Oracle Public Sector Licensing and Permitting

Implementing Security

22A

Oracle Public Sector Licensing and Permitting
Implementing Security

22A

Contents

ORACLE

Preface

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

Oracle Cloud Applications Guides

To find guides for Oracle Applications, go to the Oracle Help Center at *http://docs.oracle.com/*

Documentation Accessibility

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

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

ORACLE

1 Managing Users

Managing Users in Public Sector Licensing and Permitting

This topic provides an overview of the types of users and describes how users are created and managed within the Public Sector Licensing and Permitting offering.

Overview of User Types in Public Sector Licensing and Permitting

In the Public Sector Licensing and Permitting offerings, there are these types of users:

- Anonymous Users
- Registered Users

An anonymous user:

- Accesses the site, but either has not registered with the application, or they have not signed in.
- Could be an unregistered resident, a business owner, a contractor, and so on.
- Can perform a limited number of basic tasks, such as access the public landing page, view transaction types, use a GIS map, self-register, run specific reports, and so on.

> **Note:** You do not create anonymous users or assign roles to them. For any user who is not registered and signed in, the application automatically assigns them the anonymous user role and privileges. The anonymous user role is a Fusion Applications role, and can't be modified or cloned.

Registered users include:

- Registered public user.
- Agency staff member.

A registered public user:

- Could be a resident, a contractor, a business owner, and so on.
- Can access the registered user landing page, view their applications, apply for transaction types like permits, pay fees, manage their own user account, and so on.

An agency staff member:

- Could be a permit technician, plan reviewer, plan coordinator, building inspector, and so on.
- Can access the Agency Springboard, view assigned tasks, view all transaction types, plus they can access additional job-specific functions and data.

> **Note:** For the Public Sector Licensing and Permitting offering, you do not create users through the Security Console interface. You create them using the provided pages in the Public Sector Licensing and Permitting offering described in the following sections.

Creating Registered Public Users

When an unregistered user, clicks the Register button in the global header, and successfully completes the registration process, the application creates a user account for that user.

System administrators can define the information the anonymous user must provide during the registration process using the Public User Setup page.

For more information on the Public User Setup page, see *Setting Up Public Users*.

In addition to defining the options on the user registration page, system administrators can also define the roles that will automatically be assigned to the users upon registration using the Public User Roles page.

A registered public user would typically have a set of roles assigned to them, for example:

- The PSC Registered Public User abstract role to provide all the default access for a resident, contractor, and so on.

- The custom roles created during implementation to provide access to transactions, such as CUSTOM_PSC_MANAGE_PERMITS and CUSTOM_PSC_VIEW_PERMITS.

For more information on the Public User Roles page, see *Setting Up Public User Roles*.

For more information on the roles that need to be assigned to registered public users, see *Creating Custom Roles for Public Sector Licensing and Permitting*

Creating Agency Staff Users

The agency staff user is employed by the agency in the capacity of administering or processing transactions, such as permit applications, planning applications, and so on.

You create agency staff users on the Agency Staff page, where you can create and manage the agency staff profile.

For more information, on the Agency Staff page, see *Managing Agency Staff Profiles*.

An agency staff member would typically have a set of roles assigned to them. For example, the following list illustrates a minimum set of roles:
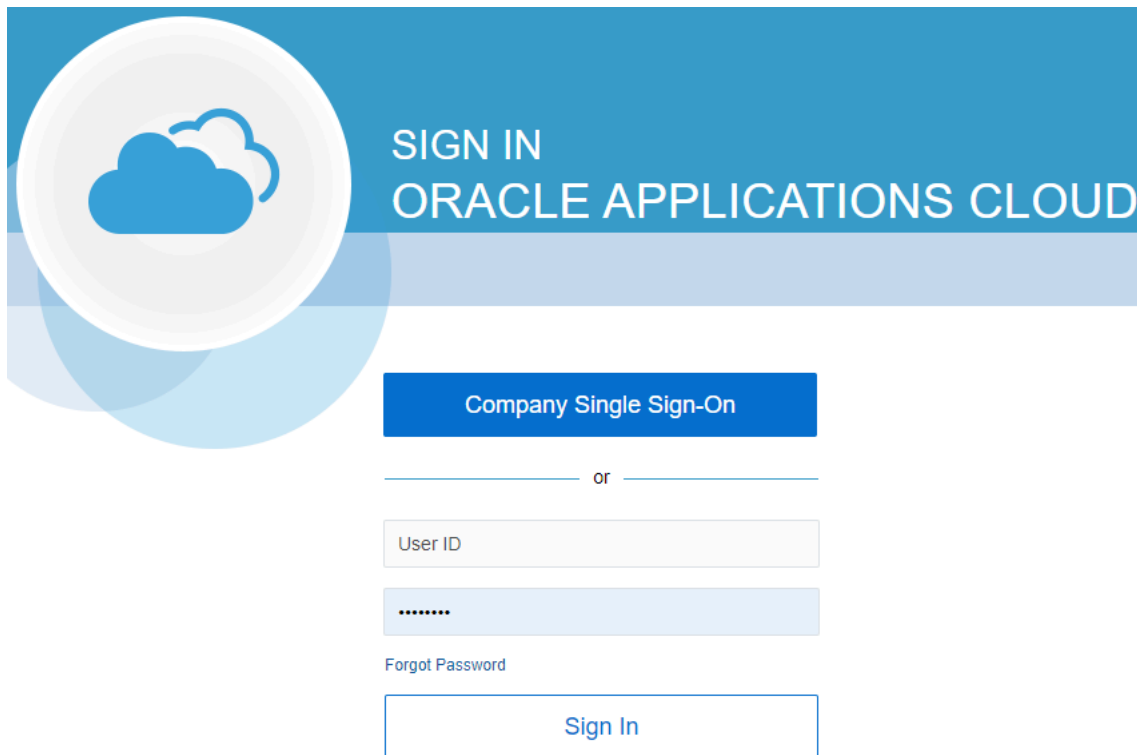
- The PSC Agency Staff abstract role to provide all the default access for an agency employee.

- At least one of the delivered job roles, such as PSC Permit Technician, to provide access to the functions and data required to complete job tasks.

- The custom roles created during implementation to provide access for job tasks, such as CUSTOM_PSC_MANAGE_PERMITS and CUSTOM_PSC_VIEW_PERMITS.

For more information on the roles that need to be assigned to various agency user types, see *Creating Custom Roles for Public Sector Licensing and Permitting*.

Signing In
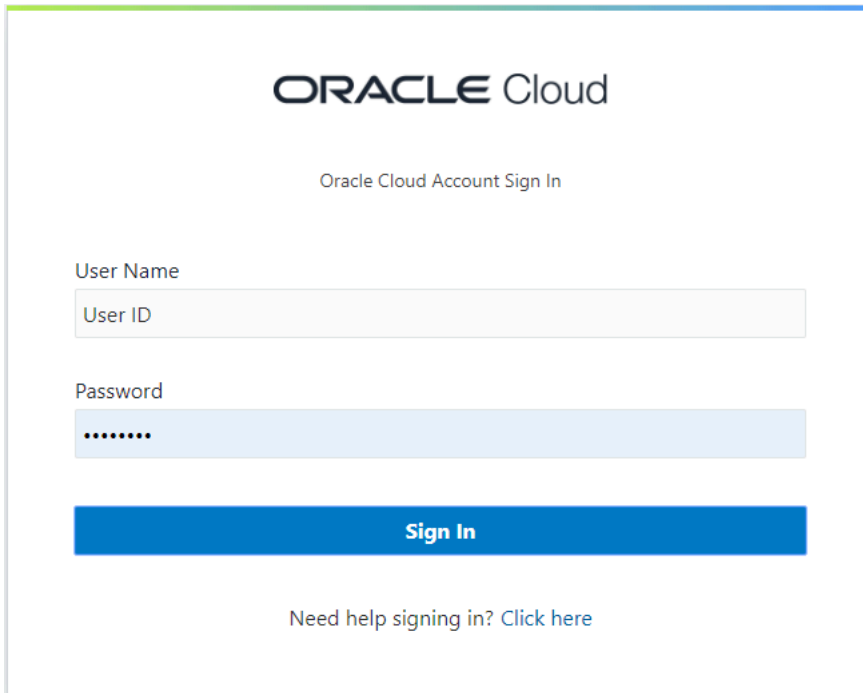
Depending on your identity provider platform, which could be Fusion or Oracle Identity Cloud Service (IDCS) the sign-in screen appears differently. You select your identity provider during licensing and implementation of the offering.

This example illustrates signing in using Fusion Security as your identity provider.

This example illustrates signing in using Oracle IDCS as your identity provider.

ORACLE Cloud

Oracle Cloud Account Sign In

User Name

User ID

Password

••••••••

Sign In

Need help signing in? Click here

This example illustrates the prompt an anonymous user receives if they attempt to perform an action that requires specific credentials, such as accessing an intake form. The anonymous user can choose to sign in using their user ID or register in the system to obtain a user ID.

Sign in with your registered user ID.

Sign In

If you are a new user, register and then sign in.

Register Now

If you are using Microsoft Active Directory to store user information, refer to *Oracle Applications Cloud:* Securing Applications, "Bridge for Microsoft Active Directory."

Note: While you can use Fusion or IDCS as your identity provider, IDCS must be used to integrate with Oracle Integration Cloud (OIC).

ORACLE

Setting the Next URL for the Default User Category

This topic describes how to set the Next URL property for the default user category so that the current user is directed to the Public Sector Compliance and Regulation offering after registering in the system and setting up user credentials and passwords.

This setup task only needs to be completed once for all users because all users are associated with the DEFAULT user category.

1. Navigate to the Security Console.
2. Select the **User Categories** tab.
3. Click the **DEFAULT** user category link.
4. On the DEFAULT User Category: Details page update the **Next URL** edit box to reflect the URL for your Oracle Public Sector Compliance and Regulation implementation.

   https://server.example.com/fscmUI/pscrAuthentication.html
5. Save your changes.

> **Note:** The URL entered using the previous steps, such as **https://server.example.com/fscmUI/pscrAuthentication.html** should only be used for setting the Next URL value. The URL that can be published for external public users is to access the service is: **https://server.example.com/fscmUI/publicSector.html** Users can bookmark the URL for accessing the Public Sector Licensing and Permitting homepage.

> **Note:** In some cases, an existing Oracle Fusion Applications customer may want employees to be redirected to the Fusion Applications homepage and may only want the public users to be redirected to Public Sector Licensing and Permitting homepage. In this case, you need to create a new user category for the public users and perform the steps above for the new category instead of for the DEFAULT user category. The new category you create would need to be referenced on the Public User Set Up page.

Setting Up Users for Oracle Mobile Applications

System administrators set up Oracle Inspector and Oracle Municipal Code Officer with profiles and security before they can implement the application on their mobile devices.

Before an inspector or agency staff member can install, configure, and use the mobile application, you must do the following:

- Create an agency staff profile for each user.

- Configure security for each user.

> **Tip:** If your agency is using Oracle Identity Cloud Service (IDCS) as your identity provider (IdP), you must send your field officers an email containing the *Mobile Application Activation* link from the Agency Mobile Setup page. For information on sending notifications, see *Managing Mobile Application Activation*.

ORACLE

> **Tip:** Oracle recommends that agencies implement mobile device management (MDM) software to protect employees' mobile devices from security threats, such as malware and theft.

Creating an Agency Staff Profile

Make sure that each user has an agency staff profile to log into the mobile application. Because the application package configuration is secure, agency staff must enter their login credentials before the environment begins to download.

For more information about creating agency staff profiles, see the documentation for *Managing Agency Staff Profiles*.

Configuring Security

Agency administrators must explicitly grant mobile application access to the necessary agency user roles. Users can open the application but need the proper credentials. Make sure the appropriate users have the following role assigned for the specific application they are using:

Mobile Application	Roles
Oracle Inspector	• ORA_PSC_BUILDING_INSPECTOR_JOB • ORA_PSC_INSPECTIONS_SUPERVISOR_JOB
Oracle Municipal Code Officer	ORA_PSC_CODE_ENFORCEMENT_OFFICER_JOB

For information about setting up roles, see the documentation for *Managing Roles in Public Sector Licensing and Permitting*.

Related Topics
- Mobile Applications Navigation Considerations

2 Managing Roles

Managing Roles in Public Sector Licensing and Permitting

This topic introduces roles that are used to implement security and the general Oracle Cloud security role types. It also highlights key roles and configuration considerations to keep in mind when implementing Public Sector Licensing and Permitting.

Role-Based Access Control

When you receive your Oracle Cloud application, access to its functionality and data is secured using the industry-standard framework for authorization, role-based access control. In a role-based access control model, users are assigned roles, and roles are assigned access privileges to protected resources. The relationship between users, roles, and privileges is shown in the following figure.

This diagram illustrates that users inherit privileges and security policy by way of roles assigned to them, which is described in the text that follows.
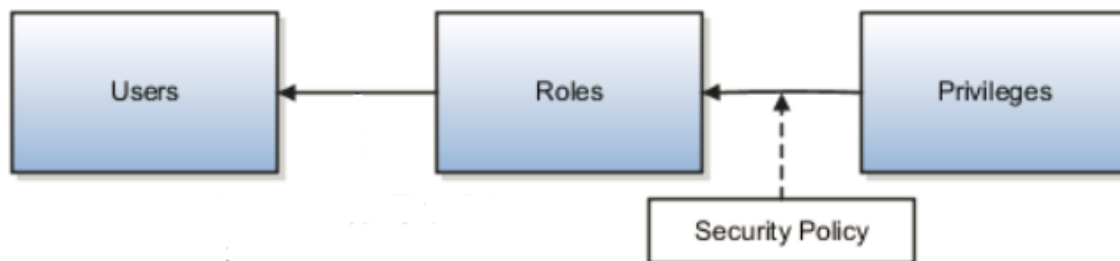
Users gain access to application data and functions when you assign them roles, which correspond to the job functions in your organization or the functions a pubic user in your municipality may perform.

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 Agency Staff role, the Permits Supervisor role, and the Permits Application Administrator role. In this case, the user has the following access:

- With the Agency Staff role, the user can access functions and data suitable for agency staff members.

- With the Permits Supervisor role, the user can access permits manager functions and data, and access and correct permit technician functions and data.

- With the Permits Application Administrator role, the user can access permit configuration settings and make necessary changes.

When the user logs into Oracle Cloud and is successfully authenticated, a user session is established and all the roles assigned to the user are loaded into the session repository. Oracle Cloud determines the set of privileges to application resources that are provided by the roles, then grants the user the most permissive level of access.

ORACLE

Role Types

Oracle Cloud defines the following types of roles:

Role Type	Description
Job Roles	Job roles represent the jobs that users perform in an organization. General Accountant and Accounts Receivables Manager are examples of predefined job roles. You can also create job roles.
Abstract Roles	Abstract roles represent people in the enterprise independently of the jobs they perform. Some predefined abstract roles in Oracle Applications Cloud include Employee and Transactional Business Intelligence Worker. You can also create abstract roles. All users are likely to have at least one abstract role that provides access to a set of standard functions. You may assign abstract roles directly to users.
Duty Roles	Duty roles represent a logical collection of privileges that grant access to tasks that someone performs as part of a job. Budget Review and Account Balance Review are examples of predefined duty roles. You can also create duty roles. Other characteristics of duty roles include: • They group multiple function security privileges. • They can inherit aggregate privileges and other duty roles. • You can copy and edit them. Job and abstract roles may inherit duty roles either directly or indirectly. You don't assign duty roles directly to users.
Aggregate Privileges	Aggregate privileges are roles that combine the functional privilege for an individual task or duty with the relevant data security policies. Functions that aggregate privileges might grant access to include task flows, application pages, work areas, dashboards, reports, batch programs, and so on. Aggregate privileges differ from duty roles in these ways: • All aggregate privileges are predefined. You can't create, modify, or copy them. • They don't inherit any type of roles. You can include the predefined aggregate privileges in your job and abstract roles. You assign aggregate privileges to these roles directly. You don't assign aggregate privileges directly to users.

Duty Role Elements

Functional security privileges and data security policies are granted to duty roles. Duty roles may also inherit aggregate privileges and other duty roles.

Elements	Description
Data Security Policies	For a given duty role, you may create any number of data security policies. Each policy selects a set of data required for the duty to be completed and actions that may be performed on that data. The duty role may also acquire data security policies indirectly from its aggregate privileges. Each data security policy combines: • A duty role, for example Expense Entry Duty.

ORACLE

Elements	Description
	• A business object that's being accessed, for example Expense Reports.
	• The condition, if any, that controls access to specific instances of the business object. For example, a condition may allow access to data applying to users for whom a manager is responsible.
	• A data security privilege, which defines what may be done with the specified data, for example Manage Expense Report.
Function Security Privileges	Many function security privileges are granted directly to a duty role. It also acquires function security privileges indirectly from its aggregate privileges.
	Each function security privilege secures the code resources that make up the relevant pages, such as the Manage Grades and Manage Locations pages.
	Tip: The predefined duty roles represent logical groupings of privileges that you may want to manage as a group. They also represent real-world groups of tasks. For example, the predefined General Accountant job role inherits the General Ledger Reporting duty role. To create your own General Accountant job role with no access to reporting structures, you could copy the predefined job role and remove the General Ledger Reporting duty role from the role hierarchy.

Aggregate Privileges

Aggregate privileges are a type of role. Each aggregate privilege combines a single function security privilege with related data security policies. All aggregate privileges are predefined. This topic describes how aggregate privileges are named and used.

- Aggregate Privilege Names

  An aggregate privilege takes its name from the function security privilege that it includes. For example, the Manage Accounts Payable Accounting Period Status aggregate privilege includes the Manage Accounting Period Status function security privilege.

- Aggregate Privileges in the Role Hierarchy

  Job roles and abstract roles inherit aggregate privileges directly. Duty roles may also inherit aggregate privileges. However, aggregate privileges can't inherit other roles of any type. As most function and data security in job and abstract roles is provided by aggregate privileges, the role hierarchy has few levels. This flat hierarchy is easy to manage.

- Use of Aggregate Privileges in Custom Roles

  You can include aggregate privileges in the role hierarchy of a custom role. Treat aggregate privileges as role building blocks.

- Creating, Editing, or Copying Aggregate Privileges

  You can't create, edit, or copy aggregate privileges, nor can you grant the privileges from an aggregate privilege to another role. The purpose of an aggregate privilege is to grant a function security privilege only in

ORACLE

combination with a specific data security policy. Therefore, you must use the aggregate privilege as a single entity.

If you copy a job or abstract role, then the source role's aggregate privileges are never copied. Instead, role membership is added automatically to the aggregate privilege for the copied role.

Understanding Role Hierarchies and Inheritance

Almost every role is a hierarchy or collection of other roles.

- Job and abstract roles inherit aggregate privileges. They may also inherit duty roles.

  In addition to aggregate privileges and duty roles, job and abstract roles are granted many function security privileges and data security policies directly. You can explore the complete structure of a job or abstract role in the Security Console.

- Duty roles can inherit other duty roles and aggregate privileges.

When you assign roles, users inherit all of the data and function security associated with those roles.

In Oracle Cloud, 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 duty roles and their associated privileges. Duty roles in turn can inherit privileges from subordinate duty roles. You can explore the complete structure of a job or abstract role on the Security Console.

This diagram illustrates the relationship between job roles, abstract roles, and duty roles, which is described in the text that follows.
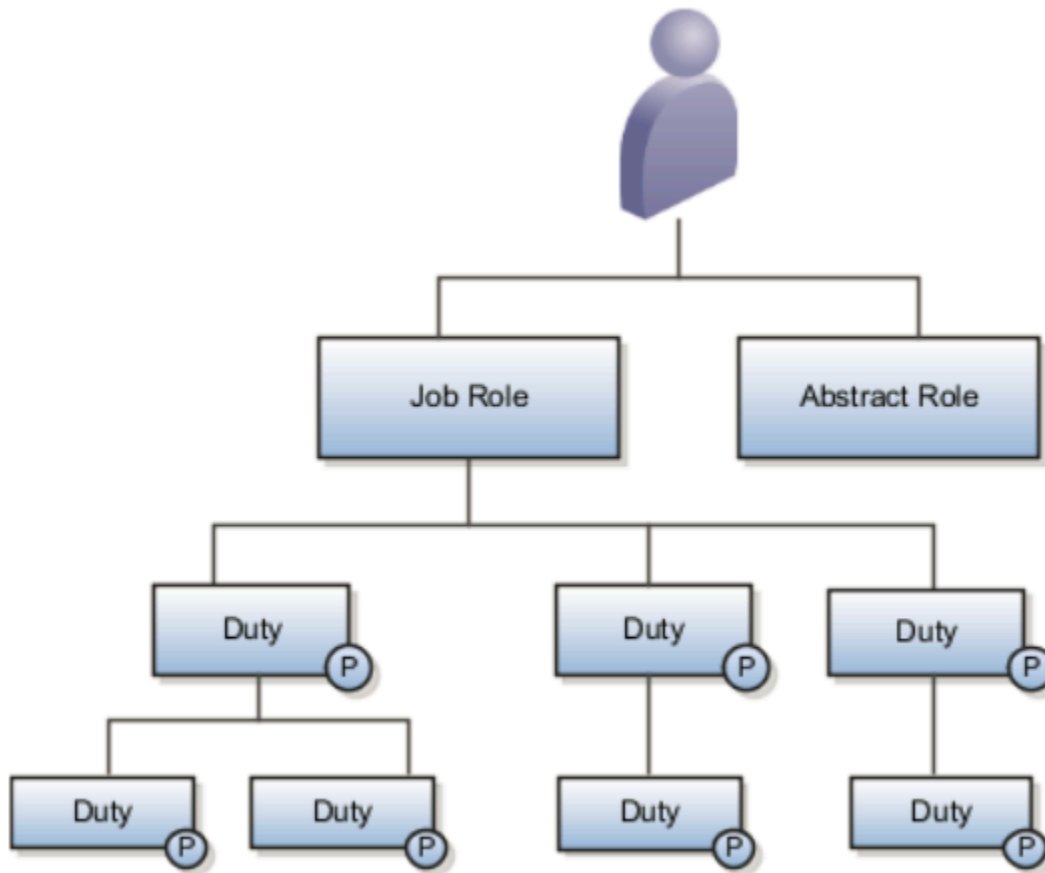
Role hierarchies allow privileges to be grouped to represent a feature set in Oracle Cloud, which simplifies feature management. Role hierarchies also provide privilege granularity and facilitate role reuse. For example, each role hierarchy beneath the job role represents a feature that is available 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 consequences in other features.

This diagram illustrates a scenario of a user's security roles and privileges and is described in the text that follows.

ORACLE
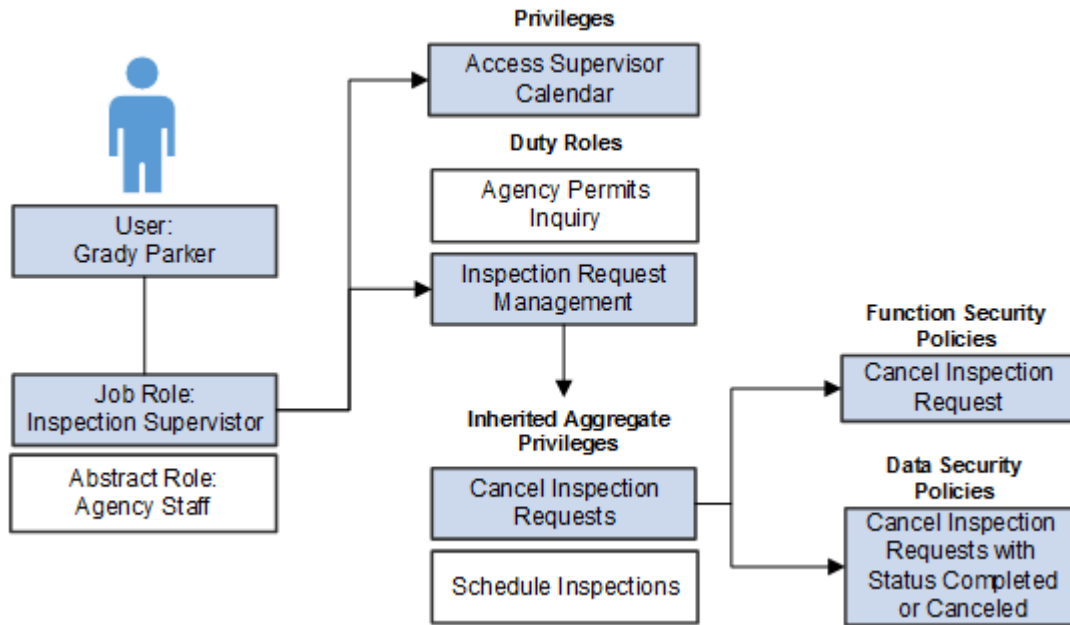
In the previous example, assume an inspection supervisor, Grady Parker.

- Because Grady is employed by the agency, he is assigned the Agency Staff abstract role, and at least one job role, which is in the is case Inspection Supervisor.

- Through the Inspection Supervisor job role, Grady inherits a set of duty roles, including the Inspection Request Management duty role. There is also a privilege unique to inspection supervisors, Access Supervisor Calendar, which is assigned directly to the job role.

- The Inspection Request Management duty role contains other duty roles as well as a set of inherited aggregate privileges, including Cancel Inspection Requests and Schedule Inspections.

- The Cancel Inspection Requests aggregate privilege is comprised of both a function security policy and data security policy.

Predefined Roles for Public Sector Licensing and Permitting

Public Sector Licensing and Permitting provides a set of predefined top-level roles that you can assign to users or clone to create additional roles. Oracle Cloud refers to the top-level roles in the system as *top roles,* because these are the roles at the top of the role hierarchy. Top roles can be job roles or abstract roles.

The following table lists a sample of the top roles in the Public Sector Licensing and Permitting offering.

Role	Role Type	Description
PSC Agency Staff	Abstract	Provides default privileges for any agency staff employee.
PSC Registered Public User	Abstract	Provides default privileges for any end user who has completed the self registration process.
PSC Building Inspector	Job	An agency staff position responsible for inspecting sites for permit approval.

Role	Role Type	Description
PSC Business Analyst	Job	A staff member that supports the agency in implementing and maintaining the applications.
PSC Cashier	Job	Responsible for the sale and record keeping for various licenses and permits.
PSC Chief Building Officer	Job	Manages a staff of permit technicians and inspectors. Oversees that the staff processes permits expeditiously and accurately and that all fees are collected and accounted.
PSC Economic Development Officer	Job	Maintains various ledgers, registers, and journals according to established account classifications. Audits fees against department activity, researches discrepancies, and performs accounting clerical work.
PSC Finance Administrator	Job	Reviews all incoming permit applications for accuracy and checks for any needed supporting documentation. Reviews the checklist to determine if they need further review or routing to other departments.
PSC Geographical Information System Administrator	Job	Uses Geographical Information System software and related programs for provision of maps, charts, graphs, and other related information for visual displays, presentations or reports.
PSC Inspections Supervisor	Job	Manages the workflow and staff to get through inspection jobs everyday. Keeps track of inspectors, districts and workload.
PSC Permit Technician	Job	Performs permit technician duties, which includes processing applications, fee assessments, fee collections, documents, standardization, and permit issuance.
PSC Permits Application Administrator	Job	An agency staff position that oversees the permit application.
PSC Permits Supervisor	Job	Manages the workflow and staff to ensure that the permit applications are assigned and processed by the permit technicians.
PSC Plan Reviewer	Job	Reviews plans for development, modification, alteration and demolition of commercial and residential properties. Checks compliance with applicable state and local zoning and building codes and related regulations. Calculates fees required for issuance of permits.

ORACLE

Role	Role Type	Description
PSC Planning Coordinator	Job	Coordinates plan review, permitting, and inspection of private construction projects in accordance with municipal ordinances and adopted building codes and code enforcement.
PSC Principal Planner	Job	Reviews construction plans for compliance with all state and local development and zoning codes, regulations, and requirements.
PSC System Administrator	Job	An agency staff position that has all access to configuration settings, security settings, and is able to access and solve issues for other users.
PSC Zoning Administrator	Job	Responsible for administering and enforcing the Planning Code. Provides written interpretations and clarifications of the Planning Code. Advises the Planning Director on amendments to the Planning Code. Monitors and maintains data related to the ongoing implementation of the Planning Code. Manages planners to ensure Planning and Zoning Code compliance.
PSC Associate Planner	Job	Prepares assessments on projects submitted for approval. Assists in the evaluation of projects submitted. Checks plans for zoning compliance.
PSC Principal Planner	Job	Reviews construction plans for compliance with all state and local development and zoning codes, regulations, and requirements.
PSC Planning Assistant	Job	Performs planning work involving the research, organization, and graphic presentation of zoning and planning data. Assists planners in compiling data, and assembling and distributing packets for board meetings.
PSC Planning and Zoning Application Administrator	Job	Administers, manages, configures the Planning and Zoning offering.
PSC Code Enforcement Application Administrator	Job	An agency staff position that oversees the Code Enforcement application.
PSC Code Enforcement Officer	Job	Enforces municipal code, follows the route to assigned cases, records notes and statuses, issues citations, records cases in the field if violations are found, researches history of address, parcel, owner, and past violations.
PSC Code Enforcement Supervisor	Job	Supervises, assigns, reviews, and participates in the operations and activities of an agency code

Role	Role Type	Description
		enforcement program, including implementing activities related to setting and ensuring compliance with applicable ordinances, codes, and related regulations. The Supervisor ensures work quality and adherence to established policies and procedures, performs the more technical and complex tasks relative to assigned area of responsibility, and conducts field inspections and participates in hearings.
PSC Code Enforcement Technician	Job	Serves as a gatekeeper for all code enforcement incidents, assigns inspections to code officers, responds to direct communications, manages noticing procedures, and supports escalations where necessary.
PSC Auditor	Job	Responsible for developing, planning, implementing, and directing the city's comprehensive audit programs in order to evaluate the adequacy of the design and effectiveness of internal controls and the management of business risks within all departments. Works with management to assist in ensuring fiscal integrity of operational and financial assets in accordance with policies, procedures, and applicable laws and regulations.
PSC Business License Manager	Job	Administers the business licensing program. Prepares annual business license bills. Prints and mails licensing bills for registered businesses, responds to inquiries from business owners and the general public, researches and resolves problem situations. Administers and enforces the provisions of the Alcohol Beverage Ordinance. Acts as a liaison between departments regarding privileged license information.
PSC Business License Specialist	Job	Assists the public with general information as well as in completing required licensing forms, provides information to the public pertaining to licensing of businesses, and creates and maintains information sheets and other documentation for distribution to the public concerning business licenses.
PSC Treasury Administrator	Job	Plans, develops, administers, and supervises the city's revenue collection and cash handling activities, including the collection and counting of revenues. Supervises, assigns, and reviews the work of supervisory, lead, technical, and clerical support staff.
PSC Treasury Supervisor	Job	Responsible for managing the cash position of the city, which includes overseeing the city's revenue collection processes and procedures,

Role	Role Type	Description
		ensuring daily liquidity and cash position, overseeing cash management services including bank accounts and banking products, account analysis, and armored car services.

The remainder of the delivered roles are lower-level child roles that group privileges and link privileges to the top-level roles.

Key Duty Roles in Public Sector Licensing and Permitting

The following table highlights a set of key duty roles to illustrate some delivered, predefined duty roles.

Duty Role	Description
PSC Apply Permit	Provides all the access required for an applicant, such as being able to access a permit, fill in and submit a permit application, add comments to the permit during the application process, and so on.
PSC Agency Permits Inquiry	Provides the read only access for the agency staff members so that they can review and process permit applications.
PSC Anonymous Permit Application Inquiry	Provides read-only access for viewing a permit application. **Note:** Oracle Fusion Applications do not allow modification of any anonymous roles.
PSC Apply Planning Application	Provides all the access required for an applicant, such as being able to access a planning application, fill in and submit a planning application, add comments to the planning application during the application process, and so on.
PSC Agency Planning Application Inquiry	Provides the read only access for the agency staff members so that they can review and process applications.
PSC Anonymous Planning Application Inquiry	Provides read-only access for viewing a planning application. **Note:** Oracle Fusion Applications do not allow modification of any anonymous roles.
PSC Report Code Enforcement Issue Duty	Provides all the access required for reporting an issue for Code Enforcement, such as being able to access issue subtype, fill in and submit an issue intake form, add comments to the report during the process, and so on.
PSC Agency Code Enforcement Case Inquiry	Provides the read only access for the agency staff members so that they can review and process cases.

ORACLE

Duty Role	Description
PSC Agency Code Enforcement Incident Inquiry	Provides the read only access for the agency staff members so that they can review and process incidents.
PSC Anonymous Code Enforcement Incident Inquiry	Provides the read only access for anonymous users so that they can review reported incidents.
PSC Agency Business Consultation Inquiry	Provides the read only access for the agency staff members so that they can review and process business license consultations.
PSC Agency Business License Inquiry	Provides the read only access for the agency staff members so that they can review and process business licenses.
PSC Anonymous Business License Inquiry	Provides the read only access for anonymous users so that they can review business licenses.
PSC Business Entity Inquiry	Allows users to view business entities.
PSC Apply Business License	Allows users to apply for business licenses.
PSC Business License Application Administrator	Enables the administration of the Business Licenses offering.

Note: For the Business Licenses offering, PSC Access Confidential Business License Information is a key aggregate privilege. It allows users to access confidential information in business licenses. It also adds access to certain confidential tabs in the business license details, such as attachments. Confidential information in an intake form is defined in the Intake Form Designer.

Working with Aggregate Privileges in Public Sector Licensing and Permitting

All aggregate privileges are predefined. Aggregate privileges combine a single functional security privilege with related data security policies.

In many cases with roles in the Public Sector Licensing and Permitting Cloud, you see a pattern, where one aggregate role provides the general, default behavior, such as allowing a user to insert comments and update only their own comments. Then there is a counterpart aggregate role that would provide more far reaching privileges, such as updating the comments for others.

For example, consider these aggregate roles:

- PSC Update Inspection Comments added by self
- PSC Update Inspection Attachments added by self
- PSC Update Inspection Comments added by others and self
- PSC Update Inspection Attachments added by others and self

ORACLE

For example, with the comments and attachments, most roles provide you with the ability to add comments or attachments and update comments or attachments inserted by yourself. However, by assigning to the user another aggregate role (with the phrase "by others and self" in the role title), that user could update comments or attachments added by others. A supervisor in the permit processing department could update comments in a permit added by one of their permit technicians if they have the following role assigned to their user account: *PSC Update Inspection Comments added by others and self.*

By default, the "by others and self" aggregate privileges are assigned only to system administrators.

Modifying Delivered Roles

| **CAUTION:** If you find you want to update a delivered role, it is not recommended to modify the role itself.

If the delivered top roles do not meet your business requirements, you can create custom roles by cloning a delivered job or abstract role, and then modifying the custom role as needed. When cloning a role, this also copies the role hierarchy, which you can modify as needed by either adding or removing elements of the hierarchy.

When creating custom roles, it is highly recommended to modify a role's access through aggregate privileges, rather than attempting to modify a job, abstract, or duty role manually. Modifying access using aggregate privileges is efficient and a more robust approach. Keep in mind that aggregate privileges contain both the functional security and the data security policy for an action. By adding or removing an aggregate privilege, you make one change, but adjust both aspects of security simultaneously.

If you update a duty role manually, you will need to always make sure you've added or removed the functional and data security counterparts. Otherwise, you may not be providing or restricting the access you intend, while in other cases, you may be creating security holes, unintentionally.

Related Topics
- Working with Roles in the Security Console

Managing Data Security Policies

This topic provides an overview of data security and discusses concepts related to how you secure data by provisioning roles that provide the necessary access.

Comparing Function Security and Data Security

Function security is a statement of what actions you can perform in which user interface pages.

Data security is a statement of what action can be taken against which data.

Function security controls access to user interfaces and actions needed to perform the tasks of a job. For example, an accounts payable manager can view invoices. The Accounts Payable Manager role provisioned to the accounts payable manager authorizes access the functions required to view invoices.

Data security controls access to data. In this example, the accounts payable manager for the North American Commercial Operation can view invoices in the North American Business Unit. Since invoices are secured objects, and a data role template exists for limiting the Accounts Payable Manager role to the business unit for which the provisioned user is authorized, a data role inherits the job role to limit access to those invoices that are in the North American

ORACLE

Business Unit. Objects not secured explicitly with a data role are secured implicitly by the data security policies of the job role.

Both function and data are secured through role-based access control.

Implementing Data Security

By default, users are denied access to all data.

Data security makes data available to users by the following means.

- Policies that define grants available through provisioned roles

- Policies defined in application code

You secure data by provisioning roles that provide the necessary access.

> **Note:** Public Sector Compliance and Regulation does not employ the use of data roles.

When you provision a job role to a user, the job role limits data access based on the data security policies of the inherited duty roles. When you provision a data role to a user, the data role limits the data access of the inherited job role to a dimension of data.

Data security consists of privileges conditionally granted to a role and used to control access to the data. A privilege is a single, real world action on a single business object. A data security policy is a grant of a set of privileges to a principal on an object or attribute group for a given condition. A grant authorizes a role, the grantee, to actions on a set of database resources. A database resource is an object, object instance, or object instance set. An entitlement is one or more allowable actions applied to a set of database resources.

Data security features include:

- Data security policy: Defines the conditions in which access to data is granted to a role.

- Role: Applies data security policies with conditions to users through role provisioning.

The sets of data that a user can access are defined by creating and provisioning roles. Oracle data security integrates with Oracle Platform Security Services (OPSS) to entitle users or roles (which are stored externally) with access to data. Users are granted access through the privilege assigned to the roles or role hierarchy with which the user is provisioned. Conditions are WHERE clauses that specify access within a particular dimension, such as by business unit to which the user is authorized.

Data Security Policies

Data security policies articulate the security requirement "Who can do what on which set of data."

For example, accounts payable managers can view AP disbursements for their business unit.

A data security policy is a statement in a natural language, such as English, that typically defines the grant by which a role secures business objects. The grant records the following.

- Table or view

- Entitlement (actions expressed by privileges)

- Instance set (data identified by the condition)

ORACLE

For example, disbursement is a business object that an accounts payable manager can manage by payment function for any employee expenses in the payment process.

> **Note:** Some data security policies are not defined as grants but directly in applications code. The security reference manuals for Oracle Fusion Applications offerings differentiate between data security policies that define a grant and data security policies defined in Oracle Fusion applications code.

A data security policy identifies the entitlement (the actions that can be made on logical business objects or dashboards), the roles that can perform those actions, and the conditions that limit access. Conditions are readable WHERE clauses. The WHERE clause is defined in the data as an instance set and this is then referenced on a grant that also records the table name and required entitlement.

Working with Database Resources and Data Security Policies

A data security policy applies a condition and allowable actions to a database resource for a role. When that role is provisioned to a user, the user has access to data defined by the policy. In the case of the predefined security reference implementation, this role is always a duty role.

The database resource defines an instance of a data object. The data object is a table, view, or flexfield.

The following figure shows the database resource definition as the means by which a data security policy secures a data object. The database resource names the data object. The data security policy grants to a role access to that database resource based on the policy's action and condition.

ORACLE
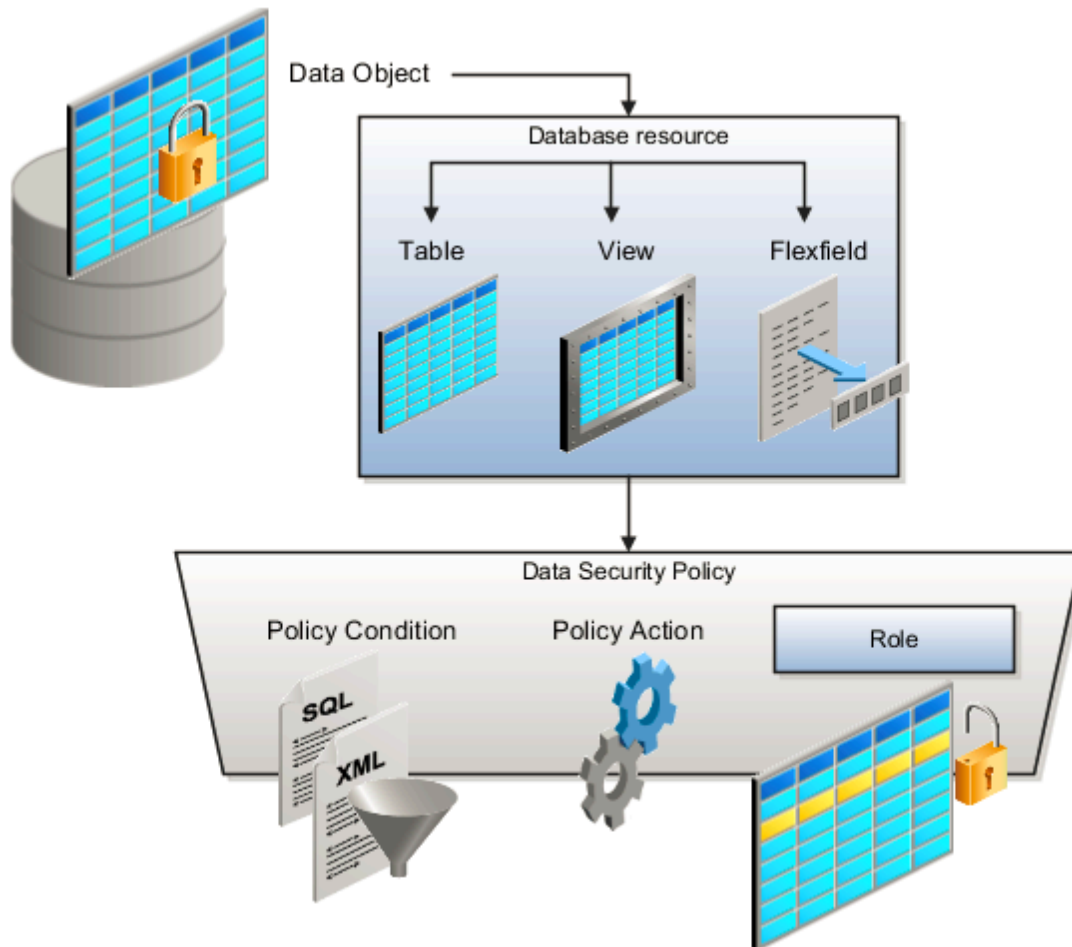
A database resource specifies access to a table, view, or flexfield that is secured by a data security policy.

- Name providing a means of identifying the database resource
- Data object to which the database resource points

Note: If the data security policy needs to be less restrictive than any available database resource for a data object, define a new data security policy.

Actions correspond to privileges that entitle kinds of access to objects, such as view, edit, or delete. The actions allowed by a data security policy include all or a subset of the actions that exist for the database resource.

A condition is either a SQL predicate or an XML filter. A condition expresses the values in the data object by a search operator or a relationship in a tree hierarchy. A SQL predicate, unlike an XML filter, is entered in a text field in the data security user interface pages and supports more complex filtering than an XML filter, such as nesting of conditions or sub queries. An XML filter, unlike a SQL predicate, is assembled from choices in the UI pages as an AND statement.

Note: An XML filter can be effective in downstream processes such as business intelligence metrics. A SQL predicate cannot be used in downstream metrics.

ORACLE

Creating Custom Roles for Public Sector Licensing and Permitting

This topic describes how to create custom roles required to enable design-time and runtime access for various features of Public Sector Licensing and Permitting offerings. These custom roles are *required.* They are not delivered, predefined roles. They *must* be created during implementation.

Creating Custom Roles Overview

In this task the following roles are created by the automated security setup process launched from Functional Setup Manager. The roles created depend on the offering you are implementing.

After the roles are created, you can then assign them to users (agency or public users) as described in the section, "Assigning Roles."

> **Note:** The Role Category for Public Sector Licensing and Permitting roles is *Financials - Job Roles.*

Running the Public Sector Security Setup Job to Create Custom Roles

You create the required custom security roles for your offering by completing the Run Public Sector Security Setup Process in the Initial Setup Functional Area of your offering in the Functional Setup Manager.

To create Public Sector Licensing and Permitting custom roles:

1. Access Functional Setup Manager.
2. Select your offering in the Setup drop-down list.
3. Select the *Initial Setup* functional area.
4. Click the Run Public Sector Security Setup Process task.

   The page displayed enables you to launch an Oracle Enterprise Scheduler (ESS) process.
5. (Optional) Use the **Process Options** and **Advanced** buttons to set any desired settings.
6. Click **Submit.**

> **Note:** The Public Sector Security Setup Job should be run with each upgrade of your pod as well as making sure you have managed users roles as per the descriptions in this topic.

The following sections describe the roles required per offering and to which users they need to be assigned.

Creating a Custom Role to Enable Sandbox Testing

In some cases, such as the PSC Custom Sandbox Access role, you need to create the role manually in the Security Console.

> **Note:** This process should not be completed in a production environment. It is only intended for testing and development environments.

ORACLE

To create PSC Custom Sandbox Access role manually:

1. Open the Security Console, select the Roles tab, and click **Create Role**.
2. Create role with these attribute values:

Page Element	Value
Role Name	*PSC Custom Sandbox Access*
Role Code	*CUSTOM_SANDBOX_ACCESS*
Role Category	*Financials - Job Roles*

3. On the Function Security Policies tab, add the Administer Sandbox (FND_ADMINISTER_SANDBOX_PRIV) privilege.
4. On the Role Hierarchy tab, add the PSC Access Sandboxes (ORA_PSC_ACCESS_SANDBOXES) duty role.
5. Add the role to relevant user IDs you will use for testing intake forms.

User Type	Configuration
Public Registered User	Create or modify the user with the Manage Public Users page and then assign the CUSTOM_SANDBOX_ACCESS role.
Agency User	Create or modify the user on the Agency Staff page, providing all relevant job functions and attributes. Use the Agency Staff Access page and assign the CUSTOM_SANDBOX_ACCESS role in addition to the prescribed list of roles.

Common Custom Roles

Role Code	Role Name	Description
CUSTOM_PSC_REGISTERED_PUBLIC_USER	PSC Custom Registered Public User	Groups all the registered public user access privileges. This role requires the following child roles, depending on your offering. For Permits: • CUSTOM_PSC_MANAGE_PERMITS • CUSTOM_PSC_VIEW_PERMITS • CUSTOM_PSC_APPLY_PERMITS_DATA

ORACLE

Role Code	Role Name	Description
		Note: Before contacts can manage attachments, comments, contacts, and inspections for their permits, you must add the PSC Contact User (ORA_PSC_CONTACT_USER_DUTY) duty role to CUSTOM_PSC_REGISTERED_ PUBLIC_USER on the Role Hierarchy page in the Security Console and enable permit access on the Contact Type page. For Planning and Zoning: • CUSTOM_PSC_MANAGE_PNZ • CUSTOM_PSC_VIEW_PNZ • CUSTOM_PSC_APPLY_PNZ_DATA For Code Enforcement: CUSTOM_PSC_ CREATE_CE_INCIDENT For Business Licenses: CUSTOM_PSC_APPLY_ BL
CUSTOM_PSC_VIEW_ALL_APPLICATIONS	PSC View All Applications	Allows view access to all custom objects to agency staff. This role requires these child roles: • CUSTOM_PSC_VIEW_PERMITS • CUSTOM_PSC_VIEW_PNZ
CUSTOM_PSCR_OIC_PROXY_USER	PSCR Proxy User for OIC	Allows the Oracle Integration Cloud (OIC) system to connect to Public Sector Licensing and Permitting to exchange data during transaction processing. **Note:** This role should not be assigned to any user other than the PSCR OIC Proxy User. This role requires these delivered child roles: • ORA_PSC_UPDATE_PERMIT_STATUS_ ALL_AGG • ORA_PSC_VIEW_PLANNER_AGG • ORA_PSC_UPDATE_PNZ_STATUS_ALL_ AGG • ORA_PSC_VIEW_BL_SPECIALIST_ ASSIGNMENT_AGG • ORA_PSC_UPDATE_BUSINESS_LICENSE_ STATUS_ALL_AGG • ORA_PSC_PLAN_COORDINATOR_JOB

Role Code	Role Name	Description
		• ORA_PSC_BUSINESS_LICENSE_ ADMINISTRATOR • ORA_PSC_OIC_PCS_USER This role requires these custom child roles: • CUSTOM_PSC_MANAGE_PERMITS • CUSTOM_PSC_MANAGE_PERMITS_ AGENCY • CUSTOM_PSC_MANAGE_PNZ • CUSTOM_PSC_MANAGE_PNZ_AGENCY • CUSTOM_PSC_MANAGE_BL_ADMIN
CUSTOM_SANDBOX_ACCESS **Note:** This role must be created manually in the Security Console.	PSC Custom Sandbox Access	

Permits Custom Roles

Role Code	Role Name	Description
CUSTOM_PSC_MANAGE_PERMITS	PSC Custom Manage Permits	Allows users to apply for permits and update permits.
CUSTOM_PSC_VIEW_PERMITS	PSC Custom View Permits	Allows users to view the permit detail tab in the permits application.
CUSTOM_PSC_APPLY_PERMITS_DATA	PSC Custom Permit Applicant Data Access	Allows users to apply for permits and update their own permits in while in the status of pending.
CUSTOM_PSC_MANAGE_PERMITS_AGENCY	PSC Custom Permit Data Access for Agency	Allows users to apply for permits and update permits that have not been closed. This role requires these child roles: • CUSTOM_PSC_MANAGE_PERMITS • CUSTOM_PSC_VIEW_PERMITS

ORACLE

Planning and Zoning Custom Roles

Role Code	Role Name	Description
CUSTOM_PSC_MANAGE_PNZ	PSC Custom Manage Planning and Zoning Applications	Allows users to apply for Planning and Zoning applications.
CUSTOM_PSC_VIEW_PNZ	PSC Custom View Planning and Zoning Applications	Allows users to view Planning and Zoning applications.
CUSTOM_PSC_APPLY_PNZ_DATA	PSC Custom Planning and Zoning Applications Applicant Data Access	Allows users to apply for Planning and Zoning applications and update their own Planning and Zoning applications in pending status.
CUSTOM_PSC_MANAGE_PNZ_AGENCY	PSC Custom Planning and Zoning Applications Data Access for Agency	Allows users to apply for Planning and Zoning applications and update Planning and Zoning applications that are not closed. While creating the CUSTOM_PSC_MANAGE_ PNZ_AGENCY role, add the following roles as child roles on the Role Hierarchy tab: • CUSTOM_PSC_MANAGE_PNZ • CUSTOM_PSC_VIEW_PNZ

Code Enforcement Custom Roles

Role Code	Role Name	Description
CUSTOM_PSC_CREATE_CE_INCIDENT	PSC Custom Create Code Enforcement Incidents	Allows users to create incidents.
CUSTOM_PSC_CREATE_CE_CASE	PSC Custom Create Code Enforcement Cases	Allows users to create cases.
CUSTOM_PSC_MANAGE_CE_AGENCY	PSC Custom Manage Incidents and Cases as CE Agency User	Allows agency users to manage cases and incidents. This role requires these child roles: • CUSTOM_PSC_CREATE_CE_INCIDENT • CUSTOM_PSC_CREATE_CE_CASE
CUSTOM_PSC_MANAGE_CE_ADMIN	PSC Custom Manage Incidents and Cases as CE Agency Admin	For system administration purposes for managing cases and incidents. This role requires these child roles: • CUSTOM_PSC_CREATE_CE_INCIDENT • CUSTOM_PSC_CREATE_CE_CASE

ORACLE

Role Code	Role Name	Description
		This role requires these functional security privileges: • FND_ADMINISTER_SANDBOX_PRIV • ZCX_MANAGE_EXTENSIBLE_OBJECT_PRIV

Business Licenses Custom Roles

Role Code	Role Name	Description
CUSTOM_PSC_VIEW_BL	PSC Custom View Business Licenses	Allows users to view business licenses.
CUSTOM_PSC_APPLY_BL	PSC Custom Apply Business Licenses	Allows users to apply for business licenses.
CUSTOM_PSC_MANAGE_BL_AGENCY	PSC Custom Manage Business License Applications as Agency Users	Allows agency users to manage business licenses.
CUSTOM_PSC_MANAGE_BL_ADMIN	PSC Custom Manage Business License Applications as Admin Users	For system administration purposes for managing business licenses.

Assigning Roles

You assign roles to users in the system using delivered setup pages. For public users, you use the Public User Roles page and for agency staff members, you use the Agency Staff Access page.

User Type	Role Assignments	Setup Page
Anonymous User	This is the default access available to all users, including users who have not signed in. You do not assign roles to this user type.	None.
Registered Public User	CUSTOM_PSC_REGISTERED_PUBLIC_USER	Public User Roles page
System Administrator	• PSC Agency Staff • PSC System Administrator • CUSTOM_PSC_MANAGE_PERMITS_AGENCY • CUSTOM_PSC_MANAGE_PNZ_AGENCY • CUSTOM_PSC_MANAGE_CE_ADMIN • CUSTOM_PSC_MANAGE_BL_ADMIN • IT Security Manager	• Create the user with the Agency Staff page. • Add roles using the Agency Staff Access page.

User Type	Role Assignments	Setup Page
	• Application Implementation Consultant • Custom Objects Administration (This role will be available for assignment only after the first transaction type is created.)	
Business Analyst	• PSC Agency Staff • PSC Business Analyst • CUSTOM_PSC_MANAGE_PERMITS_AGENCY • CUSTOM_PSC_MANAGE_PNZ_AGENCY • CUSTOM_PSC_MANAGE_CE_ADMIN • CUSTOM_PSC_MANAGE_BL_ADMIN • IT Security Manager • Application Implementation Consultant • Custom Objects Administration (This role will be available for assignment only after the first transaction type is created.)	• Create the user with the Agency Staff page. • Add roles using the Agency Staff Access page.
Branding Administrator	• PSC Agency Staff • PSC System Administrator • CUSTOM_PSC_MANAGE_PERMITS_AGENCY • CUSTOM_PSC_MANAGE_PNZ_AGENCY • CUSTOM_PSC_MANAGE_CE_ADMIN • CUSTOM_PSC_MANAGE_BL_ADMIN • PSC Registered Public User • IT Security Manager • Application Implementation Consultant • Custom Objects Administration (This role will be available for assignment only after the first transaction type is created.)	• Create the user with the Agency Staff page. • Add roles using the Agency Staff Access page. **Note:** Typically, it is not recommended to assign PSC Registered Public User to any of the agency staff users, including the administrators. This user configuration should be used only for completing branding activities, such as updating themes and menu navigation. If the same user is required to perform any of the other related transactions or setup, then the PSC Registered Public User role should be removed from the user.
Permits agency staff members: • PSC Permit Technician • PSC Permits Supervisor • PSC Plan Reviewer • PSC Planning Coordinator • PSC Building Inspector • PSC Inspections Supervisor • PSC Chief Building Officer	• PSC Agency Staff • CUSTOM_PSC_MANAGE_PERMITS_AGENCY • CUSTOM_PSC_VIEW_ALL_APPLICATIONS • CUSTOM_PSC_VIEW_BL • <Specific Job Role> (such as PSC Permit Technician, PSC Plan Reviewer, and so on)	• Create the user with the Agency Staff page. • Add roles using the Agency Staff Access page.
Planning and Zoning agency staff members:	• PSC Agency Staff • CUSTOM_PSC_MANAGE_PNZ_AGENCY	• Create the user with the Agency Staff page.

ORACLE

User Type	Role Assignments	Setup Page
• PSC Associate Planner • PSC Planning Assistant • PSC Zoning Administrator	• CUSTOM_PSC_VIEW_ALL_APPLICATIONS • CUSTOM_PSC_VIEW_BL • <Specific Job Role> (such as PSC Associate Planner, PSC Planning Assistant, PSC Zoning Administrator, and so on)	• Add roles using the Agency Staff Access page.
Code Enforcement agency staff members: • PSC Code Enforcement Technician • PSC Code Enforcement Officer • PSC Code Enforcement Supervisor	• PSC Agency Staff • CUSTOM_PSC_MANAGE_CE_AGENCY • CUSTOM_PSC_VIEW_ALL_APPLICATIONS • CUSTOM_PSC_VIEW_BL • <Specific Job Role> (such as PSC Code Enforcement Technician, PSC Code Enforcement Officer, PSC Code Enforcement Supervisor and so on)	• Create the user with the Agency Staff page. • Add roles using the Agency Staff Access page.
Code Enforcement Administrator (PSC Code Enforcement Application Admin)	• PSC Agency Staff • CUSTOM_PSC_MANAGE_CE_ADMIN • CUSTOM_PSC_VIEW_ALL_APPLICATIONS • PSC Code Enforcement Application Administrator • CUSTOM_PSC_VIEW_BL • Application Implementation Consultant • IT Security Manager	• Create the user with the Agency Staff page. • Add roles using the Agency Staff Access page.

Business License agency staff members:
 	
• PSC Business License Specialist
• PSC Business License Manager
	• PSC Agency Staff
	• CUSTOM_PSC_VIEW_ALL_APPLICATIONS
	• CUSTOM_PSC_MANAGE_BL_AGENCY
	• <Specific Job Role> (such as PSC Business License Specialist, PSC Business License Manager, and so on)
		1. Create a new Financial Job role: CUSTOM_PSC_BL_BA using security console.
		2. On the Function Security Policies tab, add these privileges:
		  o FND_ADMINISTER_SANDBOX
		  o ZCX_MANAGE_EXTENSIBLE_OBJECT_PRIV
		3. In its Role Hierarchy add these duty roles:
		  o ORA_PSC_BUSINESS_LICENSE_ADMINISTRATOR
		  o ORA_PSC_BUSINESS_LICENSE_ADMINISTRATOR_OBI
		4. Create the user with the Agency Staff page.
		5. Add roles using the Agency Staff Access page.

Business License Administrator (PSC Business License Application Administrator (Duty Role))	• PSC Agency Staff • CUSTOM_PSC_VIEW_ALL_APPLICATIONS • CUSTOM_PSC_BL_ADMIN	1. Create a new Financial Job role: CUSTOM_PSC_BL_ADMIN using the Security Console.

ORACLE

User Type	Role Assignments	Setup Page
	• CUSTOM_PSC_MANAGE_BL_ADMIN • IT Security Manager	2. On the Function Security Policies tab, add these privileges: ○ FND_ADMINISTER_SANDBOX ○ ZCX_MANAGE_EXTENSIBLE_OBJECT_ PRIV 3. On the Role Hierarchy add these duty roles: ○ ORA_PSC_BUSINESS_LICENSE_ ADMINISTRATOR ○ ORA_PSC_BUSINESS_LICENSE_ ADMINISTRATOR_OBI 4. Create the user with the Agency Staff page. 5. Add roles using the Agency Staff Access page.
Common Users: • PSC Cashier • PSC Economic Development Officer • PSC Finance Administrator • PSC Geographical Information System Administrator • PSC Auditor • PSC Treasury Supervisor • PSC Treasury Administrator	• PSC Agency Staff • CUSTOM_PSC_VIEW_ALL_APPLICATIONS • CUSTOM_PSC_VIEW_BL Specific Job Role: ○ PSC Cashier ○ PSC Economic Development Officer ○ PSC Finance Administrator ○ PSC Geographical Information System Administrator ○ PSC Auditor ○ PSC Treasury Supervisor ○ PSC Treasury Administrator PSC Cashier requires these additional roles: • CUSTOM_PSC_MANAGE_PERMITS_ AGENCY • CUSTOM_PSC_MANAGE_PZ_AGENCY • CUSTOM_PSC_MANAGE_BL_AGENCY • CUSTOM_PSC_MANAGE_CE_AGENCY	

Adding Roles to Agency Users for Creating Transaction Types

Users requiring administrative access to create transaction types, such as permit types or planning and zoning applications need to be assigned these roles:

- CUSTOM_PSC_MANAGE_PERMITS_AGENCY
- CUSTOM_PSC_MANAGE_PNZ_AGENCY

ORACLE

- ORA_CRM_EXTN_ROLE (This role will be available for assignment only after the first transaction type is created.)

- ORA_FND_IT_SECURITY_MANAGER_JOB

- ORA_ASM_APPLICATION_IMPLEMENTATION_CONSULTANT_JOB

Related Topics

- Managing Roles in Public Sector Licensing and Permitting
- Working with Roles in the Security Console
- Managing Agency Staff Profiles
- Setting Up Public Users
- Setting Up Public User Roles

Managing Custom Roles for Planning Application Access

This topic describes custom roles that need to be created for the Planning and Zoning offering.

For information on the custom planning and zoning custom roles, see *Creating Custom Roles for Public Sector Licensing and Permitting*.

ORACLE

3 Working with the Security Console

Using the Security Console

Use the Security Console to manage application security in your Oracle Applications Cloud offering. Use the IT Security Manager role to perform security-related tasks pertinent to role management, role analysis, and user-account management.

Oracle Identity Cloud Service Integration

Oracle Public Sector Licensing and Permitting also supports the use of Oracle Identity Cloud Service (IDCS) as an identify provider platform (IDP). If you are using IDCS, refer to that documentation for tasks related to user management, authentication, resetting passwords, locking accounts, and so on to become familiar with using the Identity Cloud Service Console.

For more information on completing user management tasks in the Identity Cloud Service Console, see the Oracle IDCS administration guide: *Administering Oracle Identity Cloud Service.*

If you are using Oracle IDCS as your IDP for sign on authentication, you use the Identity Cloud Service Console to manage user authentication, and you'll use the Fusion Identity Management Security Console to manage roles.

While the data shared by the two systems is synchronized automatically, the synchronization does not occur immediately (in real time). For example, new user accounts will not get activated in real time. You can wait until the user IDs are synchronized between Fusion Identity Management and IDCS, or you can create the same user ID manually using the IDCS user management console.

Security Console Tasks

You can perform these tasks in the Security Console:

Security Area	Tasks
Roles	• Create job, abstract, and duty roles. • Edit custom roles. • Copy roles. • Compare roles. • Visualize role hierarchies and assignments to users. • Review Navigator menus available to roles or users, identifying roles that grant access to Navigator items and privileges required for that access.
Users	• Create user accounts. • Review, edit, lock, or delete existing user accounts. • Assign roles to user accounts. • Reset passwords.

ORACLE

Security Area	Tasks
Analytics	• Review statistics concerning role categories, the roles belonging to each category, and the components of each role. • View the data security policies, roles, and users associated with each database resource.
Certificates	• Generate, export, or import PGP or X.509 certificates, which establish encryption keys for data exchanged between Oracle Cloud applications and other applications. • Generate signing requests for X.509 certificates.
Administration	• Establish rules for the generation of user names. • Set password policies. • Create standards for role definition, copying, and visualization. • Review the status of role-copy operations. • Define templates for notifications of user-account events such as password expiration.

Security Console Access

You must have the IT Security Manager role to use the Security Console. This role inherits the following duty roles:

- Security Management
- Security Reporting

Running Security Background Processes

To prepare the Security Console for use, arrange to run background processes that replenish security data. Also use Security Console Administration pages to select general and role-oriented options, track the status of role-copy jobs, and select, edit, or add notification templates. These generate messages to notify users of events that concern them, such as password-expiration warnings.

Run two background processes:

- The Retrieve Latest LDAP Changes process copies data from the LDAP directory to Oracle Cloud Applications Security tables. Run it once, during implementation. Select Setup and Maintenance from the Navigator. In the Setup and Maintenance work area, search for and select the Run User and Roles Synchronization Process task.

- The Import User and Role Application Security Data process copies users, roles, privileges, and data security policies from the identity store, policy store, and ApplCore grants schema to Oracle Cloud Applications Security tables. Schedule it to run regularly to update those tables: Select Scheduled Processes in the Tools work area, and then select the process from the Schedule New Process option.

General Administration Options

Select the Security Console Administration tab, and then the General tab on the Administration page, to set these options:

- User Preferences
    - Select the format of the User Name, the value that identifies a user as he signs in. It is generated automatically in the format you select. Options include first and last name delimited by a period, email address, first-name initial and full last name, and person or party number.

ORACLE

- o Select the check box labeled "Generate system user name when generation rule fails" to enable the automatic generation of User Name values if the selected generation rule cannot be implemented.

- Password Policy

  > **Note:** If you are using IDCS as your IDP, then the IDCS password policies will be applied. Refer to your IDCS administration documentation.

  - o Establish the number of days a password remains valid. Set the number of days before expiration that a user receives a warning to reset the password. And define the period in which a user must respond to a notification to reset his password ("Hours Before Password Reset Token Expiration").
  - o Select a password format.
  - o Determine whether a previous password may be reused.
  - o Determine whether an administrator can manually modify passwords in the Reset Password dialog, available from a given user's record in the Users tab. This option applies only to the manual-reset capability. An administrator can always use the Reset Password dialog to initiate the automatic reset of a user's password.

- Certificate Preferences: Set the default number of days for which a certificate remains valid. (Certificates establish keys for the encryption and decryption of data that Oracle Cloud applications exchange with other applications.)

- Synchronization Process Preferences: Specify a number of hours since the last run of the Import User and Role Application Security Data process. When a user selects the Security Console Roles tab, a warning message appears if the process has not been run in this period.

Role Administration Options

Select the Security Console Administration tab, and then the Roles tab on the Administration page, to set these options:

- Role prefixes and suffixes: Create the prefix and suffix added to the name and code of role copies. Each role has a Role Name (a display name) and a Role Code (an internal name). A role copy adopts the name and code of the source role, with this prefix or suffix (or both) added. The addition distinguishes the copy from its source. By default there is no prefix, the suffix for a role name is "Custom," and the suffix for a role code is "_CUSTOM."

- Graph node limit: Set the maximum number of nodes a visualization graph can display. When a visualization graph would contain a greater number of nodes, the visualizer displays a message advising the user to select the table view.

- Enable edit of data security policies: Determine whether users can enter data in the Data Security Policies page of the role-creation and role-edit trains available from the Roles tab.

- Enable edit of user role membership: Determine whether users can enter data in the Users page of the role-creation and role-edit trains available from the Roles tab.

- Enable default table view: Determine whether visualizations generated from the Roles tab default to the table view or, if this option is cleared, the radial graph view.

Role Copy Status

Select the Security Console Administration tab, and then the Role Copy Status tab on the Administration page, to view records of jobs to copy roles. These jobs are initiated in the Roles page. Job status is updated automatically until a final status, typically Completed, is reached. You can delete the row representing a copy job; click its x icon.

Running Retrieve Latest LDAP Changes

Information about users and roles in your LDAP directory is available automatically to Oracle Cloud Applications. However, in specific circumstances you're recommended to run the Retrieve Latest LDAP Changes process. This topic describes when and how to run Retrieve Latest LDAP Changes.

You run Retrieve Latest LDAP Changes if you believe data-integrity or synchronization issues may have occurred between Oracle Cloud Applications and your LDAP directory server. For example, you may notice differences between roles on the Security Console and roles on the Create Role Mapping page. On-premises customers should also run this process after applying monthly updates.

Sign in with the IT Security Manager job role and follow these steps:

1. Open the Scheduled Processes work area.
2. Click **Schedule New Process** in the Search Results section of the Overview page.
   The **Schedule New Process** dialog box opens.
3. In the **Name** field, search for and select the Retrieve Latest LDAP Changes process.
4. Click **OK** to close the **Schedule New Process** dialog box.
5. In the **Process Details** dialog box, click **Submit**.
6. Click **OK**, then **Close**.
7. On the Scheduled Processes page, click the **Refresh** icon.
   Repeat this step periodically until the process completes.

> **Note:** Only one instance of Retrieve Latest LDAP Changes can run at a time.

Security Visualizations

A Security Console visualization graph consists of nodes that represent security items. These may be users, roles, privileges, or aggregate privileges. Arrows connect the nodes to define relationships among them. You can trace paths from any item in a role hierarchy either toward users who are granted access or toward the privileges roles can grant.

You can select either of two views:

- Radial: Nodes form circular (or arc) patterns. The nodes in each circular pattern relate directly to a node at the center. That focal node represents the item you select to generate a visualization, or one you expand in the visualization.

- Layers: Nodes form a series of horizontal lines. The nodes in each line relate to one node in the previous line. This is the item you select to generate a visualization, or the one you expand in the visualization.

For example, a job role might consist of several duty roles. You might select the job role as the focus of a visualization (and set the Security Console to display paths leading toward privileges):

- The Radial view would initially show nodes representing the duty roles encircling a node representing the job role.

- The Layers view would initially show the duty-role nodes in a line after the job-role node.

You can then manipulate the image, for example by expanding a node to display the items it consists of.

As an alternative, you can generate a visualization table that lists items related to an item you select. For example, a table may list the roles that descend from a role you select, or the privileges inherited by the selected role. You can export tabular data to an Excel file.

ORACLE

Working with a Visualization Graph

Within a visualization graph, you can select the Radial or Layers view. In either view, you can zoom in or out of the image. You can expand or collapse nodes, magnify them, or search for them. You can also highlight nodes that represent types of security items.

To select one of the views, click Switch Layout in the Control Panel, which is a set of buttons on the visualization. Then select Radial or Layers.

Node Labels

You can enlarge or reduce a visualization, either by expanding or collapsing nodes or by zooming in or out of the image. As you do, the labels identifying nodes change:

- If the image is large enough, each node displays the name of the item it represents.

- If the image is smaller, symbols replace the names: U for user, R for role, S for predefined role, P for privilege, and A for aggregate privilege.

- If the image is smaller still, the nodes are unlabeled.

Regardless of labeling, you can hover over a node to display the name and description of the user, role, or privilege it represents.

Nodes for each type of item are visually depicted such that item types are easily distinguished.

Expanding or Collapsing Nodes

To expand a node is to reveal roles, privileges, or users to which it connects. To collapse a node is to hide those items. To perform these actions:

1. Select a node and right-click.
2. Select one of these options:

   - Expand reveals nodes to which the selected node connects directly, and Collapse hides those nodes.

   - Expand All reveals all generations of connecting nodes, and Collapse All hides those nodes.

Alternatively, double-click a collapsed node to expand it, or an expanded node to collapse it.

Using Control Panel Tools

Apart from the option to select the Radial or Layers view, the Control Panel contains these tools:

- Zoom In: Enlarge the image. You can also use the mouse wheel to zoom in.

- Zoom Out: Reduce the image. You can also use the mouse wheel to zoom out.

- Zoom to Fit: Center the image and size it so that it is as large as it can be while fitting entirely in its display window. (Nodes that you have expanded remain expanded.)

- Magnify: Activate a magnifying glass, then position it over nodes to enlarge them temporarily. You can use the mouse wheel to zoom in or out of the area covered by the magnifying glass. Click Magnify a second time to deactivate the magnifying glass.

- Search: Enter text to locate nodes whose names contain matching text. You can search only for nodes that the image is currently expanded to reveal.

ORACLE

- Control Panel: Hide or expose the Control Panel.

Using the Legend

A Legend lists the types of items currently on display. You can:

- Hover over the entry for a particular item type to locate items of that type in the image. Items of all other types are grayed out.

- Click the entry for an item type to disable items of that type in the image. If an item of that type has child nodes, it is grayed out. If not, it disappears from the image. Click the entry a second time to restore disabled items.

- Hide or expose the Legend by clicking its button.

Using the Overview

On the image, click the plus sign to open the Overview, a thumbnail sketch of the visualization. In it, click any area of the thumbnail to focus the actual visualization on that area.

As an alternative, click the background of the visualization, and move the entire image in any direction.

Refocusing the Image

You can select any node in a visualization as the focal point for a new visualization: Right-click a node, then select Set as Focus.

> **Note:** You can review role hierarchies using either a tabular or a graphical view. The view you see by default depends on the setting of the **Enable default table view** option on the Administration tab.

Working with a Visualization Table

A visualization table contains records of roles, privileges, or users related to a security item you select. The table displays records for only one type of item at a time:

- If you select a privilege as the focus of your visualization, select the Expand Toward Users option. Otherwise the table shows no results. Then use the Show option to list records of either roles or users who inherit the privilege.

- If you select a user as the focus of your visualization, select the Expand Toward Privileges option. Otherwise the table shows no results. Then use the Show option to list records of either roles or privileges assigned to the user.

- If you select any type of role or an aggregate privilege as the focus of your visualization, you can expand in either direction.

  - If you expand toward privileges, use the Show option to list records of either roles lower in hierarchy, or privileges related to your focus role.
  - If you expand toward users, use the Show option to list records of either roles higher in hierarchy, or users related to your focus role.

Tables are all-inclusive:

- A Roles table displays records for all roles related directly or indirectly to your focus item. For each role, inheritance columns specify the name and code of a directly related role.

ORACLE

- A Privileges table displays records for all privileges related directly or indirectly to your focus item. For each privilege, inheritance columns display the name and code of a role that directly owns the privilege.

- A Users table displays records for all users assigned roles related directly or indirectly to your focus item. For each user, Assigned columns display the name and code of a role assigned directly to the user.

Use a field on a column to enter search text, then press Enter. The table displays records whose column values contain text matching your search text.

You can export a table to Excel. Click the Export to Excel button. You may either open the Excel file directly or save it. If you opt to save the file, you're prompted to define a path.

Generating a Visualization

To generate a visualization:

1. Select the Roles tab in the Security Console.
2. Search for the security item on which you want to base the visualization.

   - In a Search field, select any combination of item types, for example job role, duty role, privilege, or user.

   - In the adjacent field, enter at least three characters. The search returns items of the types you selected, whose names contain the characters you entered.

   - Select one of those items. Or, click the Search button to load all the items in a Search Results column, and select an item there.

3. Select either a Show Graph button or a View as Table button.

   > **Note:** In a page for role administration, you can determine which of these is the default view.

4. In the Expand Toward list, select Privileges to trace paths from your selected item toward items lower in its role hierarchy. Or select Users to trace paths from your selected item toward items higher in its hierarchy.
5. If the Table view is active, select an item type in the Show list: Roles, Privileges, or Users. (The options available to you depend on your Expand Toward selection.) The table displays records of the item type you select. Note that an aggregate privilege is considered to be a role.

Security Console Analytics for Roles

You can review statistics about the roles that exist in your Oracle Cloud instance. Select the Analytics tab, and then the Roles tab on the Analytics page. Then view these analyses:

- 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.

ORACLE

- 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.

Data Security Policies

You can review information about data security policies that grant access to a database resource, or about roles and users granted access to that resource.

To begin, select the Analytics tab, and then the Database Resources tab on the Analytics page. Select the resource you want to review in the **Database Resource** field. Then click **Go**.

The Data Security Policies table documents policies that grant access to the selected database resource.

Each row documents a policy, specifying by default:

- The data privileges it grants.

- The condition that defines how data is selected from the database resource.

- The policy name and description.

- A role that includes the policy.

For any given policy, this table may include multiple rows, one for each role in which the policy is used.

Authorized Roles

The Authorized Roles table documents roles with direct or indirect access to the selected database resource. Any given role may:

- Include one or more data security policies that grant access to the database resource. The Authorized Roles table includes one row for each policy belonging to the role.

- Inherit access to the database resource from one or more roles in its hierarchy. The Authorized Roles table includes one row for each inheritance.

By default, each row specifies:

- The name of the role it documents.

- The name of a subordinate role from which access is inherited, if any. (If the row documents access provided by a data security policy assigned directly to the subject role, this cell is blank.)

- The data privileges granted to the role.

- The condition that defines how data is selected from the database resource.

ORACLE

> **Note:** A role's data security policies and hierarchy may grant access to any number of database resources. However, the Authorized Roles table displays records only of access to the database resource you selected.

Authorized Users

The Authorized Users table documents users who are assigned roles with access to the selected database resource.

By default, each row specifies a user name, a role the user is assigned, the data privileges granted to the user, and the condition that defines how data is selected from the database resource. For any given user, this table may include multiple rows, one for each grant of access by a data security policy belonging to, or inherited by, a role assigned to the user.

Manipulating the Results

In any of these three tables, you can:

- Add or remove columns. Select **View - Columns**.
- Search among the results. Select **View - Query by Example** to add a search field on each column in a table.
- Export results to a spreadsheet. Select the **Export to Excel** option available for each table.

Types of Secured Information

Information can be private, personally identifiable, or sensitive information.

Private information is confidential in some contexts.

Personally identifiable information (PII) identifies or can be used to identify, contact, or locate the person to whom the information pertains.

Some PII information is sensitive.

A person's name is not private. It is PII but not sensitive in most contexts. The names and work phone numbers of employees may be public knowledge within an enterprise, so not sensitive but PII. In some circumstances it is reasonable to protect such information.

Some data is not PII but is sensitive, such as medical data, or information about a person's race, religion or sexual orientation. This information cannot generally be used to identify a person, but is considered sensitive.

Some data is not private or personal, but is sensitive. Salary ranges for grades or jobs may need to be protected from view by users in those ranges and only available to senior management.

Some data is not private or sensitive except when associated with other data the is not private or sensitive. For example, date or place of birth is not a PII attribute because by itself it cannot be used to uniquely identify an individual, but it is confidential and sensitive in conjunction with a person's name.

Working with Roles in the Security Console

This topic describes the tasks associated with roles that you complete using the Security Console.

You can use the Security Console to perform a variety of tasks related to roles, including:

- View the roles assigned to a user.

- Identify users who have a specific role.

- Copying existing roles.

- Create duty, job, or abstract roles.

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

Viewing the Roles Assigned to a User

1. Open the Security Console.
2. On the Roles tab, 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:

   a. Select the role and right-click.
   b. 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 this view.

Identifying Users Who Have a Specific Role

1. On the Roles tab of 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:** 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, user names appear on hover. Users may inherit roles either directly or indirectly from other roles. 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

On the Security Console you can review the role hierarchy of a job role, an abstract role, or a duty role.

1. On the Roles tab of the Security Console, ensure that **Expand Toward** is set to **Privileges**.
2. Search for and select the role. Depending on the enterprise setting, either a table or a graphical representation of the role appears.

3. 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. Set **Show** to **Privileges** to switch from roles to privileges.

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

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

Comparing Roles

You can compare any two roles to see the structural differences between them. As you compare roles, you can also add function and data security policies existing in the first role to the second role, providing that the second role is not a predefined role.

For example, assume you have copied a role and edited the copy. You then upgrade to a new release. You can compare your edited 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 edited role. If the changes consist of new function or data security policies, you can upgrade your edited role by adding the new policies to it.

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. Select two roles for comparison.
5. Use the **Filter Criteria** field to filter for any combination of these artifacts in the two roles:
   - Function security policies
   - Data security policies
   - Inherited roles
6. Use the **Show** field to determine whether the comparison returns:
   - All artifacts existing in each role
   - Those that exist only in one role, or only in the other role
   - Those that exist only in both roles
7. Click the **Compare** button.

You can export the results of a comparison to a spreadsheet. Select the **Export to Excel** option.

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

ORACLE

Adding Policies to and Modifying Delivered Roles

For Oracle Public Sector Licensing and Permitting, you should *not* modify the functional or data security policies of delivered roles. The Oracle Public Sector Licensing and Permitting system is REST-based, and, as such, the functional and data security policies should not be separated from the roles. Doing so risks the REST layer becoming out of sync with the modified role, causing unintentional security behavior.

The intent of the Oracle Public Sector Licensing and Permitting security implementation approach is to require as little configuring and customizing as possible.

The recommendations for working with Oracle Public Sector Licensing and Permitting are:

- Assign users to the closest job role that matches their intended usage of the system. Doing so is the simplest, most efficient, and safest approach.

- If a user has a dual role, multiple job roles can be assigned to the same user.

- If you *must* modify a delivered role, consider cloning the delivered role, and adding or removing duty roles or aggregate roles on the Role Hierarchy tab.

- The Function Security Policies tab and Data Security Policies tab should *never be modified.*

Custom Role Considerations

In many cases, an efficient method of creating a role is to copy an existing role, then edit the copy to meet your requirements. Typically, you would create a role from scratch if no existing role is similar to the role you want to create.

To create a role from scratch, select the Roles tab in the Security Console, then click the Create Role button. Enter values in a series of role-creation pages, selecting Next or Back to navigate among them.

Providing Basic Information

On a Basic Information page:

1. In the Role Name field, create a display name, for example North America Accounts Receivable Specialist.
2. In the Role Code field, create an internal name for the role, such as AR_NA_ACCOUNTS_RECEIVABLE_SPECIALIST_JOB.

   Note: Do not use "ORA_" as the beginning of a role code. This prefix is reserved for roles predefined by Oracle. You cannot edit a role with the ORA_ prefix.

3. In the Role Category field, select a tag that identifies a purpose the role serves in common with other roles. Typically, a tag specifies a role type and an application to which the role applies, such as Financials - Job Roles.

   If you select a duty-role category, you cannot assign the role you are creating directly to users. To assign it, you would include it in the hierarchy of a job or abstract role, then assign that role to users.
4. Optionally, describe the role in the Description field.

Adding Function Security Policies

Note: Do not add function or data security policies manually to the roles used in Public Sector Licensing and Permitting offerings.

ORACLE

Configuring the Role Hierarchy

A Role Hierarchy page displays either a visualization graph, with the role you are creating as its focus, or a visualization table. Select the Show Graph button or View as Table button to select between them. In either case, link the role you are creating to other roles from which it is to inherit function and data security privileges.

- If you are creating a duty role, you can add duty roles or aggregate privileges to it. In effect, you are creating an expanded set of duties for incorporation into a job or abstract role.

- If you are creating a job or abstract role, you can add aggregate privileges, duty roles, or other job or abstract roles to it.

To add a role:

1. Select Add Role.
2. In a Search field, select a combination of role types and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.
3. Select the role you want, and click Add Role Membership. You add not only the role you have selected, but also its entire hierarchy.

In the graph view, you can use the visualization Control Panel, Legend, and Overview tools to manipulate the nodes that define your role hierarchy.

Adding Users to Roles

On a Users page, you can select users to whom you want to assign a job or abstract role you are creating. (You cannot assign a duty role directly to users.)

> **Note:** For the Users page to be active, you must select an "Enable edit of user role membership" option. To locate it, select the Administration tab, and then the Roles tab on the Administration page. If this option is not selected, the Users page is read-only.

To add a user:

1. Select Add User.
2. In a Search field, select the value Users or types of role in any combination and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.
3. Select a user or role. If you select a user, click Add User to Role. If you select a role, click Add Selected Users; this adds all its assigned users to the role you are creating.

The Users page lists all selected users. You can delete a user. You may, for example, have added all the users associated with a role. If you want to assign your new role only to some of them, you must delete the rest. To delete a user, click its x icon.

Copying and Editing Roles

Rather than create a role from scratch, you can copy a role, then edit the copy to create a new role. Or you can edit existing custom roles.

> **Note:** Do not edit roles delivered by Oracle.

Initiate a copy or an edit from the Roles tab in the Security Console. Do either of the following:

- Create a visualization graph and select any role in it. Right-click and select **Copy Role** or **Edit Role**.
- 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 **Copy Role** or **Edit Role**.

If you are copying a role, select one of two options in a Copy Option dialog:

- **Copy role**: You copy only the role you have selected. The source role has links to roles in its hierarchy, and the copy inherits links to the original versions of those roles. If you select this option, subsequent changes to the inherited roles affect not only the source highest role, but also your copy.
- **Copy role and inherited roles**: You copy not only the role you have selected, but also all of the roles in its hierarchy. Your copy of the highest role is connected to the new copies of subordinate roles. If you select this option, you insulate the copied role from changes to the original versions of the inherited roles.

Next, an editing train opens. You follow the same process in editing a role as you would to create one. However, note the following:

- In the Basic Information page, a **Predefined role** box is checked if you selected the Edit Role option for a role shipped by Oracle. In that case, you can:
    - Add custom data security policies. Modify or remove those custom data security policies.
    - Add or remove users if the role is a job, abstract, or discretionary role.

    You cannot:
    - Modify, add, or remove function security policies.
    - Modify or remove data security policies provided by Oracle.
    - Modify the role hierarchy.

    The **Predefined role** check box is cleared if you are editing a custom role or if you have copied a role. In that case, you can make any changes to role components.
- By default, the name and code of a copied role match the source role's, except a prefix, suffix, or both are appended. In the Roles Administration page, you can configure the default prefix and suffix for each value.
- A copied role cannot inherit users from a source job or abstract role. You must select users for the copied role. (They may include users who belong to the source role.)
- When you copy a role, the Role Hierarchy page displays all roles subordinate to it. However, you can add roles only to, or remove them from, the highest role you copied.

To monitor the status of a role-copy job, select the Administration tab, and then the Role Copy Status tab of the Administration page.

Copying a Top Role

When you copy a role on the Security Console, you select one of the following options:

- Copy top role
- Copy top role and inherited roles

If you select the **Copy top role** option, then only the top role from the selected role hierarchy is copied. Memberships are created for the copy in the roles of which the original is a member. That is, the copy of the top role references the

ORACLE

inherited role hierarchy of the source role. Any changes made to those inherited roles appear in both the source role and the copy. Therefore, you must take care when you edit the role hierarchy of the copy. You can:

- Add roles directly to the copy without affecting the source role.

- Remove any role from the copy that it inherits directly without affecting the source role. However, if you remove any role that's inherited indirectly by the copy, then any role that inherits the removed role's parent role is affected.

- Add or remove function and data security privileges that are granted directly to the copy of the top role.

If you copy a custom role and edit any inherited role, then the changes affect any role that inherits the edited role.

The option of copying the top role is referred to as a shallow copy, where the copy references the same instances of the inherited roles as the source role. No copies are made of the inherited roles.

The option of copying the top role is referred to as a shallow copy. This figure summarizes the effects of a shallow copy. It shows that the copy references the same instances of the inherited roles as the source role. No copies are made of the inherited roles.

You're recommended to create a shallow copy unless you must make changes that could affect other roles or that you couldn't make to predefined roles. To edit the inherited roles without affecting other roles, you must first make copies of those inherited roles. To copy the inherited roles, select the **Copy top role and inherited roles** option.

> **Tip:** The Copy Role: Summary and Impact Report page provides a useful summary of your changes. Review this information to ensure that you haven't accidentally made a change that affects other roles.

Copy a Top Role and the Inherited Roles

Selecting **Copy top role and inherited roles** is a request to copy the entire role hierarchy. These rules apply:

- Inherited aggregate privileges are never copied. Instead, membership is added to each aggregate privilege for the copy of the source role.

- Inherited duty roles are copied if a copy with the same name doesn't already exist. Otherwise, membership is added to the existing **copies** of the duty roles for the new role.

When inherited duty roles are copied, custom duty roles are created. Therefore, you can edit them without affecting other roles. Equally, changes made subsequently to the source duty roles don't appear in the copies of those roles. For example, if those duty roles are predefined and are updated during upgrade, then you may have to update your copies manually after upgrade.

This option is referred to as a deep copy, where copies of the inherited duty roles with the same name don't already exist. Therefore, the inherited duty roles are copied when you copy the top role. Aggregate privileges are referenced from the new role.

Copying Job and Abstract Roles

You can copy any job role or abstract role and use it as the basis for a custom role. Copying roles is more efficient than creating them from scratch, especially if your changes are minor.

1. On the Roles tab of the Security Console, search for the role to copy.
2. Select the role in the search results. The role hierarchy appears in tabular format by default.

   > **Tip:** Tip: Click the **Show Graph** icon to show the hierarchy in graphical format.

ORACLE

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.
5. Click **Copy Role**.
6. On the Copy Role: Basic Information page, review and edit the **Role Name**, **Role Code**, and **Description** values, as appropriate.

    > **Tip:** The role name and code have the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. You can overwrite these values for the role that you're copying. However, any roles inherited by the copied role are unaffected by any name changes that you make on the Copy Role: Basic Information page.

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.

    If you prefer, you can visit the intermediate train stops after the Copy Role: Basic Information page and edit your copy of the role before you save it.

Editing Job and Abstract Roles

You can create a role by copying a predefined job role or abstract role and editing the copy.

> **Note:** It is not recommended to create job or abstract roles from scratch in the Public Sector Licensing and Permitting services, except for any custom roles specifically documented in Functional Setup Manager. Copy existing roles and modify as needed.

1. On the Roles tab of the Security Console, search for and select your custom 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**.

On the Edit Role: Functional Security Policies page, any function security privileges granted to the copied role appear on the Privileges tab. Select a privilege to view details of the code resources that it secures in the Details section of the page.

> **Note:** For Oracle Public Sector Licensing and Permitting, do not remove privileges from roles.

> **Note:** If a function security privilege forms part of an aggregate privilege, then add the aggregate privilege to the role hierarchy. Don't grant the function security privilege directly to the role. The Security Console enforces this approach.

The Resources tab, which is read-only, lists any resources granted to the role directly rather than through function security privileges. As you can't grant resources directly to roles on the Security Console, only resource grants created before Release 12 could appear on this tab. You can't edit these values.

Make no changes on the Copy 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**.

ORACLE

The Edit Role: Role Hierarchy page shows the copied role and its inherited aggregate privileges and duty roles. The hierarchy is 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 confirmation message.

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. Close the **Add Role Membership** dialog box.

   The Edit Role: Role Hierarchy page shows the updated role hierarchy.
7. Click **Next**.

To provision the role to users, you must create a role mapping. Don't provision the role to users on the Security Console.

> **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**.

Copying and Editing Duty Roles

You can copy a duty role and edit the copy to create a duty role. Copying duty roles is the recommended way of creating duty roles.

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 hierarchy appears in tabular format by default.

   Tip: 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.
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 code have the default prefix and suffix for copied roles specified on the Roles subtab of the Security Console Administration tab. You can overwrite these values for the role that you're copying. However, any roles inherited by the copied role are unaffected by any name changes that you make on the Copy Role: Basic Information page.
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

ORACLE

To edit the role:

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**.

On the Edit Role: Functional Security Policies page, any function security privileges granted to the copied role appear on the Privileges tab. Select a privilege to view details of the code resources that it secures.

> **Note:** For Oracle Public Sector Licensing and Permitting, do not remove privileges from roles.

> **Note:** If a function security privilege forms part of an aggregate privilege, then add the aggregate privilege to the role hierarchy. Don't grant the function security privilege directly to the role. The Security Console enforces this approach.

The Resources tab, which is read-only, lists any resources granted to the role directly rather than through function security privileges. As you can't grant resources directly to roles on the Security Console, only resource grants created before Release 12 could appear on this tab. You can't edit these values.

Make no changes on the Edit 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**.

The Edit Role: Role Hierarchy page shows the copied duty role and any duty roles and aggregate privileges that it inherits. The hierarchy is 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**.

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

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

The role is available immediately.

Managing Implementation Users

This topic describes the tasks associated with the initial users of the implementation team.

Implementation Users

> **Note:** If you are using Oracle IDCS as your IDP, then the user IDs will not get activated in real time. You can wait until the user IDs are synchronized with IDCS, or you can create the same user ID manually using the IDCS user management console.

The initial user can perform all the necessary setup tasks. She can also perform security tasks, including resetting passwords and the granting of additional privileges to herself and to others. After you sign in the first time, you can create additional implementation users with the same broad setup privileges that Oracle provides to the initial user. If you prefer, you can restrict the privileges of these implementation users based on your own setup needs.

The setup or implementation users are typically different from the Oracle Applications Cloud application users. For example:

- Setup users are usually not part of your Oracle Applications Cloud organization.

- You don't assign them product-specific work or make it possible for them to view product-specific data.

You do, however, have to give them the necessary privileges they require to complete application setup. You provide these privileges through role assignment.

Your application includes several types of roles. A job role, such as the IT Security Manager role, corresponds to a specific job that a person does in the organization. An abstract role, such as the Employee role, corresponds to general categories of people in an organization. You assign both types of roles to users in the security console. For the setup users, these roles are:

- Application Diagnostic Administrator

- Application Implementation Consultant

- Employee

- IT Security Manager

> **Note:** The Application Implementation Consultant role has unrestricted access to large amounts of data. Limit assignment of the Application Implementation Consultant abstract role to implementation users who perform a wide range of implementation tasks and move the setup data across environments. Use other administrator roles such as the Financials Applications Administrator for users required to perform specific implementation tasks.

There is nothing to stop you from providing the same setup permissions to users that are part of the organization, if you need to. Highly privileged implementation users are not the only users who can do setup. You can create administrative users who don't have such broad permissions, yet can configure product-specific structures and perform other related setup tasks

ORACLE

Managing User Accounts

The User Accounts page of the Security Console provides summaries of user accounts that you select to review. For each account, it always provides:

- The user's login, first name, and last name, in a User column.

- Whether the account is active, whether it is locked, and the user's password-expiration date, in a Status column.

It may also provide:

- Associated worker information, if the user account was created in conjunction with a worker record in Human Capital Management. This may include person number, manager, job title, and business unit.

- Party information, if the user account was created in conjunction with a party record created in CRM. This may include party number and party usage.

The User Accounts page also serves as a gateway to account-management actions you can complete. These include:

- Reviewing details of, editing, or deleting existing accounts.

- Adding new accounts.

- Locking accounts.

- Resetting users' passwords.

Note: I you are using Oracle IDCS as your IDP, use the IDCS user management console to complete these tasks.

To begin working with user accounts:

1. Select the Users tab in the Security Console.
2. In a Search field, select any combination of user states and enter at least three characters.

   The search returns user accounts at the states you selected, whose login, first name, or last name begins with the characters you entered.

Reviewing and Editing User Accounts

To review full details for an existing account, search for it in the User Accounts page and click its user login in the User column. This opens a User Account Details page.

These details always include:

- User information, which consists of user, first, and last name values, and an e-mail address. It also includes an external identifier if one has been created. This is an external-system identifier, such as a single sign-on account ID if single sign-on is enabled.

- Account information, which comprises the user's password-expiration date, whether the account is active, and whether it is locked.

- A table listing the roles assigned to the user, including whether they are autoprovisioned or assignable. A role is assignable if it can be delegated to another user.

The page may also include an Associated Worker Information region or an Associated Party Information region. The former appears only if the user account is related to a worker record in Human Capital Management, and the latter if the user account is related to a party record in CRM.

ORACLE

To edit these details, click Edit in the User Account Details page. Be aware, however:

- You can edit values only in the User Information, Account Information, and Roles regions.

- Even in those regions, you can edit some fields only if the user is not associated with a worker or a party. If not, for example, you can modify the First Name and Last Name values in the User Information region. But if the user is associated with a worker, you would manage these values in Human Capital Management. They would be grayed out in this Edit User Details page.

- In the Roles table, Autoprovisioned check boxes are set automatically, and you cannot modify the settings. The box is checked if the user obtained the role through autoprovisioning, and cleared if the role was manually assigned. You can modify the Assignable setting for existing roles.

Click Add Autoprovisioned Roles to add any roles for which the user is eligible. Or, to add roles manually, click Add Role. Search for roles you want to add, select them, and click Add Role Membership.

You can also delete roles. Click the x icon in the row for the role, and then respond Yes to a confirmation message.

Adding User Accounts

The ability to add user accounts in the Security Console is intended for the creation of implementation users. The expectation is that an implementation user would set up Oracle Public Sector Licensing and Permitting. Once the implementation users are set up, the offering can then be configured to add the end users. For Oracle Public Sector Licensing and Permitting, the end users are created using:

- Agency Staff page for the agency employees, such as permit technicians, building inspectors, and so on.

- Self registration page for external users, such as residents applying for permits, planning applications, and so on.

To add a user account in the Security Console:

1. Select the Users tab in the Security Console to open the User Accounts page.
2. Click the Add User Account button.
3. Select a value for Associated Person Type: Worker if this account is to be linked to a worker record in HCM, or None if not.
4. By default, the account is set to be active and unlocked in the Account Information area. Typically these values are appropriate, but you may modify them.
5. Select the User Category with which you want to associate the user.

    Note: If you are not sure which user category to select, you may leave it unchanged. All new users are automatically assigned to the Default user category.
6. Enter name, e-mail, and password values in the User Information region as per the following guidance.
    - You need not enter a User Name value. It is generated automatically according to the user-name-generation rule selected in the General Administration page.
    - The First Name value is not required. However, you are expected to enter one if the selected user-name-generation rule makes use of the first name or the first-name initial.
    - The Password value must conform to the password policy established in the General Administration page. The Confirm Password value must match the Password value.
    - An external identifier is the user's ID in another system, such as a single sign-on account ID if single sign-on is enabled.
7. Click Add Autoprovisioned Roles, to assign roles for which role-provisioning rules make the user eligible.
8. Click Add Roles to assign other roles. Search for roles you want to assign, select them, then click Add Role Membership. Select Done when you are finished.

ORACLE

9. In the Roles table, select Assignable for any role that can be delegated to another user.
10. Click Save and Close.

> **Note:** If you are using Oracle IDCS as your IDP, the users created using Security Console and the Agency Staff page will not be activated immediately if. You can wait for the synchronization with IDCS, or you can create the same user ID in IDCS using IDCS user management console.

Resetting Passwords

An administrator may use the Security Console to reset other users' passwords. That action triggers an e-mail notification to each user, informing him or her of the new password.

A new password must conform to your password policy. You establish this policy in the General Administration page. The page in which you reset the password displays the policy.

> **Note:** If you are using Oracle IDCS as your IDP, this task needs to be completed in the IDCS console.

To reset a password:

1. In the User Accounts page, search for the user whose password you want to change.
2. In that user's row, click the Action icon, then Reset Password.

   As an alternative, open the user's account for editing: click the User Login value in the User Accounts page, then Edit in a User Account Details page. In that page, select Reset Password.
3. In a Reset Password dialog, select whether to generate the password automatically or change it manually. For a manual change, also enter a new password value and a confirmation value, which must match the new value.

   Note: The option to reset a password to an automatically generated value is always available. For the manual-reset option to be available, an "Administrator can manually reset password" option must be selected on the General Administration page.
4. Click the Reset Password button.

Locking and Unlocking User Accounts

An administrator may use the Security Console to lock users' accounts. When an account is locked, its user cannot sign in. He or she must either use the "forgot password" flow to reset the password or contact the help desk to have the account unlocked.

You can lock a user account in either of two ways. In either case, open the User Accounts page and search for the user whose account you want to lock.

> **Note:** If you are using Oracle IDCS as your IDP, this task needs to be completed in the IDCS console.

To complete the first procedure:

1. In the user's row, click the Action icon, then Lock Account.
2. Respond Yes to a confirmation message.

To complete the second procedure:

1. Open the user's account for editing: click the User Login value in the User Accounts page, then Edit in a User Account Details page.

ORACLE

2. In the Edit User Account page, select the Locked check box in the Account Information region.
3. Select Save and Close.

You can unlock the account only from the Edit User Account page, by clearing the Locked check box.

Deleting User Accounts

An administrator may use the Security Console to delete users' accounts.

1. Open the User Accounts page and search for the user whose account you want to delete.
2. In the user's row, click the Action icon, then Delete.
3. Respond Yes to a confirmation message.

Note: If you are using Oracle IDCS as your IDP, this task needs to be completed in the IDCS console.

Defining Notification Templates

Users may receive Email notifications of user-account events, such as account creation or password expiration. These notifications are generated from a set of templates, each of which specifies an event. A template generates a message to a user when that user is involved in the event tied to the template.

Note: If you are using Oracle IDCS as your IDP, some of the templates may not apply. For example, the welcome email, the password reset email, and so on will be triggered from IDCS.

To work with templates, click the User Categories tab in the Security Console. Then select a user category and on the User Category: Details page, click the Notifications tab. You must click the **Edit** button to make any changes.

There are eight events, and a predefined template exists for each event. Only one template linked to a given event can be enabled at a time. To use notification templates, ensure that notifications are enabled. To do that, select the **Enable Notifications** check box in the Notification Preferences region.

Even so, you can enable or disable templates, edit them, or create templates to replace existing ones. To create a template:

1. On the User Category: Notifications page, click **Add Template**.
2. Enter a name for the template and, optionally, a description.
3. Select an event. When you do, values for Message Subject and Message are copied from an already-configured template for which the same event is selected.
4. Edit the message subject, message text, or both. Note that message text may include tokens, which are replaced in runtime by literal values appropriate for a given user or account.
5. Select the **Enabled** check box to use the template immediately. If you do, the application automatically disables the template that had been enabled for that event. Or, leave the check box cleared to hold the template in reserve.
6. Click **Save and Close**.

To edit a template, select it from the templates listed in the Notification Templates table. Then follow essentially the same process as you would to create a template. Note, however, that you cannot modify the event selected for a template that has been saved. You may enable or disable an individual template by selecting or clearing its **Enabled** check box as you edit it.

Note: You can't edit or delete predefined templates that begin with the prefix name ORA. You also can't modify the message subject or the message. However, you can only enable or disable the predefined templates.

ORACLE

You can delete the templates you created. Select the template row in the table and click **Delete**.

The following table lists the tokens you can use in the message text for a template

Token	Meaning
${userLoginId}	The user name of the person whose account is being created or modified.
${firstName}	The given name of the person whose account is being created or modified.
${lastName}	The surname of the person whose account is being created or modified.
${managerFirstName}	The given name of the person who manages the person whose account is being created or modified.
${managerLastName}	The surname of the person who manages the person whose account is being created or modified.
${loginUrl}	The web address to sign in to Oracle Cloud. The user can sign in and use the Preferences page to change a password that is about to expire. Or, without signing in, the user can engage a forgot-password procedure to change a password that has already expired.
${resetUrl}	A one-time web address expressly for the purpose of resetting a password, used in the Password Generated, Password Reset, New Account, and New Account Manager templates.
${CRLFX}	Insert line break.
${SP4}	Insert four spaces.

Synchronizing User and Role Information

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.

Follow these steps:

1. Sign in to your Oracle Applications Cloud service environment as the service administrator.
2. Select **Navigator Others Setup and Maintenance** to open the Setup and Maintenance work area.
3. In the Setup and Maintenance work area, select the Run User and Roles Synchronization Process task in the Initial Users functional area.

    The process submission page for the Retrieve Latest LDAP Changes process opens.
4. Click **Submit**.
5. Click **OK** to close the confirmation message.

Resetting the Cloud Service Administrator Sign-In Details

Once you have set up your implementation users, you can reset the service administrator sign-in details for your Oracle Applications Cloud service. You reset these details to avoid problems later when you're loaded to the service as an employee. This topic describes how to reset the service administrator sign-in details.

Sign in to your Oracle Applications Cloud service using the TechAdmin user name and password and follow these steps:

1. In the Setup and Maintenance work area, select the Create Implementation Users task in the Initial Users functional area.

   The User Accounts page of the Security Console opens.
2. Search for your service administrator user name, which is typically your email. Your service activation mail contains this value.
3. In the search results, click your service administrator user name to open the User Account Details page.
4. Click **Edit**.
5. Change the **User Name** value to **ServiceAdmin**.
6. Delete any value in the **First Name** field.
7. Change the value in the **Last Name** field to **ServiceAdmin**.
8. Delete the value in the **Email** field.
9. Click **Save and Close**.
10. Sign out of your Oracle Applications Cloud service.

After making these changes, you use the user name **ServiceAdmin** when signing in as the service administrator.

Managing User Categories

You can categorize and segregate users based on the various functional and operational requirements. A user category provides you with an option to group a set of users such that the specified settings apply to everyone in that group. Typical scenarios in which you may want to group users are:

- Users have different preferences in receiving automated notifications from the Security Console. For example, employees of your organization using the organization's single sign-on don't require notifications from the Security Console about creating new users, password expiry, or password reset. However, the suppliers of your organization who aren't using the organization's single sign-on, must receive such notifications from the Security Console.

- You have built an external application for a group of users using the REST APIs of Oracle Fusion Applications. You intend to redirect this user group to the external application when using the Security Console to reset passwords or create new users.

On the Security Console page, click the User Category tab. You can perform the following tasks:

Task	Description
Segregate users into categories	Create user categories and add existing users to them. All existing users are automatically assigned to the Default user category unless otherwise specified. You may create more categories depending upon your requirement and assign users to those categories. **Note:** You can assign a user to only one category.

ORACLE

Task	Description
Specify Next URL	Specify a URL to redirect your users to a website or an application instead of going back to the Sign In page, whenever they reset their password. For example, a user places a password reset request and receives an Email for resetting the password. After the new password is authenticated, the user can be directed to a website or application. If nothing is specified, the user is directed to Oracle Applications Cloud Sign In page. You can specify only one URL per user category.
Enable notifications	Notifications are enabled by default, but you can disable them if required. You can also enable or disable notifications separately for each user category. If users belonging to a specific category don't want to receive any notification, you can disable notifications for all life cycle events. Alternatively, if users want to receive notifications only for some events, you can selectively enable the functionality for those events. Notifications are sent for a set of predefined events. To trigger a notification, you must create a notification template and map it to the required event. Depending on the requirement, you can add or delete a template that is mapped to a particular event. **Note:** You can't edit or delete predefined notification templates that begin with the prefix ORA. You can only enable or disable them. However, you can update or delete the user-defined templates. User Category feature supports both SCIM protocol and HCM Data Loader for performing any bulk updates.

Using the Security Console, you can add existing users to an existing user category or create a new category and add them. When you create new users, they are automatically assigned to the default category. At a later point, you can edit the user account and update the user category. You can assign a user to only one category.

Note: If you are creating new users using Security Console, you can also assign a user category at the time of creation.

You can add users to a user category in three different ways:

- Create a user category and add users to it
- Add users to an existing user category
- Specify the user category for an existing user

Note: You can create and delete a user category only using the Security Console. Once the required user categories are available in the application, you can use them in SCIM REST APIs and data loaders. You can't rename a user category.

Adding Users to a New User Category

To create a user category and add users:

1. On the Security Console, click **User Categories Create**.
2. Click **Edit**, specify the user category details, and click **Save and Close**.
3. Click the Users tab and click **Edit**.
4. On the Users Category: Users page, click **Add**.
5. In the Add Users dialog box, search for and select the user, and click **Add**.
6. Repeat adding users until you have added the required users and click **Done**.
7. Click **Done** on each page until you return to the User Categories page.

ORACLE

Adding Users to an Existing User Category

To add users to an existing user category:

1. On the Security Console, click **User Categories** and click an existing user category to open it.
2. Click the Users tab and click **Edit**.
3. On the Users Category: Users page, click **Add**.
4. On the Add Users dialog box, search for and select the user, and click **Add**.
5. Repeat adding users until you have added the required users and click **Done**.
6. Click **Done** on each page until you return to the User Categories page.

Specifying the User Category for an Existing User

To add an existing user to a user category:

1. On the Security Console, click **Users**.
2. Search for and select the user for whom you want to specify the user category.
3. On the User Account Details page, click **Edit**.
4. In the User Information section, select the **User Category**. The Default user category remains set for a user until you change it.
5. Click **Save and Close**.
6. On the User Account Details page, click **Done**.

You can delete user categories if you don't require them. However, you must ensure that no user is associated with that user category. Otherwise, you can't proceed with the delete task. On the User Categories page, click the **X** icon in the row to delete the user category.

Managing Notifications

Using the Security Console, you can determine whether to turn notifications on or off for the users.

1. On the Security Console, click User Categories and from the list, select the specific user category.
2. Click the Notifications tab and click **Edit**.
3. Select the **Enable Notifications** check box to enable notifications for all users of that user category. To disable notifications, deselect the check box.
4. Click **Done**.

To determine which notifications to send, you have to enable the notification template for each required event.

ORACLE