your file to the attributes required by the application. You cannot import setup users because the import process requires you to import sales resources.

  See Understanding File-Based Data Import: Getting Started and other help topics on file import.

Tasks You Accomplish by Creating Users

When you create users, you also accomplish the tasks listed in the following table. Not all the tasks apply to setup users because they are not created as resources in the application.

<table>
<thead>
<tr>
<th>Task Accomplished</th>
<th>Application Users</th>
<th>Setup User</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send automatic e-mail notifications containing the user names you entered and automatically generated temporary passwords.</td>
<td>Yes</td>
<td>Yes</td>
<td>The application sends the notifications to the user or to an administrator only once, either on creation or later, depending on the setup.</td>
</tr>
<tr>
<td>Automatically provision the job and abstract roles that provide the security settings users require to do their jobs.</td>
<td>Yes</td>
<td>Yes</td>
<td>Job and abstract roles are provisioned based on the autoprovisioning rules discussed in related security topics.</td>
</tr>
<tr>
<td>Create rudimentary employee records that can be used by Oracle HCM Cloud if you have implemented it, or if you implement it in the future.</td>
<td>Yes</td>
<td>Yes</td>
<td>You must specify each user as either an employee or as a contingent worker.</td>
</tr>
</tbody>
</table>

Creating Basic Oracle HCM Cloud Employee Records

When you create application users, you must specify information that is used to create basic employee records for the Oracle HCM Cloud application.
You must specify the following information for the employee record:

- Person Type
- Legal Employer
- Business Unit
- Manager (Required for Participant Managers)

For information about these employee-related values, see the topic Creating Application Users for Incentive Compensation: Worked Example.

Creating Setup Users for Oracle Incentive Compensation: Worked Example

This topic describes how to create setup users. The initial user you receive when you activate Oracle Incentive Compensation can perform all of the application setup tasks. As a best practice, Oracle recommends that you create additional setup users with the type of broad setup privileges Oracle provides to the initial user you received.

To create the setup user in this example you do the following:

1. Create a job called Setup Administrator.
   
   You create this job for creating setup users only.

2. Create a provisioning rule that automatically provisions the following security job roles to all users with the Setup Administrator job.

<table>
<thead>
<tr>
<th>Job Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Diagnostics Administrator</td>
<td>Provides access to diagnostic tests and data.</td>
</tr>
<tr>
<td>Application Implementation Consultant</td>
<td>Provides access to all setup tasks across all products.</td>
</tr>
<tr>
<td>IT Security Manager</td>
<td>Provides access to security tasks, including the ability to assign other enterprise roles.</td>
</tr>
</tbody>
</table>

3. Create each setup user as a user of type employee with the Setup Administrator job.

Creating the Job for Provisioning Setup Users

Use this procedure to create a job that you can use to assign setup users with the same implementation privileges as the initial user. You use this job as a condition in the provisioning rule you create to assign users with roles.

1. Sign in as the initial user.
2. Navigate to the Setup and Maintenance work area.
3. Search for and open the Manage Job task.
   
   The Manage Jobs page appears.

4. Click Create.
The Create Job: Basic Details page appears.

5. Enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Setup Administrator</td>
</tr>
<tr>
<td>Code</td>
<td>SetupAdministrator. (No spaces)</td>
</tr>
</tbody>
</table>

6. Click **Next** at the top of the page.
7. Click **Submit** on the next page, and click **OK** when the warning is displayed.

The job might take a couple of minutes to create. You can use search on the Manage Job page to verify that it has been created.

Creating the Provisioning Rule for Setup Users

Use this procedure to create a provisioning rule that automatically provisions users assigned the Setup Administrator job with the job roles required to perform the initial setup of Incentive Compensation.

1. Navigate to the Setup and Maintenance work area.
2. Search for and open the Manage HCM Role Provisioning Rules task.

   The Manage Role Mappings page appears.

3. Click **Create**.

   The Create Role Mapping page appears.

4. In the **Mapping Name** field, enter a name, for example, **Setup User**.
5. In the Conditions region, select **Setup Administrator**, the job you created earlier, from the **Job** list. If the job does not appear in the list, click Search and search for it using the full name.
6. Select **Active** from the **HR Assignment Status** list.

   This additional condition ensures that the provisioned roles are automatically removed if the user is terminated.
7. In the Associated Roles region, click **Add** to add the following job roles:
   - Application Implementation Consultant
   - IT Security Manager
   - Application Diagnostics Administrator
   - Sales Analyst (required for Sales Predictor)
8. Make sure the **Autoprovision** option is selected for each of the job roles.
9. Click **Save and Close**.

Creating the Setup User

Use the following steps to create other setup users.

1. In the Navigator, select the **Manage Users** link under the **My Team** heading.
The Manage Users page appears.

2. Click **Create**.

The Create User page appears.

3. Enter the user’s name and a unique e-mail in the Personal Details region.

   The application automatically sends the initial sign-in credentials to this e-mail when you save the record.

   You can leave the **Hire Date** as is.

4. In the User Details region, enter the user name. If you leave the **User Name** field blank, then the application creates a user name based on the entries you have already made.

5. In the User Notification region, select the **Send User Name and Password** option so setup users receive initial e-mail notifications with their login and password details when you save the record.

6. In the **Employment Information** region, enter the information shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person Type</td>
<td>Select <strong>Employee</strong>.</td>
</tr>
<tr>
<td>Legal Employer</td>
<td>Select the legal employer Oracle created for you using the information you provided when you signed up with Oracle Incentive Compensation.</td>
</tr>
<tr>
<td>Business Unit</td>
<td>Select the business unit created for you using the information you provided when you signed up with Oracle Incentive Compensation.</td>
</tr>
<tr>
<td>Job</td>
<td>Select <strong>Setup Administrator</strong>, the job you just created.</td>
</tr>
</tbody>
</table>

7. Click **Autoprovision Roles**.

   The Roles region displays the roles for the Setup Administrator job:

   - Application Implementation Consultant
   - IT Security Manager
   - Application Diagnostics Administrator

8. Click **Save and Close**.

   An e-mail is sent to the new setup user containing the initial credentials for signing in the application.
6 Getting Ready to Create Application Users

Creating Rules to Automatically Provision Job Roles to Incentive Compensation Users

Before you create Incentive Compensation Cloud application users, you must create the rules to automatically provision them with the job roles they require. The rules use the values that you select when importing employee resources or when manually entering users as the trigger condition. You must create a separate rule to provision each incentive compensation security job role.

Creating a Provisioning Rule

1. Sign in as a setup user.
2. Navigate to the Setup and Maintenance work area.
3. Search for and open the Manage HCM Role Provisioning Rules task.

   The Manage Role Mappings page appears.
4. Click Create.

   The Create Role Mapping page appears.
5. In the Mapping Name field, enter a name that will help you identify the mapping, for example, Incentive Compensation Analyst.
6. In the Conditions region, select the job or resource role which best identifies the employees that you want to provision. For example, select the job Incentive Compensation Analyst to create a provisioning rule for the analyst.
7. Select Active from the HR Assignment Status list.

   This additional condition ensures that the provisioned roles are automatically removed if the user is terminated in Global Human Resources.
8. In the Associated Roles region, click Add to add the job roles you want to provision. For example, select the job Incentive Compensation Analyst to create a provisioning rule for the analyst.
9. Make sure the Autoprovision option is selected for all the roles.
10. Click Save and Close.

Role Provisioning and Deprovisioning: Explained

You must provision roles to users. Otherwise, they have no access to data or functions and can’t perform application tasks. This topic explains how role mappings control role provisioning and deprovisioning. Use the Manage Role Provisioning Rules or Manage HCM Role Provisioning Rules task to create role mappings.
Role Provisioning Methods

You can provision roles to users:

- Automatically
- Manually
  - Users such as line managers can provision roles manually to other users.
  - Users can request roles for themselves.

For both automatic and manual role provisioning, you create a role mapping to specify when a user becomes eligible for a role.

Role Types

You can provision data roles, abstract roles, and job roles to users. However, for Oracle HCM Cloud users, you typically include job roles in HCM data roles and provision those data roles.

Automatic Role Provisioning

Users acquire a role automatically when at least one of their assignments satisfies the conditions in the relevant role mapping. Provisioning occurs when you create or update worker assignments. For example, when you promote a worker to a management position, the worker acquires the line manager role automatically if an appropriate role mapping exists. All changes to assignments cause review and update of a worker’s automatically provisioned roles.

Role Deprovisioning

Users lose automatically provisioned roles when they no longer satisfy the role-mapping conditions. For example, a line manager loses an automatically provisioned line manager role when he or she stops being a line manager. You can also manually deprovision automatically provisioned roles at any time.

Users lose manually provisioned roles automatically only when all of their work relationships are terminated. Otherwise, users keep manually provisioned roles until you deprovision them manually.

Roles at Termination

When you terminate a work relationship, the user automatically loses all automatically provisioned roles for which he or she no longer qualifies. The user loses manually provisioned roles only if he or she has no other work relationships. Otherwise, the user keeps manually provisioned roles until you remove them manually.

The user who’s terminating a work relationship specifies when the user loses roles. Deprovisioning can occur:

- On the termination date
- On the day after the termination date

If you enter a future termination date, then role deprovisioning doesn’t occur until that date or the day after. The Role Requests in the Last 30 Days section on the Manage User Account page is updated only when the deprovisioning request is created. Entries remain in that section until they’re processed.

Role mappings can provision roles to users automatically at termination. For example, a terminated worker could acquire the custom role Retiree at termination based on assignment status and person type values.
Reversal of Termination
Reversing a termination removes any roles that the user acquired automatically at termination. It also provisions roles to the user as follows:

- Any manually provisioned roles that were lost automatically at termination are reinstated.
- As the autoprovisioning process runs automatically when a termination is reversed, roles are provisioned automatically as specified by current role-provisioning rules.

You must reinstate manually any roles that you removed manually, if appropriate.

Date-Effective Changes to Assignments
Automatic role provisioning and deprovisioning are based on current data. For a future-dated transaction, such as a future promotion, role provisioning occurs on the day the changes take effect. The Send Pending LDAP Requests process identifies future-dated transactions and manages role provisioning and deprovisioning at the appropriate time. These role-provisioning changes take effect on the system date. Therefore, a delay of up to 24 hours may occur before users in other time zones acquire their roles.

Assigning Security Profiles to Abstract Roles: Worked Example
To enable basic data access for the predefined Employee, Contingent Worker, and Line Manager abstract roles, you assign predefined security profiles to them during implementation. This example shows how to assign security profiles to abstract roles using the Assign Security Profiles to Role task.

Searching for the Employee Abstract Role
1. Sign in as the TechAdmin user. On-premises users must sign in with a role that has the IT Security Manager job role.
2. Select Navigator - Setup and Maintenance to open the Setup and Maintenance work area.
3. Search for and select the Assign Security Profiles to Role task.
4. On the Manage Data Roles and Security Profiles page, enter Employee in the Role field. Click Search.
5. In the Search Results section, select the predefined Employee role and click Edit.

Assigning Security Profiles to the Employee Abstract Role
1. On the Edit Data Role: Role Details page, click Next.
2. On the Edit Data Role: Security Criteria page, select the security profiles shown in the following table. You may see a subset of these security profiles, depending on the combination of cloud services that you’re implementing.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Security Profile</td>
<td>View All Organizations</td>
</tr>
</tbody>
</table>
### Field | Value
---|---
**Position Security Profile** | View All Positions
**Country Security Profile** | View All Countries
**LDG Security Profile** | View All Legislative Data Groups
**Person Security Profile (Person section)** | View Own Record
**Person Security Profile (Public Person section)** | View All Workers
**Document Type Security Profile** | View All Document Types

3. Click **Review**.
4. On the Edit Data Role: Review page, click **Submit**.
5. On the Manage Data Roles and Security Profiles page, search again for the predefined Employee role.
6. In the Search Results region, confirm that a green check mark appears in the **Security Profiles** column for the Employee role.

   The check mark confirms that security profiles are assigned to the role.

   Repeat the steps in Searching for the Employee Abstract Role and Assigning Security Profiles to the Employee Abstract Role for the predefined Contingent Worker role.

### Searching for the Line Manager Abstract Role

1. On the Manage Data Roles and Security Profiles page, enter Line Manager in the **Role** field. Click **Search**.
2. In the Search Results section, select the predefined Line Manager role and click **Edit**.

### Assigning Security Profiles to the Line Manager Abstract Role

1. On the Edit Data Role: Role Details page, click **Next**.
2. On the Edit Data Role: Security Criteria page, select the security profiles shown in the following table. You may see a subset of these security profiles, depending on the combination of cloud services that you're implementing.

   | Field | Value |
   ---|---|
   **Organization Security Profile** | View All Organizations
   **Position Security Profile** | View All Positions
   **Country Security Profile** | View All Countries
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LDG Security Profile</strong></td>
<td>View All Legislative Data Groups</td>
</tr>
<tr>
<td><strong>Person Security Profile (Person section)</strong></td>
<td>View Manager Hierarchy</td>
</tr>
<tr>
<td><strong>Person Security Profile (Public Person section)</strong></td>
<td>View All Workers</td>
</tr>
<tr>
<td><strong>Document Type Security Profile</strong></td>
<td>View All Document Types</td>
</tr>
<tr>
<td><strong>Payroll</strong></td>
<td>View All Payrolls</td>
</tr>
<tr>
<td><strong>Payroll Flow</strong></td>
<td>View All Flows</td>
</tr>
</tbody>
</table>

3. Click **Review**.
4. On the Edit Data Role: Review page, click **Submit**.
5. On the Manage Data Roles and Security Profiles page, search again for the predefined Line Manager role.
6. In the search results, confirm that a green check mark appears in the **Security Profiles** column for the Line Manager role.

The check mark confirms that security profiles are assigned to the role.

**FAQs for Preparing for Application Users**

**What happens when I autoprovion roles for a user?**

The role-provisioning process reviews the user’s assignments against all current role mappings. The following changes are made to the user’s roles:

- The user acquires any role for which he or she qualifies but doesn’t have
- The user loses any role for which he or she no longer qualifies

It’s recommended that you autoprovion roles to individual users on the Edit User page when new or changed role mappings exist. Otherwise, no automatic updating of roles occurs until you next update the user’s assignments.

**Why did some roles appear automatically?**

In a role mapping:

- The conditions specified for the role match the user’s assignment attributes, such as job.
- The role has the **Autoprovion** option selected.
7 Creating Application Users

User Setup Options: Critical Choices

This topic describes the enterprise options that are available for controlling default functionality when users are created in the application. You might have made decisions about user setup options when you configured your application security environment and set up the Security Console. If you did not, then it’s recommended that you configure these options before you start to create users.

To review user setup options, navigate to the Administration tab of the Security Console. For detailed information about configuring the options, see the chapter Setting Up Applications Security.

User Name and Password Notifications

By default, users automatically receive an e-mail notification containing their sign-in details when their user account is created. You can customize the text of the e-mail notification the user receives or suppress e-mail notifications altogether.

Password Policy

During implementation, you set the password policy for the enterprise. For example, you can configure how complex passwords must be, when they expire, and when a user is notified that a password is about to expire.

Default User Name Format

You can select the default format used to generate user names for application users in cases where a user name is not specified. Unless you specify otherwise, the default format is e-mail address.

Related Topics

- Setting Password Policy: Explained

Setting the Default User Name Format: Procedure

During implementation, you specify the default format of user names for the enterprise. The default format you select is used to automatically generate a user name for a user if you don’t explicitly specify the user name when you create the user. This topic describes how to specify the default format of user names and the formats that are available.

Specifying the Format of User Names

Perform the steps in the following procedure to select the default format for user names:

1. Navigate to the Setup and Maintenance work area.
2. On the Setup and Maintenance page, search for and select the task Manage Applications Security Preferences. The Administration tab of the Security Console opens with the General subtab selected. (You can also navigate directly to the Security Console at any time by selecting Navigator - Tools - Security Console.)
3. In the User Preferences section of this subtab, select a user-name format. Select one of the options shown in the following table.

<table>
<thead>
<tr>
<th>Format Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-Mail</td>
<td>The work e-mail (or party e-mail, for party users) is the user name. For example, the user name for <a href="mailto:john.smith@example.com">john.smith@example.com</a> is <a href="mailto:john.smith@example.com">john.smith@example.com</a>. To make duplicate names unique, a number is added. For example, <a href="mailto:john.smith2@example.com">john.smith2@example.com</a> may be used if <a href="mailto:john.smith@example.com">john.smith@example.com</a> and <a href="mailto:john.smith1@example.com">john.smith1@example.com</a> already exist. E-Mail is the default format.</td>
</tr>
<tr>
<td>FirstName.LastName</td>
<td>The user name is the user’s first and last names separated by a single period. For example, the user name for John Frank Smith is john.smith. To make duplicate names unique, either the user’s middle name or a random character is used. For example, John Smith’s user name could be john.frank.smith or john.x.smith.</td>
</tr>
<tr>
<td>FNameName</td>
<td>The user name is the user’s last name prefixed with the initial of the user’s first name. For example, the user name for John Smith is jsmith.</td>
</tr>
<tr>
<td>Person or party number</td>
<td>The person or party number generated by the application is the user name. For example, if John Smith’s party number is 100000000178803, then the user name is 100000000178803. User names generated from party or person numbers can be difficult to remember so it’s recommended that you don’t select this option.</td>
</tr>
</tbody>
</table>

4. Enable or disable the option Generate system user name when generation rule fails. This option controls whether a system user name is generated if the user name rule fails, for example, if the default user name format is FirstName.LastName but a first name isn’t available.
   - If the option is enabled, a system user name is generated by applying these options in the following order until a unique user name is defined:
     1. E-Mail
     2. FirstName.LastName
     3. If only the last name is available, then a random character is prefixed to the last name.
   - If the option is disabled, then an error is raised if the user name can’t be generated in the selected format.

5. Click Save. Any changes take effect immediately.

Editing User Names
When creating users on the Create User page, you can enter user names in any format to override the default user names. You can also edit user names for individual users on the Edit User page.

Managing Data Access for Users: Explained
You can assign users access to appropriate data based on their job roles. The Oracle Fusion security model requires a three-way link between users, role, and data. It is summarized as: who can do what on which data. Who refers to the users, what are the job roles the user is assigned, and which refers to the data that is specific to a particular security context, typically an element of the enterprise structure, such as a business unit, asset book, or ledger.
For example, consider a user, Mary Johnson, who manages accounts payable functions, such as creating invoices for the US Operations business unit. In this scenario, Mary Johnson must be assigned the job role of an Accounts Payable Specialist, and given access to the US Operations business unit.

The following table lists the elements of the enterprise structure to which users can be assigned access based on their job roles.

<table>
<thead>
<tr>
<th>Product</th>
<th>Security Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Fusion Financials</td>
<td>Business Unit</td>
</tr>
<tr>
<td></td>
<td>Data Access Set</td>
</tr>
<tr>
<td></td>
<td>Ledger</td>
</tr>
<tr>
<td></td>
<td>Asset Book</td>
</tr>
<tr>
<td></td>
<td>Control Budget</td>
</tr>
<tr>
<td></td>
<td>Intercompany Organization</td>
</tr>
<tr>
<td></td>
<td>Reference Data Set</td>
</tr>
<tr>
<td>Oracle Fusion Supply Chain</td>
<td>Inventory Organization</td>
</tr>
<tr>
<td>Management</td>
<td>Reference Data Set</td>
</tr>
<tr>
<td></td>
<td>Cost Organization</td>
</tr>
<tr>
<td></td>
<td>Inventory Organization</td>
</tr>
<tr>
<td></td>
<td>Manufacturing Plant</td>
</tr>
<tr>
<td>Oracle Fusion Procurement</td>
<td>Business Unit</td>
</tr>
<tr>
<td>Oracle Fusion Project Portfolio</td>
<td>Project Organization Classification</td>
</tr>
<tr>
<td>Management</td>
<td></td>
</tr>
<tr>
<td>Oracle Fusion Incentive</td>
<td>Business Unit</td>
</tr>
<tr>
<td>Compensation</td>
<td></td>
</tr>
</tbody>
</table>

Assigning Data Access

Assigning data access to users is a three step process:

1. Create users using one of the following:
   - Manage Users task in Oracle Fusion Functional Setup Manager
     - Specify user attributes such as user name, assigned business unit, legal employer, department, job, position, grade, and location.
   - Security Console

2. Assign at least one job role to users. Use Oracle Fusion Human Capital Management or the Security Console to assign job roles.
3. Assign data access using the Manage Data Access for Users task in the Functional Setup Manager. For General Ledger users, you can also use the Manage Data Access Set Data Access for Users task to assign data access.

Creating Application Users for Oracle Incentive Compensation Cloud

Follow the steps in this example to create Oracle Incentive Compensation Cloud application users.

Before creating application users, make sure you have:

- Set up any additional resource roles or autoprovisioning rules for job and abstract roles that are required.

> **Note:** When you create application users, you automatically set up the HR management hierarchy by indicating each person’s manager. For this reason, you must first create the user at the top of the hierarchy and work your way down.

Steps to Create an Application User

To create an application user:

1. In the Navigator, select the Manage Users link under the My Team heading.
   
The Manage Users page appears.
2. Click Create.
   
The Create User page appears.
3. In the Personal Details region, enter the following values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>Enter the user’s last name. This entry is required.</td>
</tr>
<tr>
<td>First Name</td>
<td>Optionally, enter the user’s first name.</td>
</tr>
<tr>
<td>E-Mail</td>
<td>Enter a unique e-mail. The application sends the initial password notification to this e-mail by default. You can change the default behavior so that e-mail notifications are not sent, or are sent to a different e-mail to the user’s. For information, see the topic Setting Up E-Mail Notifications for New Users: Procedure.</td>
</tr>
</tbody>
</table>

You can leave the Hire Date as is.

4. In the User Details region, enter the user name.

   If you leave the User Name field blank, then Oracle Identity Manager automatically creates a user name for you. By default, Oracle Identity Manager uses the e-mail as the user name.
5. In the User Notification Preferences region, select the **Send user name and password** option to send the e-mail notification with the login and password to the user when you save the record.

6. In the Employment Information region, enter the following values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Person Type</strong></td>
<td>Select Employee.</td>
</tr>
<tr>
<td><strong>Legal Employer</strong></td>
<td>Select the legal employer Oracle created using the information you provided when you signed up with the service.</td>
</tr>
<tr>
<td><strong>Business Unit</strong></td>
<td>Select the business unit for the user. Oracle creates an initial business unit using the information you provided when you signed up with the service.</td>
</tr>
<tr>
<td><strong>Job and Job Grade</strong></td>
<td>Optionally select the job and job grade values. If you have defined provisioning rules based on these values, then always select the job and job grade values.</td>
</tr>
<tr>
<td><strong>Department</strong></td>
<td>Optionally select the department. If you have defined provisioning rules based on these values, then always select the department.</td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>Optionally select the location. If you have defined provisioning rules based on these values, then always select the location.</td>
</tr>
<tr>
<td><strong>Manager</strong></td>
<td>Select the user’s manager. The management hierarchy is used for participant reporting and routing of incentive compensation business objects, such as paysheets.</td>
</tr>
</tbody>
</table>

7. In the Resource Information region, enter the following values if you have defined provision rules using the resource role.

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource Role</strong></td>
<td>Select the role the user plays in the resource organization.</td>
</tr>
</tbody>
</table>

8. Click **Autoprovision Roles**.

Any roles for which the user qualifies automatically appear in the Role Requests table with the status Add Requested.

The application provisions roles according to the provisioning you have set up. Each employee user must have both the Employee abstract role in addition to the job roles they require.

9. You can also provision a role manually to the user if required by clicking Add Role. The Add Role dialog box opens.

10. Search for and select the role. The role is added to the Role Requests table with the status Add Requested.

   **Tip:** Roles that you can provision to others appear in a role mapping for which you satisfy the role-mapping conditions and where the Requestable option is selected for the role.

11. Click **Save and Close**.
Assigning Data Access to Users: Worked Example

Use the Manage Data Access for Users page to assign data access to users based on their job roles. You can assign data access to:

- One user at a time
- Group of users with similar job roles

This example demonstrates how you can assign access to a business unit to a group of users with similar job roles. The following table summarizes the key decisions for this scenario:

<table>
<thead>
<tr>
<th>Decision to Consider</th>
<th>In This Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which user role is being given data access?</td>
<td>Accounts Payable Manager</td>
</tr>
<tr>
<td>What is the security context to which access is being given?</td>
<td>Business Unit</td>
</tr>
</tbody>
</table>

Prerequisites

Before you can complete this task, you must:

1. Create users and specify the user attributes such as a user name, assigned business unit, legal employer, department, job, position, grade and location, and so on. To create users, use the Manage Users task in the Functional Setup Manager or the Create User page. If you're implementing Oracle Fusion HCM, you can also use the Hire an Employee page. You can also use the Security Console to create the implementation users who create the setups, such as legal entities, business units, and so on, that are needed to create the users in the Manage Users or Hire an Employee page.

2. Assign users their job roles. You can either use Oracle Fusion Human Capital Management or the Security Console to assign job roles.

3. Run the Retrieve Latest LDAP Changes process.

Assigning Data Access to Users Using a Spreadsheet

1. Sign in to the Functional Setup Manager as an IT Security Manager or Application Implementation Consultant and navigate to the Setup and Maintenance page.

2. Search for and select the Manage Data Access for Users task. Alternatively, you can perform this task through the product specific task list.

3. Click Users without Data Access to view users who don’t have data access. Alternatively, to assign additional data access to users, use the Users with Data Access option.

4. Select the Security Context, for our example, select Business Unit.

5. Search for users with no data access. For our example, enter Accounts Payable Specialist in the Role field.
Note: The search fields are related to the user attributes.

6. Click **Search**. The Search Results region displays users who don’t have any data access.
7. Click the **Authorize Data Access** button to export the search results to a Microsoft Excel spreadsheet. You can provide data access to a group of users through the spreadsheet.
8. Click **OK** to open the spreadsheet using Microsoft Excel.
9. Select the **Security Context** from the drop-down list for each user.
10. Enter the **Security Context Value**.
   - To provide additional data access to the user, add a new row and enter the user name, role, security context, and security context value.
   - You can click the **View Data Access** button to see what other data access the user already has even if this is outside the parameters of the search. This may help to identify users you want to grant access to because of existing access.
11. Click the **Upload** button on the spreadsheet when you have assigned data access.
12. Select the upload options on the Upload Options window and click **OK**.
13. Note the status of your upload in the **Upload** column.
   - If the status of the upload is **Successful** and there are no validation errors in the log file, you can view the data access assignment to the users using the search criteria on the Manage Data Access for Users page.
   - If the upload status is **Failed**, check the details in your upload file, correct any errors, and upload the file again.
Managing Application Users

Resetting User Passwords

Setup users, who are provisioned with the IT Security Manager job role, can use the Users tab in the Security Console work area to reset passwords for all application users. Users who cannot access to the Security Console can reset only their own passwords using the Set Preferences link in the Settings and Actions menu available by clicking their user name in the application or by using the Forgot Password link on the sign-in page.

Note: Use the Security Console only for changing passwords and for updating user account information such as user first and last name, e-mail address, and status. To manage users, use the Manage Users work area.

To reset a user’s password in the Security Console, do the following:

1. From the implementation project, open the Manage Application Security Preferences task. Alternatively, you can search for this task by name in the Setup or Maintenance work area or use the Navigator.

   You can close any warnings regarding the scheduling of the Import Users and Roles Application Security Data job.

2. Click the Users tab.

3. Search for the user using one of the following:
   
   - First or last name, but not both
   - User name

   The following figure shows the Users tab in the Security Console work area.

4. From the Action menu (callout 1 in the preceding figure), select Reset Password.
The Reset Password window appears, as shown in the following figure. The window displays the password strength policy, which is set on the Security Console Administration tab.

5. If you want the application to send an e-mail to users with a URL that they can use to create their own passwords, then select the **Automatically generate password** option.

6. To reset the password yourself, do the following:
   a. Select the **Manually change the password** option
   b. Enter the new password twice.

   **Note:** The option to reset a password to an automatically generated value is always available. For the manual-reset option, you must select the **Administrator can manually reset password** option on the Security Console **Administration** tab.

7. Click **Reset Password**.

### Inactive Users Report

Run the Inactive Users Report to identify users who haven’t signed in for a specified period.

To run the report:

1. Select **Navigator - Tools - Scheduled Processes** to open the Scheduled Processes work area.
2. Click **Schedule New Process**.
3. Search for and select the Import User Login History process.

   **Note:** Whenever you run the Inactive Users Report process, you must first run the Import User Login History process. This process imports information that the Inactive Users Report process uses to identify inactive users. You’re recommended to schedule Import User Login History to run daily.

4. When the Import User Login History process completes, search for and select the Inactive Users Report process.
5. In the **Process Details** dialog box, set parameters to identify one or more users.
6. Click **Submit**.

### Inactive Users Report Parameters

All parameters except **Days Since Last Activity** are optional.
User Name Begins With
Enter one or more characters.

First Name Begins With
Enter one or more characters.

Last Name Begins With
Enter one or more characters.

Department
Enter the department from the user’s primary assignment.

Location
Enter the location from the user’s primary assignment.

Days Since Last Activity
Enter the number of days since the user last signed in. Use this parameter to specify the meaning of the term inactive user in your enterprise. Use other parameters to filter the results.

This value is required and is 30 by default. This value identifies users who haven’t signed in during the last 30 or more days.

Last Activity Start Date
Specify the start date of a period in which the last activity must fall.

Last Activity End Date
Specify the end date of a period in which the last activity must fall.

Viewing the Report
The process produces an Inactive_Users_List_processID.xml file and a Diagnostics_processID.zip file.

The report includes the following details for each user who satisfies the report parameters:

- Number of days since the user was last active
- Date of last activity
- User name
- First and last names
- Assignment department
- Assignment location
- City and country
- Report time stamp
Related Topics

- Importing User Login History: Explained
9 Using the Security Console

Security Console Visualizations: Explained

On the Roles tab, you can review role hierarchies. You see either a tabular or a graphical view of a role hierarchy. Which view you see by default depends on the setting of the Enable default table view option on the Administration tab. This topic describes how to use each of these views.

Role hierarchies stretch from users at the top of the hierarchy to privileges at the bottom. In both graphical and tabular views, you can set the direction of the displayed hierarchy.

- To show from the selected user, role, or privilege up the hierarchy, set Expand Toward to Users.
- To show from the selected user, role, or privilege down the hierarchy, set Expand Toward to Roles.

The Tabular View

If the tabular view doesn’t appear when you select a security artifact on the Roles tab, then you can click the View as Table icon. In the tabular view, you can:

- Review the complete role hierarchy for a selected user or role. The table shows roles inherited both directly and indirectly.
- Search for a security artifact by entering a search term in the field above any column and pressing Enter.
- Set the contents of the table as follows:
  - If Expand Toward is set to Privileges, then you can set Show to either Privileges or Roles.
  - If Expand Toward is set to Users, then you can set Show to either Roles or Users.

The resulting contents of the table depend on the start point. For example, if you select a privilege, Expand Toward is set to Privileges, and Show is set to Roles, then the table is empty.

- Export the displayed details to a Microsoft Excel spreadsheet.

The Graphical View

If the graphical view doesn’t appear when you select a security artifact on the Roles tab, then you can click the Show Graph icon. In the graphical view, users, privileges, and the various types of roles are represented by nodes and differentiated by both color and labels. These values are defined in the Legend. You can:

- Review roles inherited directly by the selected role or user. To see roles and privileges inherited indirectly, select a directly inherited role, right-click, and select either Expand or Expand All. Select Collapse or Collapse All to reverse the action. Alternatively, double-click a node to expand or collapse it.
- Use the Set as Focus action to make any selected node the center of the visualization.
- Use the Overview in the bottom right of the display area to manipulate the visualization. For example, clicking a node in the Overview moves the node to the center of the visualization. You can also use drag and drop.
- Hover on a Legend entry to highlight the corresponding nodes in the visualization. Click a legend entry to add or remove corresponding nodes in the visualization.
In the Control Panel, you can:

- Switch the layout between radial and layered representations.
- Click the **Search** icon and enter a search term to find a security artifact among currently displayed nodes.
- Zoom in and out using either the **Zoom in** and **Zoom out** icons or the mouse wheel.
- Magnify areas of the visualization by clicking the **Magnify** icon and dragging it to the area of interest. Click the icon again to switch it off.
- Click the **Zoom to Fit** icon to center the image and fill the display area

**Simulating Navigator Menus in the Security Console: Procedure**

You can simulate Navigator menus available to roles or users. From a simulation, you can review the access inherent in a role or granted to a user. You can also determine how to alter that access to create roles.

**Opening a Simulation**

To open a simulated menu:

1. Select the Roles tab in the Security Console.
2. Create a visualization graph, or populate the Search Results column with a selection of roles or users.
3. In the visualization graph, right-click a role or user. Or, in the Search Results column, select a user or role and click its menu icon.
4. Select **Simulate Navigator**.

**Working with the Simulation**

In a Simulate Navigator page:

- Select **Show All** to view all the menu and task entries that may be included in a Navigator menu.
- Select **Show Access Granted** to view the menu and task entries actually assigned to the selected role or user.

In either view:

- A padlock icon indicates that a menu or task entry can be, but is not currently, authorized for a role or user.
- An exclamation icon indicates an item that may be hidden from a user or role with the privilege for it, because it has been modified.

To plan how this authorization may be altered:

1. Click any blue menu entry.
2. Select either of two options:
   - One lists roles that grant access to the menu item.
   - The other lists privileges required for access to the menu item.
Security Console Analytics: Explained

Use the Analytics page in the Security Console functional area to review statistics about:

- Role Categories. Each role belongs to a category that defines some common purpose. Typically, a category contains a type of role configured for an application, for example "Financials - Duty Roles."

  For each category, a Roles Category grid displays the number of:
  - Roles
  - Role memberships (roles belonging to other roles within the category)
  - Security policies created for those roles

  In addition, a Roles by Category pie chart compares the number of roles in each category with those in other categories.

- Roles in Category. Click a category in the Role Categories grid to list roles belonging to that category. For each role, the Roles in Category grid also shows the number of:
  - Role memberships
  - Security policies
  - Users assigned the role

- Individual role statistics. Click the name of a role in the Roles in Category grid to list the security policies and users associated with the role. The page also presents collapsible diagrams of hierarchies to which the role belongs.

Click Export to export data from this page to a spreadsheet.
10 Reviewing Roles and Role Assignments

Reviewing Role Assignments: Procedure

You can use the Security Console to:

• View the roles assigned to a user.
• Identify users who have a specific role.

You must have the IT Security Manager job role to perform these tasks.

Viewing the Roles Assigned to a User

Follow these steps:

2. On the Security Console, search for and select the user.

Depending on the enterprise setting, either a table or a graphical representation of the user’s role hierarchy appears. Switch to the graphical representation if necessary to see the user and any roles that the user inherits directly. User and role names appear on hover. To expand an inherited role:

1. Select the role and right-click.
2. Select Expand. Repeat these steps as required to move down the hierarchy.

Tip: Switch to the table to see the complete role hierarchy at once. You can export the details to Microsoft Excel from here.

Identifying Users Who Have a Specific Role

Follow these steps:

1. On the Security Console, search for and select the role.
2. Depending on the enterprise setting, either a table or a graphical representation of the role hierarchy appears. Switch to the graphical representation if it doesn’t appear by default.
3. Set Expand Toward to Users.

Tip: Set the Expand Toward option to control the direction of the graph. You can move either up the hierarchy from the selected role (toward users) or down the hierarchy from the selected role (toward privileges).

In the refreshed graph, blue diamond shapes identify users. User names appear on hover. Users may inherit roles either directly or indirectly from other roles, which appear as green circles. Expand a role to view its hierarchy.

4. In the Legend, click the Tabular View icon for the User icon. The table lists all users who have the role. You can export this information to Microsoft Excel.
Reviewing Role Hierarchies: Explained

On the Security Console you can review the role hierarchy of a job role, an abstract role, or a duty role. You must have the IT Security Manager job role to perform this task.

To review a role’s hierarchy:

1. On the home page, click **Tools - Security Console**.
2. On the Security Console, ensure that the **Expand Toward** field is set to **Privileges**.
3. Search for and select the role.

   Depending on the enterprise setting, either a table or a graphical representation of the role is displayed.

4. If the table doesn’t appear by default, click the **View as Table** icon.

   The table lists every role inherited either directly or indirectly by the selected role. To view the privileges inherited by the role, set the **Show** field to **Privileges**.

   **Tip:** Enter text in the field above a column and press **Enter** to show only those roles or privileges that contain the specified text.

5. Click **Export to Excel** to export the current table data to Microsoft Excel.

Comparing Roles: Procedure

Compare any two roles to see the structural differences between them.

For example, assume you have copied a role and customized the copy. You then upgrade to a new release. You can compare your customized role from the earlier release with the role as shipped in the later release. You may then decide whether to incorporate upgrade changes into your custom role.

1. Select the Roles tab in the Security Console.
2. Do any of the following:
   - Click the **Compare Roles** button.
   - Create a visualization graph, right-click one of its roles, and select the **Compare Roles** option.
   - Generate a list of roles in the **Search Results** column of the Roles page. Select one of them, and click its menu icon. In the menu, select **Compare Roles**.
3. Select roles for comparison:
   - If you began by clicking the Compare Roles button, select roles in both **First Role** and **Second Role** fields.
   - If you began by selecting a role in a visualization graph or the Search Results column, the **First Role** field displays the name of the role you selected. Select another role in the **Second Role** field.

   For either field, click the search icon, enter text, and select from a list of roles whose names contain that text.

4. Filter for any combination of these artifacts in the two roles:
   - Function security policies
49

5. For the combination you select, choose whether to show:
   - All artifacts
   - Those that exist only in one role, or only in the other role
   - Those that exist only in both roles

6. Click the Compare button.

After you create the initial comparison, you can change the filter and show options. When you do, a new comparison is generated automatically.

Reviewing Roles and Role Assignments in Identity Manager: Procedure

You can use Oracle Identity Manager to manage Incentive Compensation job roles.

This procedure explains how to use Oracle Identity Manager to:

- View the roles assigned to a user.
- List users who have a specific role.

Viewing the Roles Assigned to a User in Oracle Identity Manager

Sign in to Oracle Sales Cloud with the IT Security Manager job role and follow these steps:

1. Select Navigator - Tools - Setup and Maintenance to open the Setup and Maintenance work area.
2. On the All Tasks tab of the Overview page, search for and select the Manage Job Roles task.
   The Oracle Identity Manager - Self Service page opens.
3. On the Welcome tab of the Oracle Identity Manager - Self Service page, click the Administration link in the top-right corner.
   The Oracle Identity Manager - Delegated Administration page opens.
4. On the Welcome tab of the Oracle Identity Manager - Delegated Administration page, click Advanced Search - Users. In the Display Name field, enter a user’s display name (for example, John Smith) and select this user’s name in the search results.
   A user page opens for this user.
5. Click the Roles tab to view the roles assigned to the user. This page shows all abstract and job roles (if any) assigned to this user.
6. Return to the Welcome tab on the Oracle Identity Manager - Delegated Administration page.

Listing Users Who Have a Specific Role in Oracle Identity Manager

Follow these steps:

1. On the Welcome tab of the Oracle Identity Manager - Delegated Administration page, click Advanced Search - Roles.
2. Search for a role, for example, the Incentive Compensation Participant Manager abstract job role, and open it. The role page opens for the role. The Attributes tab of the role page shows the role category name, such as IC - Job Roles. This value identifies both the role type and the application where the role is used.

3. Click the Members tab. On this tab, you can see all users who currently have the selected role.

4. Click the Overview - Setup and Maintenance tab to return to Oracle Setup and Maintenance.

---

**Viewing the Duties of a Predefined Job Role in Authorization Policy Manager: Procedure**

Job roles and abstract roles inherit privileges from duty roles as well as inheriting privileges directly. To view the duties inherited by a predefined job role, you can:

- Use the Security Console
- Run the User and Role Access Audit Report
- Use Authorization Policy Manager

This topic explains how to view the duties of a job or abstract role using Authorization Policy Manager.

To view the duties of a job role, sign in using the IT Security Manager role and follow these steps:

1. Select **Navigator - Tools - Setup and Maintenance** to open the Setup and Maintenance work area.
2. Search for and open the Manage Duties task. The Authorization Management page opens.
3. In the Application Name section of the Authorization Policy Manager Home tab, select fscm.
4. In the Search and Create section, click **Search - External Roles**.
   The Search External Roles page opens. Job roles and abstract roles are known as external roles in Authorization Policy Manager.
5. In the **Display Name** field, enter the name of the job role. For example, enter Incentive Compensation Analyst. Click **Search**.
6. Select the job role in the Search Results and click **Open Role**.
7. On the job role page, click the Application Role Mapping tab and open the fscm folder. In the fscm folder you can see the top-level application role associated with the job role. Expand the application role to view the duty roles the job role inherits, for example the Incentive Compensation Credit and Earnings Duty and the Incentive Compensation Participant Assignments Duty.
8. When your review is complete, click the Overview - Setup and Maintenance tab to return to the Setup and Maintenance work area.

---

**User and Role Access Audit Report**

The User and Role Access Audit Report provides details of the function and data security granted to specified users or roles. This information is equivalent to the information that you can see for a user or role on the Security Console. This report is based on data in the Applications Security tables, which you populate by running the Import User and Role Application
Security Data process. Any security changes made outside the Security Console since that process last ran may not appear in the User and Role Access Audit Report.

To run the User and Role Access Audit Report:

1. Select **Navigator - Tools - Scheduled Processes** to open the Scheduled Processes work area.
2. Click **Schedule New Process**.
3. Search for and select the User and Role Access Audit Report.
4. In the **Process Details** dialog box, set parameters and click **Submit**.
5. Click **OK** to close the confirmation message.

**User and Role Access Audit Report Parameters**

**Report Type**

Set this parameter to one of these values to run the report for one user, one role, multiple users, or all roles.

- All roles
- Multiple users
- Role name
- User name

**User Name**

Search for and select the user name of a single user.

This field is enabled only when **Report Type** is **User name**.

**Role Name**

Search for and select the name of a single aggregate privilege or data, job, abstract, or duty role.

This field is enabled only when **Report Type** is **Role name**.

**From User Name Starting With**

Enter one or more characters from the start of the first user name in a range of user names.

This field is enabled only when **Report Type** is **Multiple users**.

**To User Name Starting With**

Enter one or more characters from the start of the last user name in a range of user names.

This field is enabled only when **Report Type** is **Multiple users**.

**User Role Name Starts With**

Enter one or more characters from the start of a role name.

This field is enabled only when **Report Type** is **Multiple users**.
Viewing the Report Results

The report produces three .zip files, one of data security policies and two of functional security policies in hierarchical and tabular formats. The file names are in the following format: [FILE_PREFIX]_[PROCESS_ID]_[DATE]_[TIME]_[FILE_SUFFIX]. The file prefix depends on the specified **Report Type** value, as shown in this table.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>File Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>USER_NAME</td>
</tr>
<tr>
<td>Role name</td>
<td>ROLE_NAME</td>
</tr>
<tr>
<td>Multiple users</td>
<td>MULTIPLE_USERS</td>
</tr>
<tr>
<td>All roles</td>
<td>ALL_ROLES</td>
</tr>
</tbody>
</table>

This table shows the file suffix, file format, and file contents for each report type.

<table>
<thead>
<tr>
<th>Report Type</th>
<th>File Suffix</th>
<th>File Format</th>
<th>File Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>DataSec</td>
<td>XML</td>
<td>Data security policies. The .zip file contains one file for each user or role.</td>
</tr>
<tr>
<td>Any</td>
<td>Hierarchical</td>
<td>XML</td>
<td>Functional security policies in a hierarchical format. The .zip file contains one file for each user or role.</td>
</tr>
<tr>
<td>User name</td>
<td>TabularFormat</td>
<td>XML</td>
<td>Functional security policies in a tabular format.</td>
</tr>
<tr>
<td>Role name</td>
<td></td>
<td>CSV</td>
<td>Functional security policies in a comma-separated, tabular format.</td>
</tr>
<tr>
<td>Multiple users</td>
<td>CSV</td>
<td>CSV</td>
<td></td>
</tr>
<tr>
<td>All roles</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The process also produces a .zip file containing a diagnostic log.

For example, if you report on a job role at 13.30 on 17 December 2015 with process ID 201547, then the report files are:

- ROLE_NAME_201547_12-17-2015_13-30-00_DataSec.zip
- ROLE_NAME_201547_12-17-2015_13-30-00_Hierarchical.zip
- ROLE_NAME_201547_12-17-2015_13-30-00_TabularFormat.zip
- Diagnostic.zip
11 Certificate Management

Managing Certificates: Explained

Certificates establish keys for the encryption and decryption of data that Oracle Cloud applications exchange with other applications. Use the Certificates page in the Security Console functional area to work with certificates in either of two formats, PGP and X.509.

For each format, a certificate consists of a public key and a private key. The Certificates page displays one record for each certificate. Each record reports these values:

- **Type**: For a PGP certificate, "Public Key" is the only type. For an X.509 certificate, the type is either "Self-Signed Certificate" or "Trusted Certificate" (one signed by a certificate authority).
- **Private Key**: A check mark indicates that the certificate’s private key is present. For either certificate format, the private key is present for your own certificates (those you generate in the Security Console). The private key is absent when a certificate belongs to an external source and you import it through the Security Console.
- **Status**: For a PGP certificate, the only value is "Not Applicable." (A PGP certificate has no status.) For an X.509 certificate, the status is derived from the certificate.

To the right in the row for each certificate, click a button to display a menu of actions appropriate for the certificate. Or, to view details for a certificate, select its name ("alias"). Actions include:

- Generate PGP or X.509 certificates.
- Generate signing requests to transform X.509 certificates from self-signed to trusted.
- Export or import PGP or X.509 certificates.
- Delete certificates.

Generating Certificates: Explained

For a PGP or X.509 certificate, one operation creates both the public and private keys. From the Certificates page, select the Generate option. In a Generate page, select the certificate format, then enter values appropriate for the format.

For a PGP certificate, these values include:

- An alias (name) and passphrase to identify the certificate uniquely.
- The algorithm by which keys are generated, DSA or RSA.
- A key length.

For an X.509 certificate, these values include:

- An alias (name) and private key password to identify the certificate uniquely.
- A common name, which is an element of the "distinguished name" for the certificate. The common name identifies the entity for which the certificate is being created, in its communications with other web entities. It must match the name of the entity presenting the certificate. The maximum length is 64 characters.
Optionally, other identifying values: Organization, Organization Unit, Locality, State/Province, and Country. These are also elements of the distinguished name for the certificate, although the Security Console does not perform any validation on these values.

- An algorithm by which keys are generated, MD5 or SHA1.
- A key length.
- A validity period, in days. This period is preset to a value established on the General Administration page. You can enter a new value to override the preset value.

Generating a Signing Request: Procedure

You can generate a request for a certificate authority (CA) to sign a self-signed X.509 certificate, to make it a trusted certificate. (This process does not apply to PGP certificates.)

1. Select Generate Certificate Signing Request. This option is available in either of two menus:
   - One menu opens in the Certificates page, from the row for a self-signed X.509 certificate.
   - The other menu is the Actions menu in the details page for that certificate.
2. Provide the private key password for the certificate, then select a file location.
3. Save the request file. Its default name is [alias]_CSR.csr.

You are expected to follow a process established by your organization to forward the file to a CA. You would import the trusted certificate returned in response.

Importing and Exporting X.509 Certificates: Procedure

For an X.509 certificate, you import or export a complete certificate in a single operation.

To export:

1. From the Certificates page, select the menu available in the row for the certificate you want to export. Or open the details page for that certificate and select its Actions menu.
2. In either menu, select Export, then Certificate.
3. Select a location for the export file. By default, this file is called [alias].cer.

To import, use either of two procedures. Select the one appropriate for what you want to do:

- The first procedure replaces a self-signed certificate with a trusted version (one signed by a CA) of the same certificate. (A prerequisite is that you have received a response to a signing request.)
  - In the Certificates page, locate the row for the self-signed certificate, and open its menu. Or, open the details page for the certificate, and select its Actions menu. In either menu, select Import.
  - Enter the private key password for the certificate.
  - Browse for and select the file returned by a CA in response to a signing request, and click the Import button.

In the Certificates page, the type value for the certificate changes from self-signed to trusted.

- The second procedure imports a new X.509 certificate. You can import a .cer file, or you can import a keystore that contains one or more certificates.
  - In the Certificates page, click the Import button. An Import page opens.
b. Select X.509, then choose whether you are importing a certificate or a keystore.

c. Enter identifying values, which depend on what you have chosen to import. In either case, enter an alias (which, if you are importing a .cer file, need not match its alias). For a keystore, you must also provide a keystore password and a private key password.

d. Browse for and select the import file.

e. Select Import and Close.

Importing and Exporting PGP Certificates: Procedure

For a PGP certificate, you export the public and private keys for a certificate in separate operations. You can import only public keys. (The assumption is that you will import keys from external sources, who will not provide their private keys to you.)

To export:

1. From the Certificates page, select the menu available in the row for the certificate you want to export. Or open the details page for that certificate and select its Actions menu.
2. In either menu, select Export, then Public Key or Private Key.
3. If you selected Private Key, provide its passphrase. (The public key does not require one.)
4. Select a location for the export file. By default, this file is called [alias]_pub.asc or [alias]_priv.asc.

To import a new PGP public key:

1. On the Certificates page, select the Import button.
2. In the Import page, select PGP and specify an alias (which need not match the alias of the file you are importing).
3. Browse for the public-key file, then select Import and Close.

The Certificates page displays a record for the imported certificate, with the Private Key cell unchecked.

Use a distinct import procedure if you need to replace the public key for a certificate you have already imported, and do not want to change the name of the certificate:

1. In the Certificates page, locate the row for the certificate whose public key you have imported, and open its menu. Or, open the details page for the certificate, and select its Actions menu. In either menu, select Import.
2. Browse for the public-key file, then select Import.

Deleting Certificates: Procedure

You can delete both PGP and X.509 certificates:

1. In the Certificates page, select the menu available in the row for the certificate you want to delete. Or, in the details page for that certificate, select the Actions menu.
2. In either menu, select Delete.
3. Respond to a warning message. If the certificate’s private key is present, you must enter the passphrase (for a PGP certificate) or private key password (for an X.509 certificate) as you respond to the warning. Either value would have been created as your organization generated the certificate.
12 Customizing Security

Security Customization: Overview

This chapter describes some of the ways in which you can customize the Oracle Sales Cloud security model.

The Oracle implementation of role-based access control is designed to handle a wide range of security requirements in different environments. As a result, most companies can use the standard security settings without modification. If necessary, however, you can configure the default settings to meet specific business requirements. For example, you can create custom roles and role hierarchies. Before making any changes to the security reference implementation, however, do the following:

- Clearly define the change that is required and review the proposed changes with Oracle Support.
- Make sure you understand the interrelationships of the various security components and the effect of the proposed change on user access.
- Document any changes you make.

For additional information about changing the standard security settings for Oracle Sales Cloud, go to the Security Resource Center, which is available at 1609084.1 (Article ID) on My Oracle Support. The Security Resource Center provides templates you can use to track the changes you make to standard settings.

Customizing Security: Points to Consider

If the predefined security reference implementation doesn’t fully represent your enterprise, then you can make changes.

For example, the predefined Incentive Compensation Analyst job role includes payment duties. If some business groups in your organization have the incentive compensation manager do all payment processing, then you can create a custom Analyst role without those duties. Alternatively, if a predefined job role is too narrowly defined, then you can create a job role with a greater range of duties than its predefined equivalent.

During implementation, you evaluate the predefined roles and decide whether changes are needed. The Functional Setups User abstract role is required for any custom role intended to perform implementation tasks.

⚠️ Caution: Never edit the predefined roles. (You can identify predefined application roles by the ORA prefix in the role code.)

During each upgrade, predefined roles are updated to the specifications for that release, so any customizations would be overwritten. Instead, use one of these options:

- Copy the predefined roles and edit the copies in the Security Console.
- Create custom roles from scratch in the Security Console.

All predefined roles are granted many function security privileges and data security policies. They also inherit duty roles. To make minor changes to a role, copying the predefined role and editing the copy is the more efficient approach. Creating roles from scratch is most successful when the role has very few privileges and you can identify them easily.
Missing Enterprise Jobs
If jobs exist in your enterprise that aren't represented in the security reference implementation, then you create custom job roles. Add duty roles to custom job roles, as appropriate.

Predefined Roles with Different Privileges
If the privileges for a predefined job role don’t match the corresponding job in your enterprise, then you create a custom version of the role. If you copy the predefined role, then you can edit the copy to add or remove duty roles, function security privileges, and data security policies, as appropriate.

Predefined Roles with Missing Privileges
If the privileges for a job aren’t defined in the security reference implementation, then you create custom duty roles.

Creating Job or Abstract Roles from Scratch: Procedure
If the predefined roles aren’t suitable or you need a role with few privileges, then you can create a role from scratch. This topic explains how to create a job role or abstract role. To perform this task, you must have the IT Security Manager job role.

Entering Basic Information
Follow these steps:

1. On the Roles tab of the Security Console, click Create Role.
2. On the Create Role: Basic Information page, enter the role’s display name in the Role Name field. For example, enter Sales Department Administration Job Role.
3. Complete the Role Code field. For example, enter SALES_DEPT_ADMIN_JOB.
   Abstract roles have the suffix _ABSTRACT, and job roles have the suffix _JOB.
4. In the Role Category field, select either HCM - Abstract Roles or HCM - Job Roles, as appropriate.
5. Click Next.

Adding Functional Security Policies
When you create a role from scratch, you’re most likely to add one or more aggregate privileges or duty roles to your role. You’re less likely to grant function security privileges directly to the role.

If you aren’t granting function security privileges, then click Next. Otherwise, to grant function security privileges to the role:

2. In the Add Function Security Policy dialog box, search for and select a privilege or role.
3. If you select a role, then click Add Selected Privileges to add all function security privileges from a selected role to your custom role. If you select a single privilege, then click Add Privilege to Role.
4. Click OK to close the confirmation message.
5. Repeat from step 2 for additional privileges.
7. Click Next.
Creating Data Security Policies

Make no entries on the Create Role: Data Security Policies page.

**Note:** Whether this page is enabled for edit depends on the current setting of the Enable edit of data security policies option. Set this option on the Roles subtab of the Security Console Administration tab.

Click Next.

Building the Role Hierarchy

The Create Role: Role Hierarchy page shows the hierarchy of your custom role in tabular format by default. You can add one or more aggregate privileges, job roles, abstract roles, and duty roles to the role. Typically, when creating a job or abstract role you add aggregate privileges. Roles are always added directly to the role that you’re creating.

To add a role:

1. Click the Add Role icon.
2. In the Add Role Membership dialog box, search for and select the role to add.
3. Click Add Role Membership.
4. Click OK to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. When you finish adding roles, close the Add Role Membership dialog box.
7. Click Next.

Provisioning the Role

To provision the role to users, you must create a role mapping in the usual way once the role exists. Don’t provision the role to users here.

**Note:** Whether this page is enabled for edit depends on the current setting of the Enable edit of user role membership option. Set this option on the Roles subtab of the Security Console Administration tab.

Click Next.

Reviewing the Role

On the Create Role: Summary and Impact Report page, review the summary of the changes. Click Back to make corrections. Otherwise:

1. Click Save and Close to save the role.
2. Click OK to close the confirmation message.

Your custom role is available immediately.
Copying and Editing Duty Roles: Procedure

You can copy a duty role and edit the copy to create a custom duty role. Copying duty roles is the recommended way of creating custom duty roles. This topic explains how to copy a duty role and edit the copy. You must have the IT Security Manager job role to perform these tasks.

Copying a Duty Role

To copy a duty role:

1. On the Roles tab of the Security Console, search for the duty role to copy.
2. Select the role in the search results.
   - The role is displayed in tabular format by default. Click the Show Graph icon to show the hierarchy in graphical format.
3. In the search results, click the down arrow for the selected role and select **Copy Role**.
4. In the **Copy Options** dialog box, select a copy option.
   - If you select **Copy top role**, then only the selected role is copied. The copied role inherits the same role instances as the source role.
   - If you select **Copy top role and inherited roles**, then a copy is made of every role in the role hierarchy provided that a copy of the role with the same name doesn’t already exist.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

   **Tip:** The **Role Name** and **Role Code** values are assigned the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. The prefix **ORA_** is also removed from the role code. You can overwrite the default prefix and suffix for the role that you’re copying. However, any roles inherited by the copied role are unaffected by any name changes that you make here.

7. Click the **Summary and Impact Report** train stop.
8. Click **Submit and Close**, then **OK** to close the confirmation message.
9. Review the progress of your copy on the Role Copy Status subtab of the Security Console Administration tab. Once the status is **Complete**, you can edit the copied role.

Editing the Copied Duty Role

To edit the copied role, perform the following steps:

1. On the Roles tab of the Security Console, search for and select your copy of the duty role.
2. In the search results, click the down arrow for the selected role and select **Edit Role**.
3. On the Edit Role: Basic Information page, you can edit the role name and description, but not the role code.
4. Click **Next**.
Managing Functional Security Policies

On the Edit Role: Function Security Policies page, any functional security privileges granted directly to the copied role appear. Click Load Inherited Policies to populate the table with privileges that the role inherits. To view details of the code resources that a privilege secures, select the privilege in the Details section of the page.

You can add or delete existing privileges from copied duty roles but can’t create new functional security policies. To delete a privilege that is added directly to the custom role, select the privilege and click the Delete icon. You can’t delete inherited privileges.

To add a privilege to the role:

1. Click Add Function Security Policy.
2. In the Add Function Security Policy dialog box, search for and select a privilege or role.
3. If you select a role, then click Add Selected Privilege to grant all function security privileges from the role to your custom role. If you select a single privilege, then click Add Privilege to Role.
4. Click OK to close the confirmation message.
5. Repeat from step 2 for additional privileges.

All the privileges you selected are listed on the Edit Role: Function Security Policies page.
7. Click Next.

Managing Data Security Policies

On the Edit Role: Data Security Policies page, any data security policies granted to the copied role appear. You can edit or remove policies from the copied role, or create a new policy for the role, provided that the page is enabled for editing (editing is enabled by default). Whether or not this page is enabled for edit depends on the current setting of the Enable edit of data security policies option. Set this option on the Roles subtab of the Security Console Administration tab. For information about creating, editing, and adding data security policies to a custom role, see the topic Managing Data Security Policies.

Click Next to continue to the next page.

Adding and Removing Inherited Roles

The Edit Role: Role Hierarchy page shows the copied duty role and any duty roles that it inherits. The hierarchy is displayed in tabular format by default. You can add or remove roles.

To remove a role:

1. Select the role in the table.
2. Click the Delete icon.
3. Click OK to close the information message.

To add a role:

1. Click Add Role.
2. In the Add Role Membership dialog box, search for and select the role to add.
3. Click Add Role Membership.
4. Click OK to close the confirmation message.
5. Repeat from step 2 for additional roles.
6. Close the Add Role Membership dialog box.
The Edit Role: Role Hierarchy page shows the updated role hierarchy.

7. Click Next.

Viewing Users Assigned the Role
On the Edit Role: Users page, click Next. You can't provision duty roles directly to users.

Reviewing the Role
On the Edit Role: Summary and Impact Report page, review the summary of changes. Then do the following:

1. Click Back to make corrections.
2. When you have completed any corrections required, click Save and Close to save the role.
3. Click OK to close the confirmation message.

The role is available immediately.

Related Topics
- Copying Sales Roles: Points to Consider

Role Optimization Report
Use the Role Optimization Report to create the most efficient role hierarchy for your organization. Use the report results to evaluate and, if necessary, update your role hierarchy. The report results enable you to create a role hierarchy with the minimum number of roles necessary to authorize every job role to every privilege it is currently authorized to.

⚠️ Important: The use of the Role Optimization Report is not included in the cost of your service subscription or application license and incurs charges in addition to your subscription or licensing fee.

Users with the IT Security Manager role can run the Role Optimization Report, which is available from the security console. You should run this report if you:

- Make changes to the predefined role hierarchy.
- Implement your own role hierarchy instead of the predefined role hierarchy.

⚠️ Important: The process makes no changes to your role hierarchies.

📝 Note: The predefined role hierarchy in the security reference implementation is optimized as delivered.

Report Files
Monitor the process status on the Overview page. When the status value is Succeeded, two files appear in the Log and Output section of the report details. The following table describes the two files:
File Name | Description
--- | ---
ClusterAnalysis-Job-CSVs. zip | Contains one CSV file for every job role. Each CSV file contains the duty roles and privileges that make up the optimized job role hierarchy. The name of a CSV file, identifies the job role hierarchy data that the file contains.

For example, the ClustersforJob-AR_REVENUE_MANAGER_JOB_14240.csv file contains all of the role hierarchy data for the Accounts Receivables Revenue Manager job role.

Diagnostics. zip | Contains a log file that provides technical details about the analysis process. You can use this file for troubleshooting purposes.

Import the raw data from the CSV file into your preferred application to read the results. Report data appears in these two sections:

- Privilege Clusters
- Cluster Details

**Role Optimization Report Results**

**Privilege Clusters**
The Privilege Clusters section lists each privilege and the name of a recommended privilege cluster. Specific cluster recommendations are described in the cluster details section.

**Cluster Details**
A Cluster Details section appears for each privilege cluster referenced in the Privilege Clusters section. Each detail section includes:

- Cluster name.
- Names of recommended candidate roles that map to the privilege cluster.
- Names and descriptions of the jobs and privileges associated with the cluster.

This table provides descriptions of the fields that appear the Cluster Details section:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>The name of the optimized cluster, usually in this format: Cluster ###</td>
</tr>
</tbody>
</table>
| Primary, Secondary, Tertiary Candidate Role | Recommended role mappings for the privileges in the cluster. Up to three recommended duty roles map to the listed privileges.
Select a role. Then assign the privileges in the cluster to that role. |
| Jobs in Cluster | The number of job roles that inherit the privilege cluster.
A list of job names and descriptions is also included. |
| Privileges in Cluster | The number of privileges that make up the cluster.
A list of privilege names and descriptions is also included. |
Managing Database Resources: Procedure

Data security policies secure the database resources of an enterprise. This topic describes how to manage database resources and data security policies if, for example, you want to define and secure custom database resources, or if the predefined data security conditions for a database resource don’t meet your needs. Using the Manage Database Resources and Policies page of the Security Console, you can:

- Define custom database resources
- Create data security policies to secure a custom database resource
- Create new database resource conditions for a database resource

To perform the tasks in this topic, you must have the IT Security Manager job role.

Defining Custom Database Resources

A database resource is a database table or view that corresponds to a business object. When you create a custom business object that you want to secure, you must define its associated database table or view as a database resource. To define a table or view as a database resource, you must:

- Specify the primary key column of the database resource
- Filter columns of the database resource to exclude columns from being included in the row instance sets that can be made available to users through data security policies
- Identify conditions and actions for the database resource to determine what portions of the resource can be secured by data security policies and the operations that can be performed on the data

The following procedure describes each of these tasks.

To define a new custom database resource:

1. On the Security Console Administration tab, select the General subtab, then click **Manage Database Resources**.
   The Manage Database Resources and Policies page is displayed.
2. In the Search Results region, click the Create icon.
   The Create Database Resource page is displayed. The General Information subtab is selected by default.
3. Enter the values shown in the following table for the new database resource.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Name</td>
<td>The name of the custom business object you want to define as a database resource.</td>
</tr>
<tr>
<td>Display Name</td>
<td>The display name of the custom business object</td>
</tr>
<tr>
<td>Data Object</td>
<td>Select the data resource (table or view) that the custom business object represents.</td>
</tr>
<tr>
<td>Module</td>
<td>Select the user module associated with the resource.</td>
</tr>
</tbody>
</table>

When you select a value for the **Data Object** field, the Primary Key Columns and Filter Column Details areas are displayed.
4. Click the **Function Security Enabled** check box if the business object has been enabled for functional security.
5. In the **Primary Key Columns** area, click the Create icon.
6. In the **Primary Key** field, select the primary key column of the database table or view that the business object represents.
7. In the **Filter Column Details** area, select columns you want to exclude from the row instance sets defined by data security policies. The data from filtered columns isn’t accessible by users. To select a column as a data filter, move it from the Available Columns list to the Selected Columns list.
8. Click the Condition subtab to create conditions for the new database resource, then click the Create icon. The **Create Database Resource Condition** dialog box is displayed. Conditions specify the rows of the database resource that can be secured by data security policies.
9. Create resource conditions as described in the procedure Creating Conditions for a Database Resource later in this topic.
10. Click the Action subtab. You define actions on the database resource to specify the operations data security policies can secure on a business object. For example, you can specify whether a user might have read, update, or delete access by naming actions for each of these and granting them in a data security policy to a particular role. An action must correspond with an operation that the business object implements.
11. Click the Add Row icon.
12. Enter a value in the **Name** and **Display Name** fields. The action name you enter must match an operation name defined for the corresponding business object. Actions act on the row instance sets specified by the database resource conditions that you define in a data security policy, that is, conditions determine the row instance set available to a user for a given action.
   You can specify more than one action.
13. Click **Submit**.
14. When the confirmation dialog box is displayed confirming that the database resource was created, click **OK**.

### Creating Conditions for a Database Resource

Database resource conditions define what portions of a database resource can be secured by data security policies. You can’t edit the predefined conditions provided by Oracle but you can create new conditions for a predefined database resource or for a custom database resource.

A condition is a group of row instances that are determined by a simple XML filter or an SQL predicate (WHERE clause) that queries the attributes of the resource itself. You can define a condition to specify multiple row instance sets using an SQL WHERE clause with parameters. You don’t need to define a condition for single row instance conditions (single value) or for all row instance conditions (all values). Both the single-value case and the all-values case can be easily defined when you create the data security policy.

To create conditions for a database resource:

1. On the General subtab of the Security Console Administration tab, click **Manage Database Resources**. The Manage Database Resources and Policies page is displayed.
2. Search for the database resource whose conditions you want to edit.
3. In the Search Results list, select the appropriate database resource, then click the Edit icon. The Edit Data Security page is displayed.
4. Select the Condition subtab to define a new condition for the resource.
Any existing conditions defined for the database resource are displayed. You can’t delete or edit any predefined conditions.

5. Click the Create icon.

The Create Database Resource Condition dialog box is displayed.

6. Enter a name and display name for the condition.

7. For the Condition Type, select one of the following:
   - Select Filter if you want to use the attribute picker to define a simple condition. If you select the filter condition type, you also must specify the following values:
     - For the Match option, select the All option if you want the filter conditions to include AND clauses or select the Any option if you want the filter conditions to include OR clauses.
     - In the Conditions area, click the Add icon.
     - To define the filter values, enter values similar to those in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column Name</td>
<td>Select the column for which you’re defining the filter.</td>
</tr>
<tr>
<td>Tree Operators</td>
<td>Select this option if the operator you want to use in the filter is a tree operator.</td>
</tr>
<tr>
<td>Operator</td>
<td>Choose the operator for the selected column filter.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter a value as the test for the operator.</td>
</tr>
</tbody>
</table>

   - Click Save.
   - Select SQL Predicate if you know the attribute names of your condition and you want to use an SQL predicate consisting of a query on the table or view named by the database resource. Enter the SQL values in the SQL Predicate field.

8. Click Save to save the new condition.

Create a Data Security Policy for a Custom Database Resource

When you register a new business object as a database resource, users will initially be prevented from initiating the operations of the business object or from accessing the data of the resource. You define data security policies to make the data of a custom business object available to the users of the application.

Before you create a data security policy, make sure that the following tasks have been completed:

- Identify the business object that you want to secure and register its associated database table or view as a database resource.
- Identify and define any conditions that you want to make available for the database resource.
- Identify and register the actions that you want to secure for this database resource.

To create a new policy for a custom database resource:

1. On the General subtab of the Security Console Administration tab, click Manage Database Resources.
The Manage Database Resources and Policies page is displayed.

2. Search for the database resource that you want to secure by defining a policy.

3. In the Search Results list, select the database resource, then scroll down to the Policies Details area.

All the policies defined for the database resource are displayed.

4. You can select an existing policy for editing by selecting the policy then clicking the Edit icon. In this case, however, click the Create icon to create a new policy.

The Create Policy dialog box is displayed with the General subtab selected.

5. Specify the following information for the new policy:
   - In the Name field, enter a name for the policy.
   - In the Start Date field, enter the date on which the policy is to become active.

The Module field is pre-filled with the name of the module associated with the database resource for which you’re creating the policy but you can change this value.

6. Click the Roles subtabs, then click the Add icon to select the roles that are to be assigned the new policy.

The Select and Add: Roles dialog box is displayed.

7. Select the roles to be assigned the new policy as follows:
   - In the Role Name field, enter the name of the role.
   - In the Application field, enter the application stripe of the role, for example, CRM, HCM, or FSCM, then click Search.
   - Select a role from the list of roles displayed, then click Apply to associate the role with the new policy.
   - Select any additional roles from the list and, when you have finished adding roles, click OK.

All users assigned the roles you select are provided with access to the data defined in the policy.

8. Click the Rule subtab to define a rule to specify the rows of the database resource to which the policy applies.

9. Select one of the following values in the Row Set field:
   - To secure a specific row, select Single Value, then search for and select the row you want to secure in the Row field.
   - To secure all rows in the resource, select All Values.
   - To secure a subset of the data in the data resource select Multiple Values, then search for and select the condition that defines the subset of the data to be secured in the Condition field.

10. Click the Action subtab, then move actions from the Available Actions list to the Selected Actions list to specify the actions, applicable to the data secured on the database resource, which you want to grant to the role.

11. Click Save and Close.
13 Synchronizing with Oracle Identity Management

Synchronizing User and Role Information: Procedure

You run the process Retrieve Latest LDAP Changes once during implementation. This process copies data from the LDAP directory to the Oracle Fusion Applications Security tables. Thereafter, the data is synchronized automatically. To run this process, perform the task Run User and Roles Synchronization Process as described in this topic.

Running the Retrieve Latest LDAP Changes Process

Follow these steps:

1. Sign in to the application as a setup user.
2. Select Navigator - Setup and Maintenance to open the Setup and Maintenance work area.
3. Search for and select the Run User and Roles Synchronization Process task.
   The process submission page for the Retrieve Latest LDAP Changes process opens.
4. Click Submit.
5. Click OK to close the confirmation message.

Scheduling the Send Pending LDAP Requests Process: Procedure

The Send Pending LDAP Requests process sends bulk requests and future-dated requests that are now active to your LDAP directory. You're recommended to schedule the Send Pending LDAP Requests process to run daily. This procedure explains how to schedule the process.

Note: Schedule the process only when your implementation is complete. Once you schedule the process you can’t run it on an as-needed basis, which may be necessary during implementation.

Scheduling the Send Pending LDAP Requests Process

Follow these steps:

1. Select Navigator - Tools - Scheduled Processes to open the Scheduled Processes work area.
2. Click Schedule New Process in the Search Results section of the Scheduled Processes work area.
3. In the Schedule New Process dialog box, search for and select the Send Pending LDAP Requests process.
4. In the Process Details dialog box, set User Type to identify the types of users to be processed. Values are Person, Party, and All. You’re recommended to leave User Type set to All.
5. The Batch Size field specifies the number of requests in a single batch. For example, if 400 requests exist and you set Batch Size to 25, then the process creates 16 batches of requests to process in parallel.
The value A, which means that the batch size is calculated automatically, is recommended.

6. Click Advanced.
7. On the Schedule tab, set Run to Using a schedule.
8. In the Frequency field, select Daily.
9. Enter the start and end dates and times.
10. Click Submit.

Related Topics
• Send Pending LDAP Requests: Explained

Send Pending LDAP Requests: Explained

You're recommended to run the Send Pending LDAP Requests process daily to send future-dated and bulk requests to your LDAP directory server. Schedule the process in the Scheduled Processes work area. This topic describes the purpose of Send Pending LDAP Requests.

Send Pending LDAP Requests sends the following items to the LDAP directory:

• Requests to create, suspend, and reactivate user accounts.
  o When you create a person record for a worker, a user-account request is generated automatically.
  o When a person has no roles and no current work relationships, a request to suspend the user account is generated automatically.
  o A request to reactivate a suspended user account is generated automatically if you rehire a terminated worker.

The process sends these requests to the LDAP directory unless the automatic creation and management of user accounts are disabled for the enterprise.

• Work e-mails.

If you include work e-mails when you create person records, then the process sends those e-mails to the LDAP directory.

• Role provisioning and deprovisioning requests.

The process sends these requests to the LDAP directory unless automatic role provisioning is disabled for the enterprise.

• Changes to person attributes for individual users.

The process sends this information to the LDAP directory unless the automatic management of user accounts is disabled for the enterprise.

† Note: All of these items are sent to the LDAP directory automatically unless they're either future-dated or generated by bulk data upload. You run the process Send Pending LDAP Requests to send future-dated and bulk requests to the LDAP directory.

Only one instance of Send Pending LDAP Requests can run at a time.
Security for Incentive Compensation Analytics and Reports: Overview

Analytics is available throughout Oracle Incentive Compensation as embedded analytics and also in standalone mode by way of the transactional work areas. Oracle Incentive Compensation users interact with information in Oracle BI Applications and Oracle Transactional Business Intelligence using Oracle Business Intelligence Enterprise Edition (Oracle BI EE) components, such as Dashboards.

The analytics and reports that are delivered with Incentive Compensation are secured based on the roles that use each report. For example, participant managers can access analytics and reports that participants don’t have access to. If you want to create analytics or reports or edit existing ones, then you should become familiar with Incentive Compensation security concepts and how access is secured to Oracle Transactional Business Intelligence subject areas, Oracle BI Presentation Catalog folders, and Oracle Business Intelligence reports.

Subject Areas

Subject areas are functionally secured using duty roles. The supplied user roles include the necessary duty roles to access the Oracle Business Intelligence content. The names of duty roles that grant access to subject areas include the words Transaction Analysis Duty (for example, Incentive Compensation Transaction Analysis Duty). Access to a subject area is needed to run or create reports for that subject area.

Note: The BI Author Role is required to create OTBI reports. By default, the Incentive Compensation Participant job role is not assigned the BI Author role.

BI Presentation Catalog Folders

BI Presentation Catalog folders are functionally secured using the same duty roles that secure access to the subject areas. Therefore, a user who inherits the Incentive Compensation Transaction Analysis Duty can access both the Incentive Compensation folder in the BI Presentation Catalog and the Incentive Compensation subject areas.

Oracle Business Intelligence Reports

Analyses are secured based on the folders in which they’re stored. If you haven’t secured BI reports using the report permissions, then they’re secured at the folder level by default. You can set permissions against folders and reports for application roles, catalog groups, or users.
For More Information

When you receive your Incentive Compensation implementation, access to its functionality and data is secured using role-based access control (RBAC). For more information about securing subject areas, BI catalog folders and reports, see the following guides:

- **Oracle Incentive Compensation Security Reference**
  
  Available from the Oracle Cloud Documentation library, this guide describes the Incentive Compensation application security reference implementation and includes descriptions of all the predefined data that is included in the security reference implementation for an offering. The security reference implementation can be customized to fit divergent enterprise requirements.

- **Oracle Fusion Middleware Security Guide for Oracle Business Intelligence Enterprise Edition.**
  
  This guide provides information about using Transactional Analysis Duty roles to secure access to the BI catalog.

Displaying Direct Report Data in Participant Manager Reports: Procedure

You must enable the Secure by Manager Hierarchy person security profile before participant managers can see direct report participant data in their business intelligence reports. The application automatically generates and associates data grants using this security profile.

In the Setup and Maintenance work area:

1. Add the security profile.
2. Refresh the manager hierarchy.

Adding the Security Profile

Only users with either View All HCM Data or IT Security access can do the following.

1. Search for and go to the Manage Data Role and Security Profiles task.
2. Search for roles staring with *Incentive*.
3. In the Search Results section, select *Incentive Compensation Participant Manager*.
4. On the toolbar, click **Assign** to open the Assign Data Role: Role Details page.
5. Click **Next** to open the Security Criteria page.
6. In the Person Security Profile field, select **View Manager Hierarchy**.
7. Click the **Secure by Manager** check box if it isn’t already selected.
8. Click **Review**.
9. Click **Submit** to return to the Manage Data Role and Security Profiles page.
10. Click **Done** to return to the All Tasks tab.
Refreshing the Manager Hierarchy
You must run and schedule the Refresh Manager Hierarchy process to populate the HR Foundation Person tables with the manager hierarchy information. Reporting data is unavailable until you run the process.

1. On the Navigator menu under Tools, select Scheduled Processes.
3. In the Name field, search for and select Refresh Manager Hierarchy.
4. Click OK to return to the Schedule New Process dialog box.
5. Click OK to open the Process Details dialog box.
6. Click Submit, which causes the Confirmation dialog box to appear.
7. Click OK to return to the Process Details dialog box.
8. Click Cancel to return to the Overview page.

Business Intelligence Roles Used by Incentive Compensation: Explained

Business Intelligence roles apply to both Oracle Business Intelligence Publisher (Oracle BI Publisher) and Oracle Transactional Business Intelligence (OTBI). They grant access to Business Intelligence functionality, such as the ability to run or author reports. Users need one or more of these roles in addition to the roles that grant access to reports, subject areas, Business Intelligence catalog folders, and Incentive Compensation data. This topic describes the Business Intelligence roles.

Business Intelligence roles are defined as application roles. This table identifies those roles.

<table>
<thead>
<tr>
<th>Business Intelligence Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BI Consumer Role</td>
<td>Runs Business Intelligence reports.</td>
</tr>
<tr>
<td>BI Author Role</td>
<td>Creates and edits reports.</td>
</tr>
<tr>
<td>BI Administrator Role</td>
<td>Performs administrative tasks such as creating and editing dashboards and modifying security permissions for reports, folders, and so on.</td>
</tr>
<tr>
<td>BI Publisher Data Model Developer Role</td>
<td>Creates and edits Oracle Business Intelligence Publisher data models.</td>
</tr>
</tbody>
</table>

BI Consumer Role
The predefined Incentive Compensation Transaction Analysis Duty roles inherit the BI Consumer Role. The following predefined application roles are assigned the Incentive Compensation Transaction Analysis Duty:

- Incentive Compensation Manager
- Incentive Compensation Analyst
- Incentive Compensation Participant Manager
- Incentive Compensation Participant
BI Author Role
BI Author Role inherits BI Consumer Role. Users with BI Author Role can create, edit, and run OTBI reports.

All predefined Incentive Compensation job roles that inherit an OTBI Transaction Analysis Duty role are also assigned the BI Author Role at the job role level.

The following predefined external job roles are assigned the Transactional Business Intelligence Worker job:

- Incentive Compensation Manager
- Incentive Compensation Analyst
- Incentive Compensation Participant Manager
- Incentive Compensation Participant

BI Administrator Role
BI Administrator Role is a superuser role. It inherits BI Author Role, which inherits BI Consumer Role.

The predefined Incentive Compensation job roles do not have BI Administrator Role access.

BI Publisher Data Model Developer Role
BI Publisher Data Model Developer Role is inherited by the Application Developer role, which is inherited by the Application Implementation Consultant role. Therefore, users with either of these predefined job roles can manage BI Publisher data models.

Customizing Security for Oracle Transactional Business Intelligence: Explained

Oracle Transactional Business Intelligence secures reporting objects and data through the following types of roles:

- Reporting objects and data are secured through the predefined OTBI Transactional Analysis Duty roles, for example, Sales Managerial Transaction Analysis Duty. The Transaction Analysis Duty roles control which subject areas and analyses a user can access and what data a user can see.
- Business Intelligence roles, for example, BI Consumer Role, or BI Author Role. These roles grant access to Business Intelligence functionality, such as the ability to run or author reports. Users need one or more of these roles in addition to the roles that grant access to reports and subject areas to create and run reports and view analytics.

You can’t copy or customize the Business Intelligence roles or the Transaction Analysis Duty roles provided with Oracle Sales Cloud, or the associated security privileges. In addition, any role with a role code prefix of OBIA, for example, Business Intelligence Applications Analysis Duty (OBIA_ANALYSIS GENERIC DUTY), can also not be copied. However, you can customize reporting security according to your security requirements as described in this topic.

Modifying Transaction Analysis Duty Role Assignments
If you want to customize the subject areas that users have access to, then create a custom job role and provide the custom role with the Oracle Transactional Business Intelligence duty roles that provide the required access.
For example, you can create a custom role that provides access to both partner and sales team subject areas by assigning both the Sales Managerial Transaction Analysis Duty and the Partner Channel Transaction Analysis Duty to the custom role.

Modifying Business Intelligence Role Assignments
The Business Intelligence roles enable users to perform tasks within Business Intelligence tools such as Oracle Business Intelligence Publisher. The default Business Intelligence roles used in Oracle Sales Cloud are BI Consumer and BI Author.

The delivered Transaction Analysis Duty roles inherit the BI Consumer Role, which provides view-only access to analyses and reports. You assign the BI Author Role at the job role level, giving you flexibility in granting the BI Author privilege to only those job roles that you want to have access to create and edit analyses and reports.

All predefined Sales Cloud job roles that inherit a Transaction Analysis Duty role are also assigned the BI Author Role by default, except for the Sales Representative job role. However, you can optionally create custom copies of the predefined job roles and add or remove the BI Author Role from the custom roles as required.

Viewing Reporting Security Roles: Procedure

Viewing reporting roles can help you to understand Oracle Transactional Business Intelligence (OTBI) security. This topic explains how to view the following:

1. OTBI roles that a job role inherits
2. All of the duty roles you are assigned

Note: A user must be assigned the Transactional Analysis Duty role to run queries and reports. You can verify that a user, or the job role assigned to a user, has the Transactional Analysis Duty by performing the procedures in this topic. The Transactional Analysis Duty role is inherited by the Transactional Business Intelligence Worker abstract role.

Viewing OTBI Duty Roles Assigned to a Job Role

To view all the duty roles assigned to a job role, perform the steps in the following procedure.

1. Sign in with the IT Security Manager job role.
2. Select Navigator - Tools - Setup and Maintenance to open the Setup and Maintenance work area.
3. On the All Tasks tab of the Overview page, search for and select the Manage Duties task.

The Oracle Entitlements Server Authorization Management page opens. On the Home tab:

1. In the Application Name section, select fscm.
2. In the Search and Create section, click Search - External Roles.

The Search - External Roles page opens.

4. In the Display Name field, enter the name of the job role. For example, enter Incentive Compensation Participant Manager, then click Search.
5. In the search results, select Incentive Compensation Participant Manager, then click Open Role.

The Incentive Compensation Participant Manager page opens.

6. Select the Application Role Mapping tab.
7. Expand the \texttt{obi} folder.

Notice the Incentive Compensation Transaction Analysis Duty roles that the Incentive Compensation Participant Manager job role inherits. Note also that the Incentive Compensation Participant Manager job role inherits BI Author Role.

8. Expand the Incentive Compensation Transaction Analysis Duty role.

It inherits BI Consumer Role.


Viewing the Duty Roles You Are Assigned

To view all of the duty roles that you are assigned, including Business Intelligence roles and Transactional Analysis Duty roles, perform the following steps.

1. Sign in to Oracle Incentive Compensation using your user ID and password.
2. Select \texttt{Navigator - Tools - Reports and Analytics} to open the Reports and Analytics work area.
3. In the Contents pane, click the Browse Catalog icon. The Business Intelligence Catalog page opens.
4. Click your user name in the global header, then select \texttt{My Account}.
5. Click the Roles and Catalog Groups tab.

All the duty roles you are assigned are listed, including Transaction Analysis Duty roles and Business Intelligence roles.

6. Click \texttt{OK}.
7. Return to the Oracle Fusion Applications window and sign out.

How can I customize Oracle Transactional Business Intelligence duty roles?

If you are using Oracle Incentive Compensation, you can’t customize the delivered OTBI duty roles or the associated security privileges.

You can customize Oracle Transactional Business Intelligence reporting security by assigning different OTBI duty roles to a job role according to your needs.
Advanced Data Security

Advanced Data Security: Explained

Advanced Data Security offers two types of extended data protections. Database Vault protects data from access by highly privileged users and Transparent Data Encryption encrypts data at rest. Advanced Data Security is available for Oracle Applications Cloud by subscription to Break-Glass service.

Oracle Database Vault

Database Vault reduces the risk of highly privileged users such as database and system administrators accessing and viewing your application data. This feature restricts access to specific database objects, such as the application tables and SOA objects.

Administrators can perform regular database maintenance activities, but cannot select from the application tables. If a DBA requires access to the application tables, she can request temporary access to the Fusion schema at which point keystroke auditing is enabled.

Transparent Data Encryption

Transparent Data Encryption (TDE) protects Fusion Applications data which is at rest on the file system from being read or used. Data in the database files (DBF) is protected because DBF files are encrypted. Data in backups and in temporary files is protected. All data from an encrypted tablespace is automatically encrypted when written to the undo tablespace, to the redo logs, and to any temporary tablespace.

Advanced security enables encryption at the tablespace level on all tablespaces which contain applications data. This includes SOA tablespaces which might contain dehydrated payloads with applications data.

Encryption keys are stored in the Oracle Wallet. The Oracle Wallet is an encrypted container outside the database that stores authentication and signing credentials, including passwords, the TDE master key, PKI private keys, certificates, and trusted certificates needed by secure sockets layer (SSL). Tablespace keys are stored in the header of the tablespace and in the header of each operating system (OS) file that makes up the tablespace. These keys are encrypted with the master key which is stored in the Oracle Wallet. Tablespace keys are AES128-bit encryption while the TDE master key is always an AES256-bit encryption.
Glossary

abstract role
A description of a person’s function in the enterprise that is unrelated to the person’s job (position), such as employee, contingent worker, or line manager.

action
The kind of access, such as view or edit, named in a security policy.

aggregate privilege
A predefined role that combines one function security privilege with related data security policies.

assignment
A set of information, including job, position, pay, compensation, managers, working hours, and work location, that defines a worker's or nonworker’s role in a legal employer.

data security
The control of access and action a user can take against which data.

duty role
A group of function and data privileges representing one duty of a job. Duty roles are specific to applications, stored in the policy store, and shared within an application instance.

enterprise
An organization with one or more legal entities under common control.

entitlement
Grant of access to functions and data. Oracle Fusion Middleware term for privilege.

function security
The control of access to a page or a specific use of a page. Function security controls what a user can do.

HCM data role
A job role, such as benefits administrator, associated with instances of HCM data, such as all employees in a department.

job
A generic role that is independent of any single department or location. For example, the jobs Manager and Consultant can occur in many departments.
job role
A role, such as an accounts payable manager or application implementation consultant, that usually identifies and aggregates the duties or responsibilities that make up the job.

LDAP

person type
A subcategory of a system person type, which the enterprise can define. Person type is specified for a person at the assignment level.

privilege cluster
In the output of the Role Optimization Report, a group of privileges that you can map to a duty role.

role
Controls access to application functions and data.

role hierarchy
Structure of roles to reflect an organization’s lines of authority and responsibility. In a role hierarchy, a parent role inherits all the entitlement of one or more child roles.

role mapping
A relationship between one or more roles and one or more assignment conditions. Users with at least one assignment that matches the conditions qualify for the associated roles.

role provisioning
The automatic or manual allocation of a role to a user.

security profile
A set of criteria that identifies HCM objects of a single type for the purposes of securing access to those objects. The relevant HCM objects are persons, organizations, positions, countries, LDGs, document types, payrolls, and payroll flows.

security reference implementation
Predefined function and data security that includes role based access control, and policies that protect functions, and data. The reference implementation supports identity management, access provisioning, and security enforcement across the tools, data transformations, access methods, and the information life cycle of an enterprise.

work relationship
An association between a person and a legal employer, where the worker type determines whether the relationship is a nonworker, contingent worker, or employee work relationship.