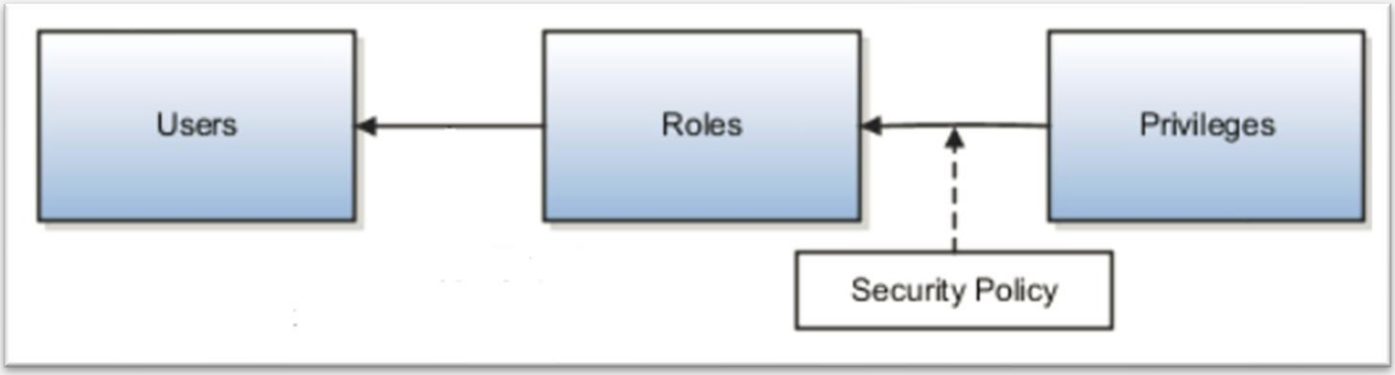
Oracle **Fusion** Technical

Securing Applications

Security Configuration Overview

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



What is

Role

A role is some **kind of privilege** that you can assign to the user allowing them to perform certain type actions in the application.

Privilege

A privilege is a single, **real–world action** on a single business object.

Data security

- Data security **consists of privileges** conditionally granted to a role and used to **control access** to the data.
- Data security is a statement of what action can be taken against which data.

Data security policy

Data security policy is a grant of a set of privileges to a principal on an object or attribute group for a given condition.

Function security

- Function security is a statement of what actions you can perform in which user interface pages.
- Function security controls access to user interfaces and actions needed to perform the tasks of a job.

HCM security profile

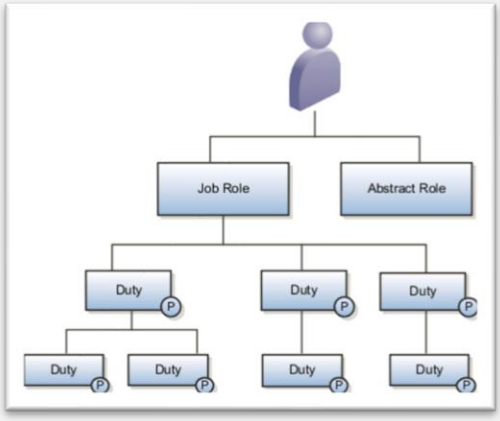
HCM security profiles are used to secure HCM data, such as people and departments. Data authorization for some roles, such as the Manager role, is managed in HCM, even in ERP and SCM applications. You can use HCM security profiles to generate grants for a job role such as Manager. The resulting data role with its role hierarchy and grants operates in the same way as any other data role.

For example, an HCM security profile identifies all employees in the Finance division.

Applications outside of HCM can use the HCM Data Roles UI pages to give roles access to HR people.

Types of Roles

- Job Rore
- Duty Role
- Aggregate Privileges
- Abstract Role



Job Role/ Enterprise roles

- These roles get mapped to **one or more duty roles**, because a person that takes a job in a company, then they are meant to perform several duties.
- Job roles represent the jobs that users perform in an organization.
- **For example**, a HR Recruiter Job will have a duty to scan resumes submitted and place an offer to the individual.
- Job roles are also referred to as external roles.
- The name of this role has the suffix_ JOB.

Duty Role/ Application Roles

- Duty roles represent a logical **collection of privileges** that grant access to tasks that someone performs as part of a job.
- It is like saying to a new staff that you can perform xyz duties within your job or it is your duty to perform x y z things in your organization
- **For example** , Invoice Creation Duty, Invoice Approval Duty, GL Journal Entry Duty, GL Journal Approval Duty, GL Journal Posting Duty etc..
- Here are some duty role characteristics:
    - 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.
- The name of this role has the suffix_DUTY.

Duty Role Components

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.

These are the **components of a data security policy**:

- A duty role, for example Expense Entry Duty.
- 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.

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 Privilege Names

- An aggregate privilege takes its name from the function security privilege that it includes.
- **For example**, the Promote Worker aggregate privilege includes the Promote Worker 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.

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.

Create, Edit, or Copy 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 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.

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.

Abstract Role/ Enterprise roles

- These roles are associated with a user irrespective of the Job they perform within an enterprise. Therefore, abstract roles are at a higher level spanning various jobs, and hence their name abstract.
- Abstract roles represent a worker's role in the enterprise, independently of the job that the worker is hired to do. There are three seeded abstract roles delivered with Oracle Fusion HCM. These are the Employee, Line Manager, and Contingent Worker roles. Abstract roles are assigned to user automatically when some event occurs like Hire an employee, terminate an employee or Promote an employee.
- 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.
- Examples: Enterprise Resource Planning Self Service User and Project Team Member

Role 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.
- 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.

Security configuration cases

Missing Enterprise Jobs

If jobs exist in your enterprise that aren't represented in the security reference implementation, then you can create your own job roles. Add privileges, aggregate privileges, or duty roles to custom job roles, as appropriate.

Predefined Roles with Different Privileges

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

Predefined Roles with Missing Privileges

If the privileges for a job aren't defined in the security reference implementation, then you can create your own duty roles. However, a typical implementation doesn't use custom duty roles. You can't create aggregate privileges.

Role Name & Role Code

Role name	Role code
Accounts Payable Manager	**ORA_AP_ACCOUNTS_PAYABLE_MANAGER_JOB**
can be duplicated	**cannot be duplicated**

Security console

is a centralized tool that empowers administrators to manage security across various Oracle Fusion Applications and services. It encompasses a plethora of security-related tasks such as user provisioning, role management, access policies, authentication, and authorization settings.

You must have the **IT Security Manager role** to use the Security Console. This role inherits the Security Management and Security Reporting duty roles.

Security Console Tasks

Roles

- Create job, abstract, and duty roles.
- Edit custom roles.
- Copy roles
- Compare roles.
- Visualize role hierarchies and assignments to users.
- Review Navigator menu items available to roles or users.
- Identify roles that grant access to Navigator menu items and privileges required for that access.

Users

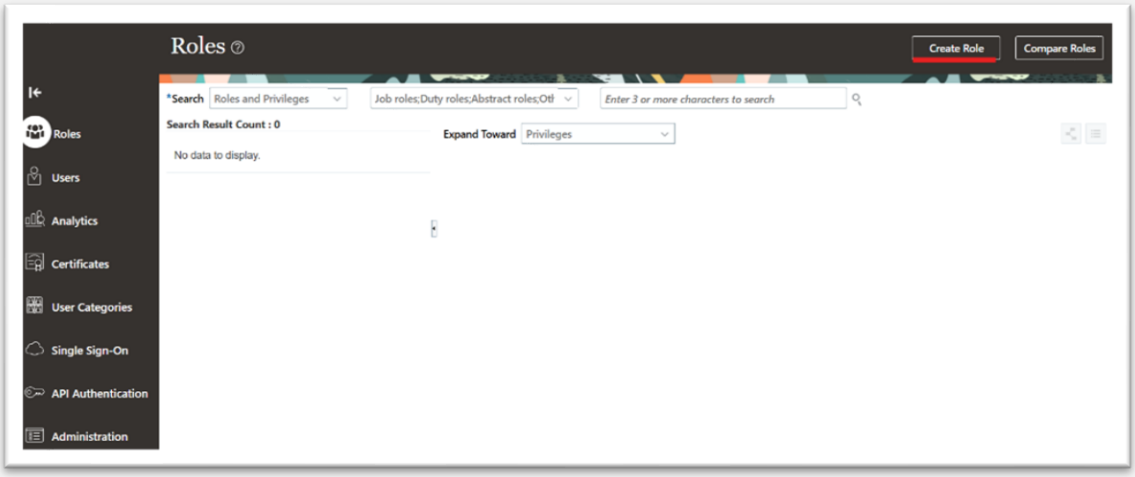
- Create user accounts.
- Review, edit, lock, or delete existing user accounts.
- Assign roles to user accounts.
- Reset users' passwords.

Roles

Create the Custom Role

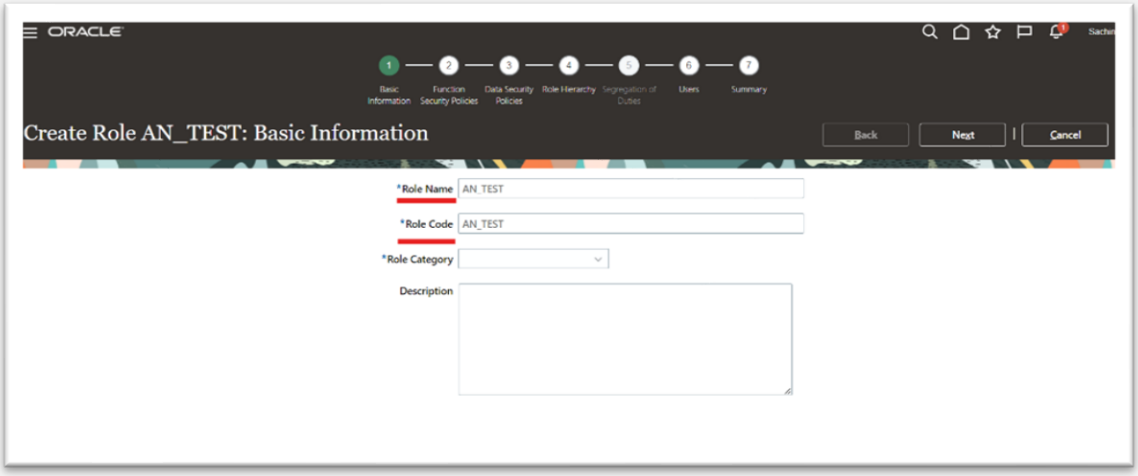
You can create a duty role, job role, or an abstract role using the Security Console.

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.

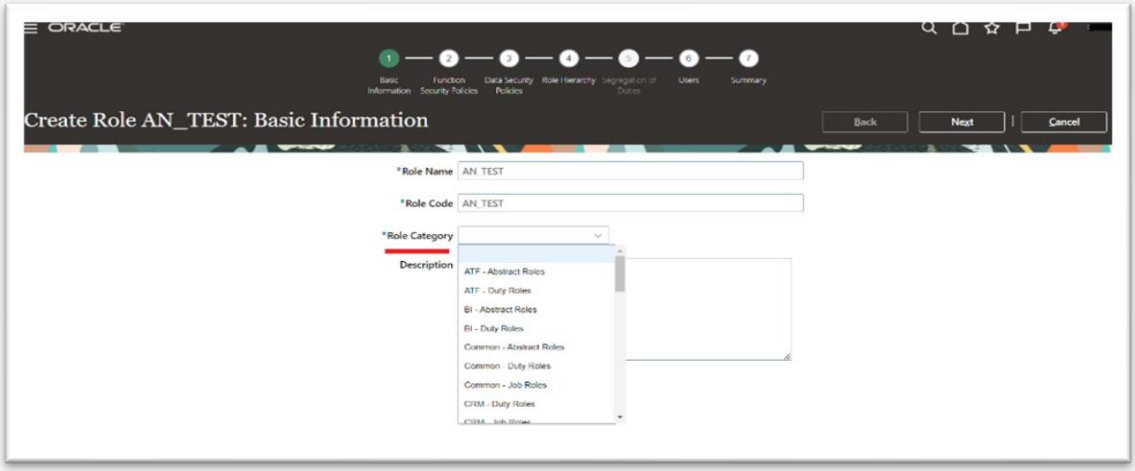
Enter values in a series of role-creation pages, selecting Next or Back to navigate among them.



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 can't 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 can't assign the role you're 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.

Note: You can't change the role category for existing roles.

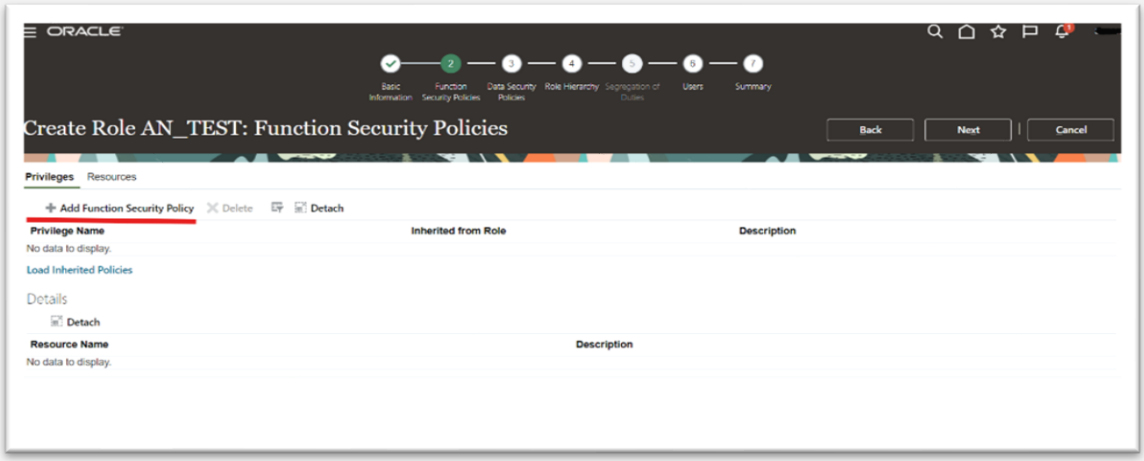
4. Optionally, describe **the role in the Description** field.

A Function Security policy selects a set of functional privileges, each of which permits use of a field or other user-interface feature. On a Function Security Policies page, you may define a policy for:

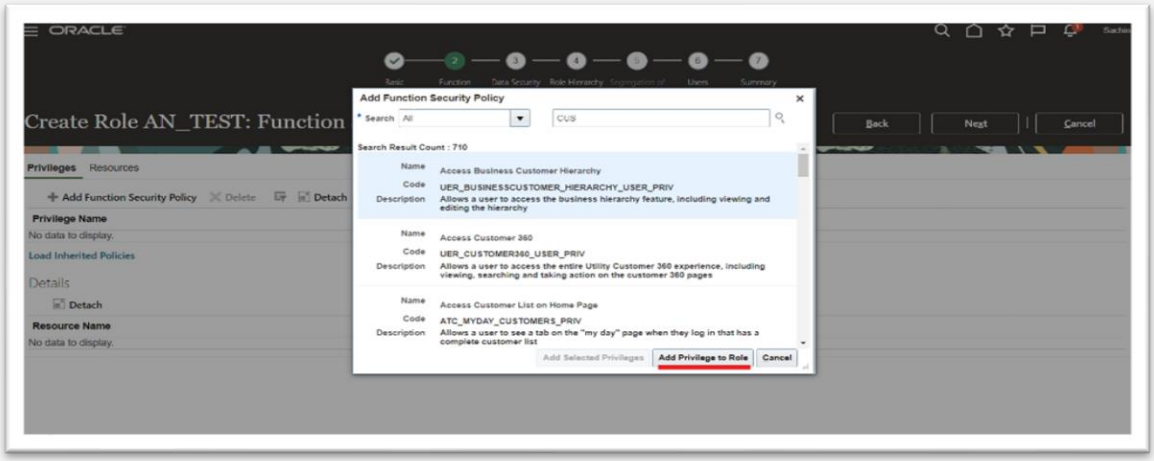
- **A duty role**. In this case, the policy selects functional privileges that may be inherited by duty, job, or abstract roles to which the duty is to belong.
- **A job or abstract role**. In this case, the policy selects functional privileges specific to that role.

As you define a policy, you can either add an individual privilege or copy all the privileges that belong to an existing role:

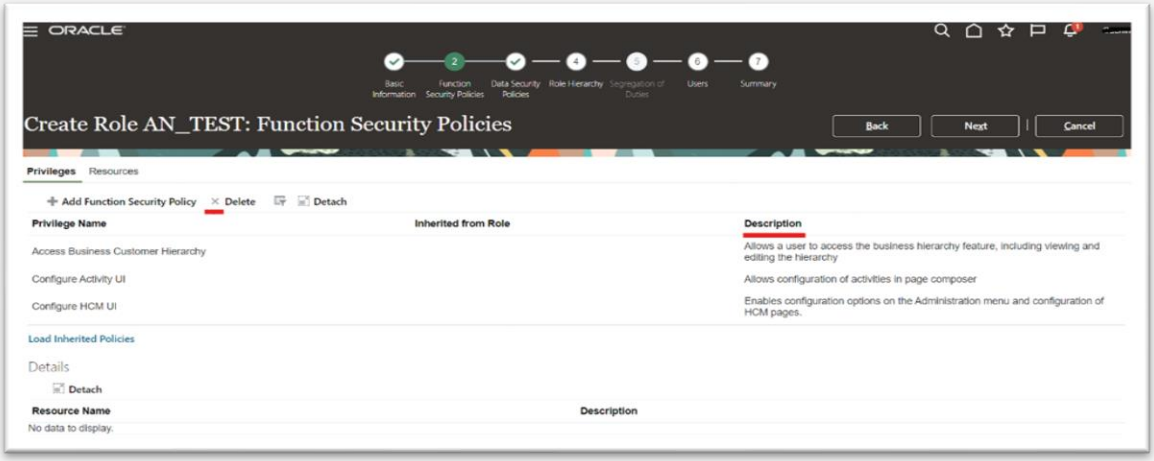
Select **Add** Function Security Policy.



Search with Privilege and click on Add Privilege to Role

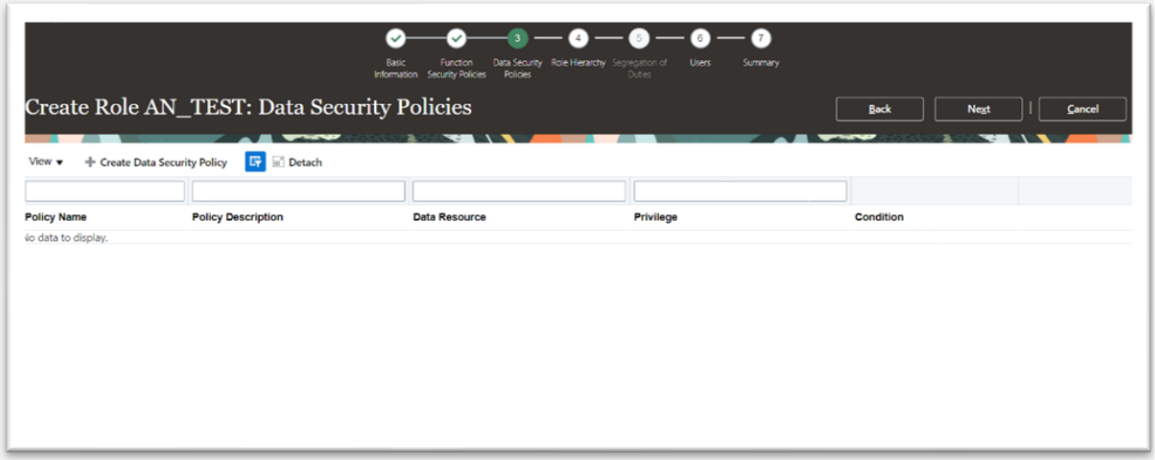


- In the Search field, select the value Privileges or types of role in any combination and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.
- Select a privilege or role. If you select a privilege, click Add Privilege to Role. If you select a role, click Add Selected Privileges.
- Note: The search results display all roles, whether they contain privileges or not. If a role doesn't contain privileges, there's nothing to add here. To add roles that don't contain privileges, go to the Role Hierarchy page.



The Function Security Policies page lists all selected privileges. When appropriate, it also lists the role from which a privilege is inherited. You can:

- Click a privilege to view details of the code resource it secures.
- **Delete** a privilege. You may, for example, have added the privileges associated with a role. If you want to use only some of them, you must delete the rest. To delete a privilege, click its x icon.

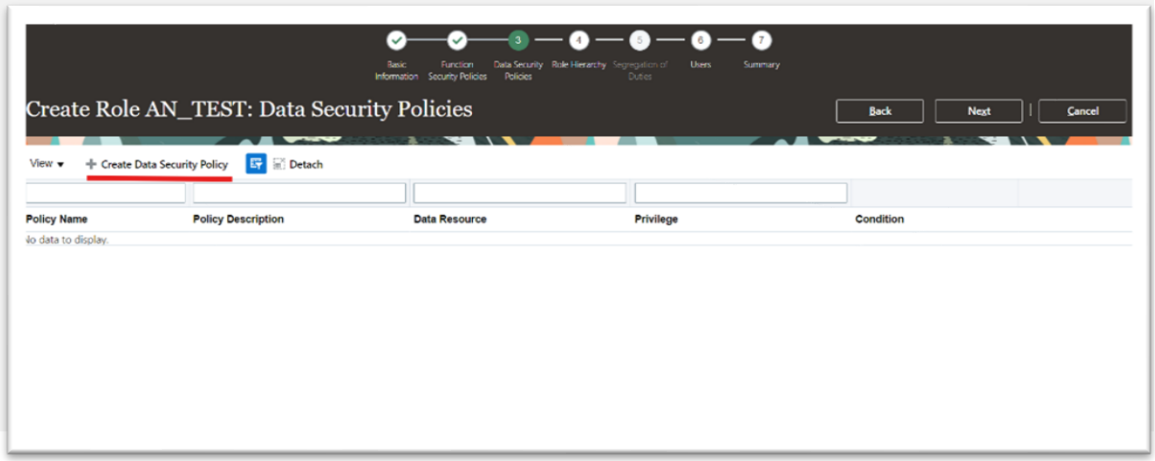


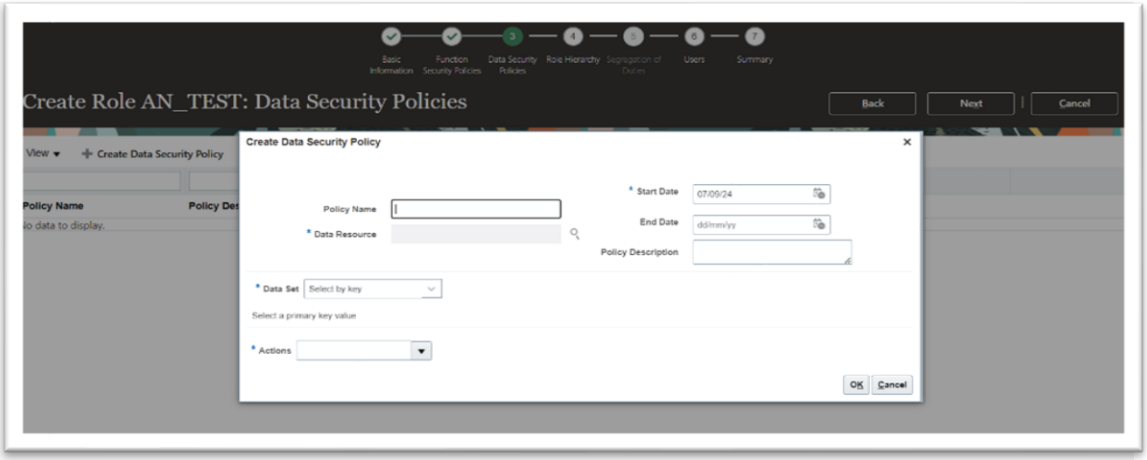
A **data security policy** may be explicit or implicit.

- An explicit policy grants access to a particular set of data, such as that pertaining to a particular business unit. This type of policy isn't used in predefined roles in Oracle Fusion Cloud ERP.
- An implicit policy applies a data privilege (such as read) to a set of data from a specified data resource. Create this type of policy for a duty, job, or abstract role. For each implicit policy, you must grant at least the read and view privileges.

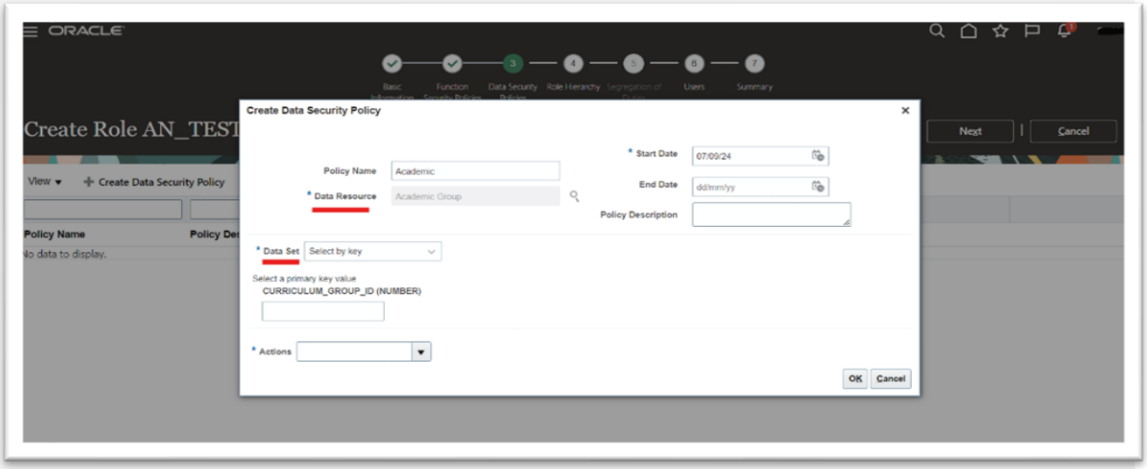
You can use a Data Security Policies page to manage implicit policies.

To create a data security policy, click the **Create Data Security Policy** button

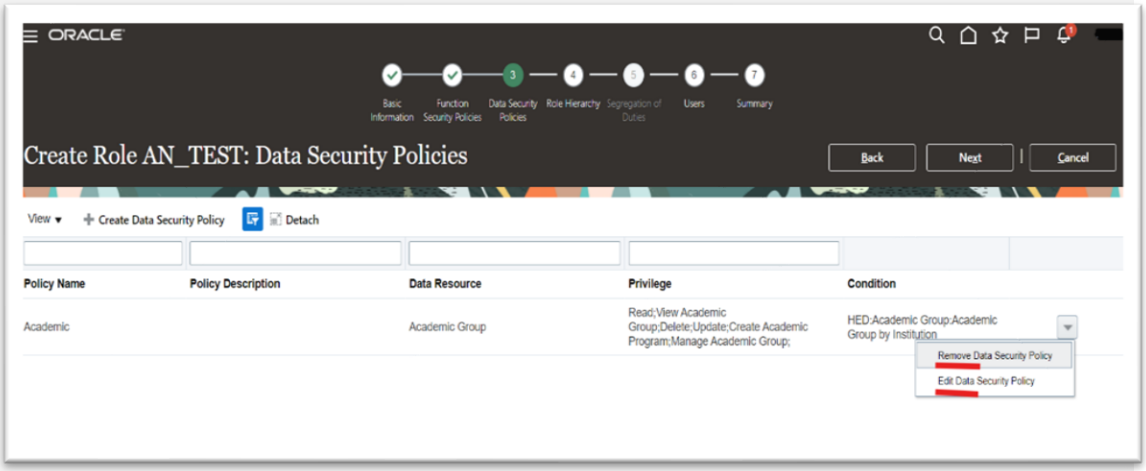




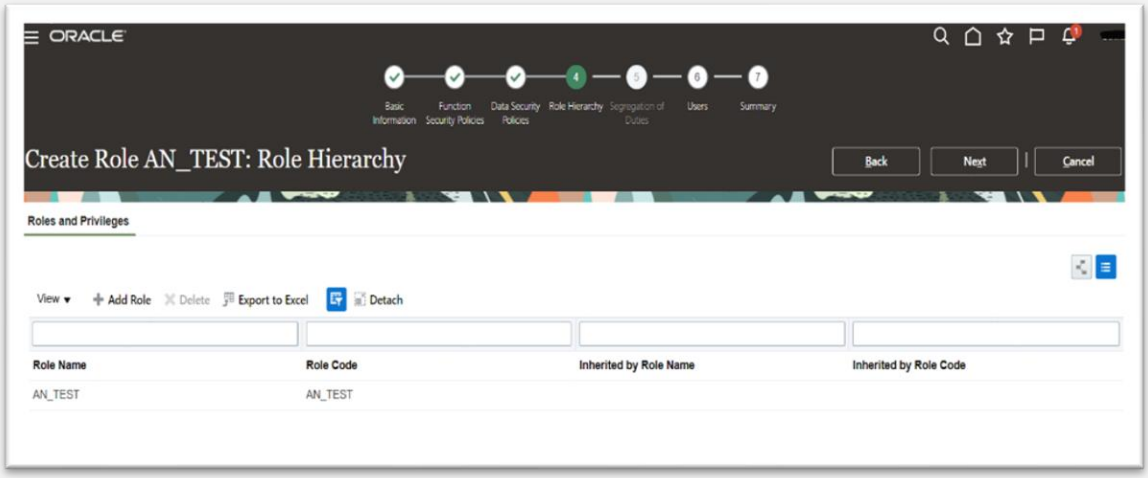
then enter values that define the policy. A start date is required; a name, an end date, and a description are optional Values that define the data access include:



- Data Resource: A database table.
- Data Set: A definition that selects a subset of the data made available by the data resource.
    - Select by **key**. Choose a primary key value, to limit the data set to a record in the data resource whose primary key matches the value you select.
    - Select by **instance set**. Choose a condition that defines a subset of the data in the data resource. Conditions vary by resource.
    - **All values**: Include all data from the data resource in your data set.
- Actions: Select one or more data privileges to apply to the data set you have defined.

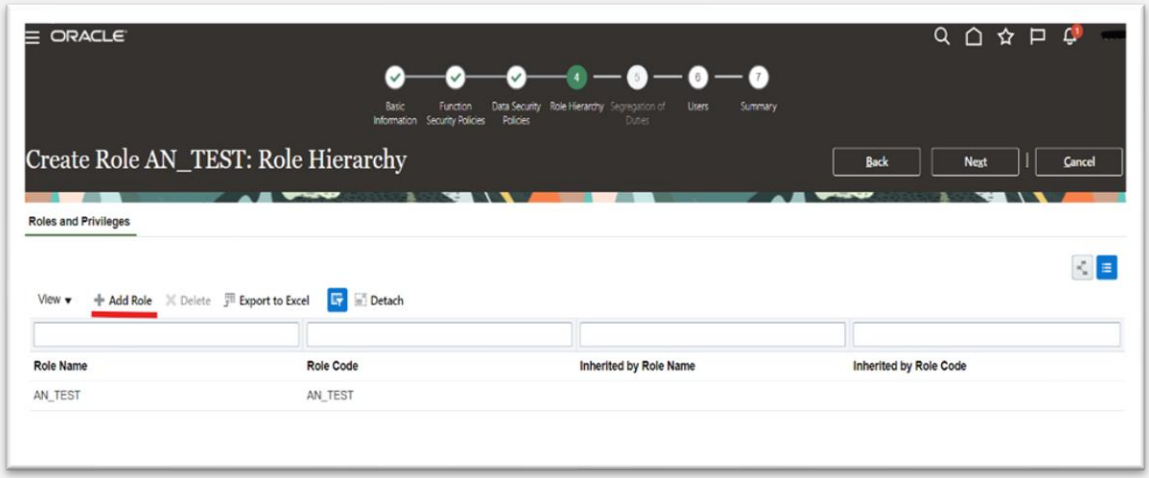


The Data Security Polices page lists all policies defined for the role. You can edit or delete a policy: click the Actions button, and select the Edit or Remove option.



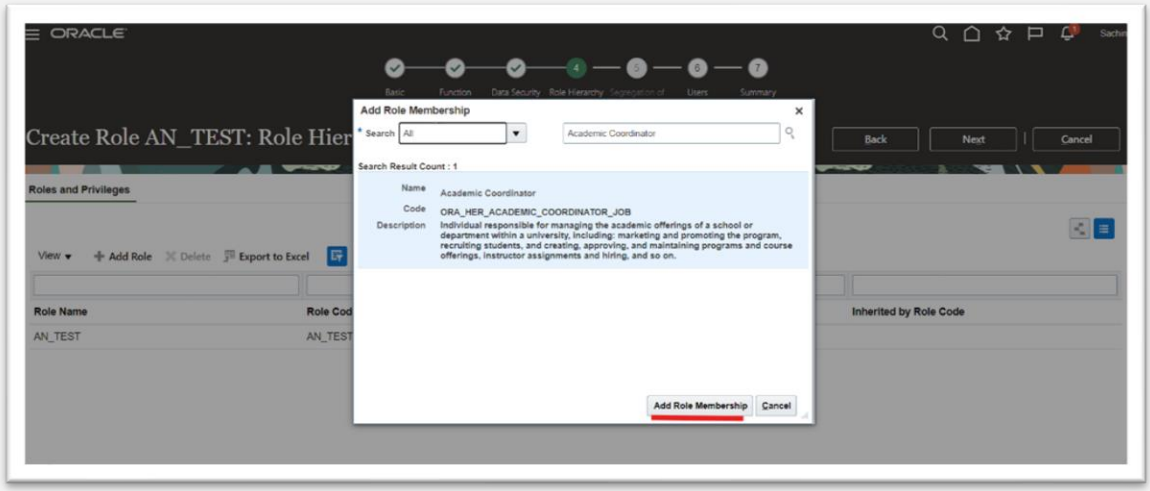
A **Role Hierarchy page** displays either a visualization graph, with the role you're creating as its focus, or a visualization table. Select the Show Graph button or View as Table button to select between them. In either case, link the role you're creating to other roles from which it's to inherit function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

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

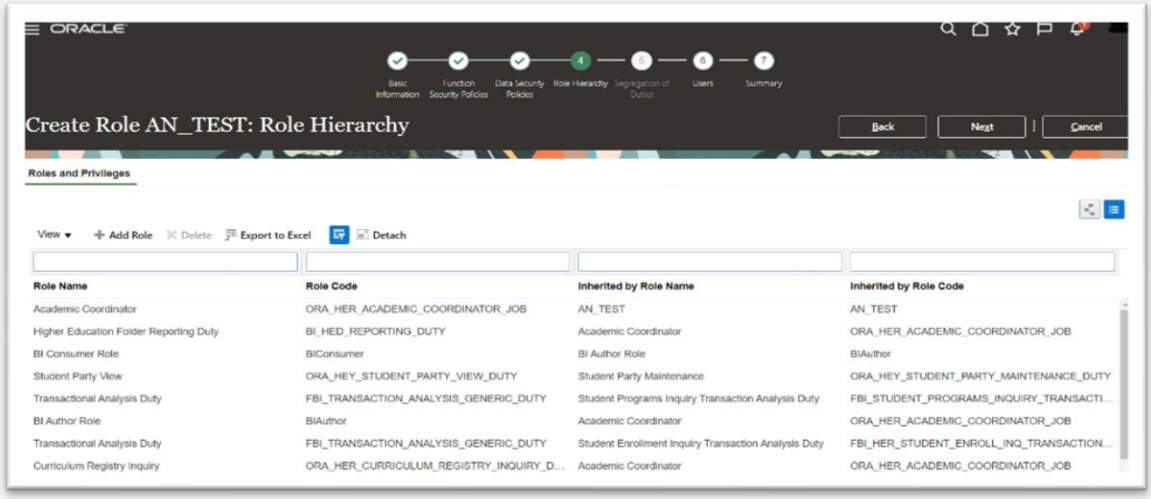


To add a role:

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.

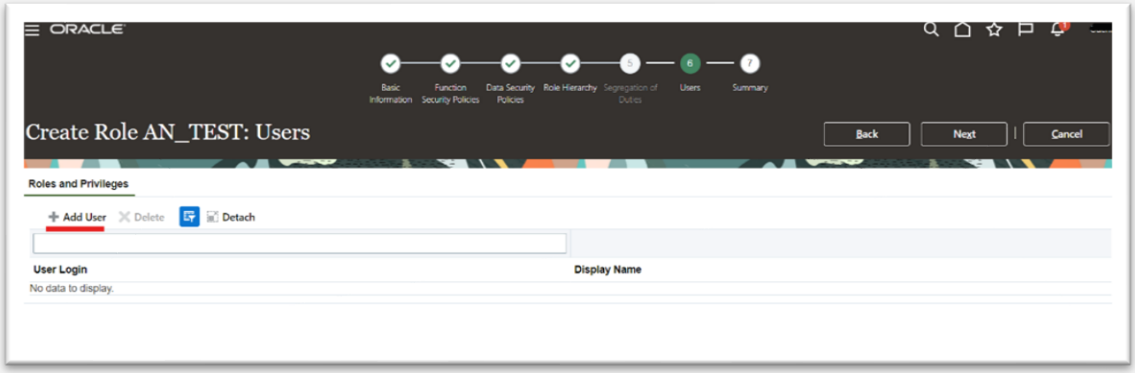


In the graph view, you can use the visualization Control Panel, Legend, and Overview tools to manipulate the nodes that define your role hierarchy.

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

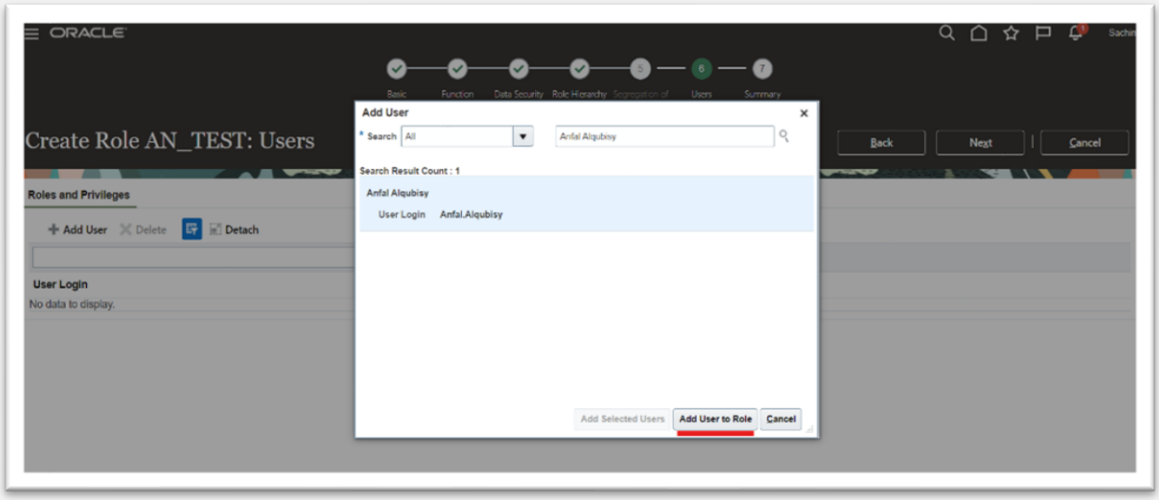
To add a user:

1. Select Add User.

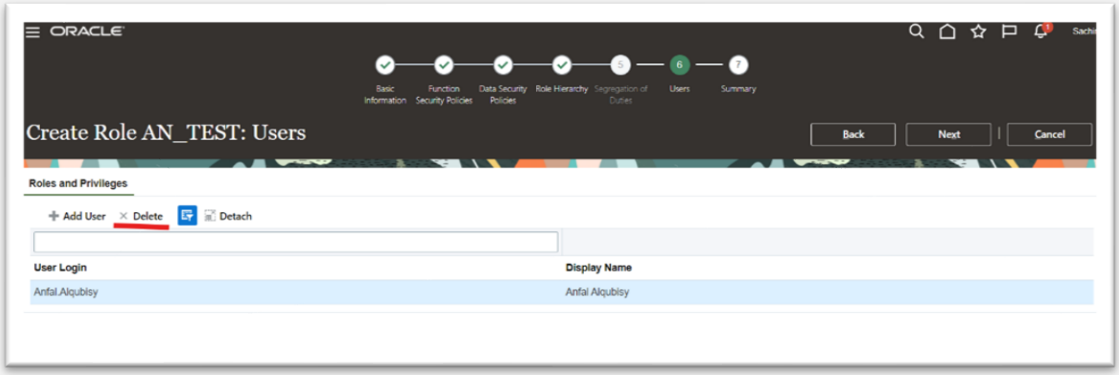


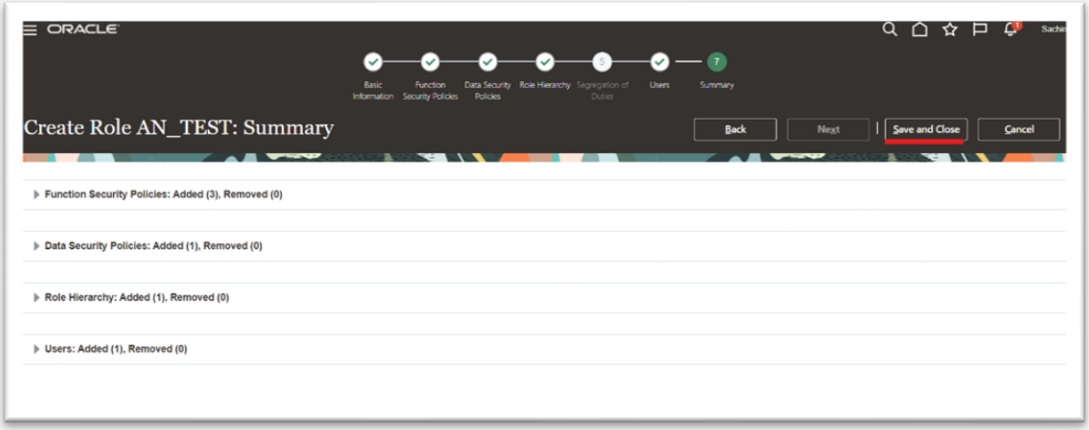
2. In a Search field, select the value Users or types of role in any combination and enter at least three characters. The search returns values including items of the type you selected, whose names contain the characters you entered.

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're creating.



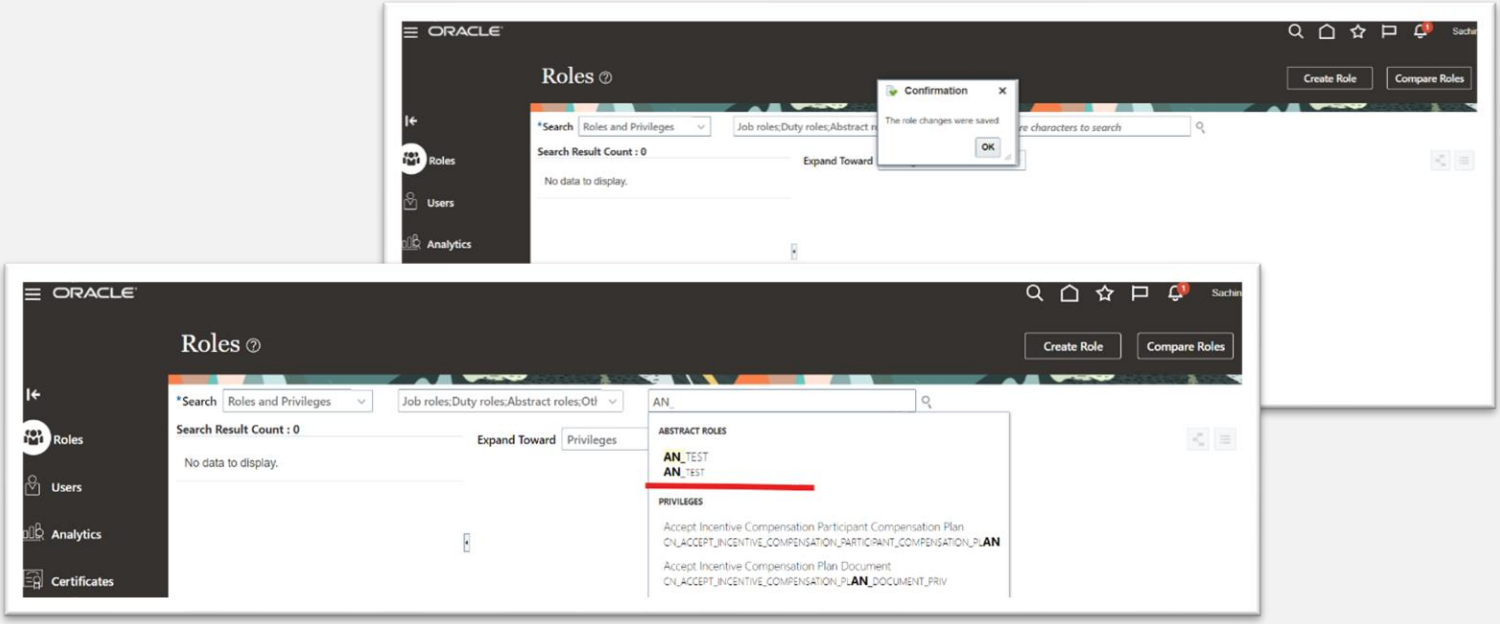
The Users page lists all selected users. You can delete a user. You may, for example, have added all the users associated with a role. If you want to assign your new role only to some of them, you must delete the rest. To delete a user, click its x icon.



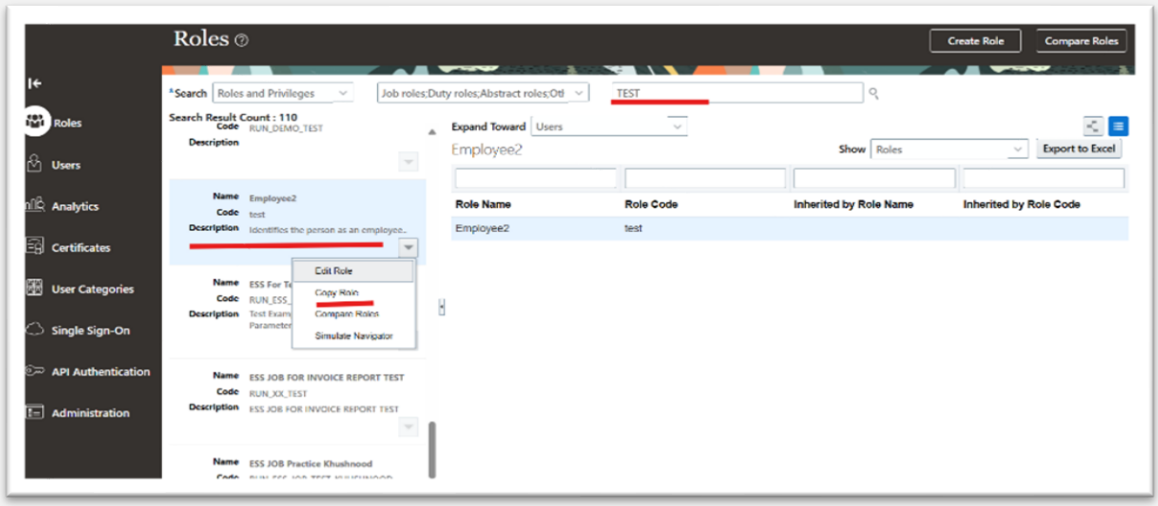


On a Summary and Impact Report page, review the selections you have made. Summary listings show the numbers of function security policies, data security policies, roles, and users you have added and removed. An Impact listing shows the number of roles and users affected by your changes. Expand any of these listings to see names of policies, roles, or users included in its counts.

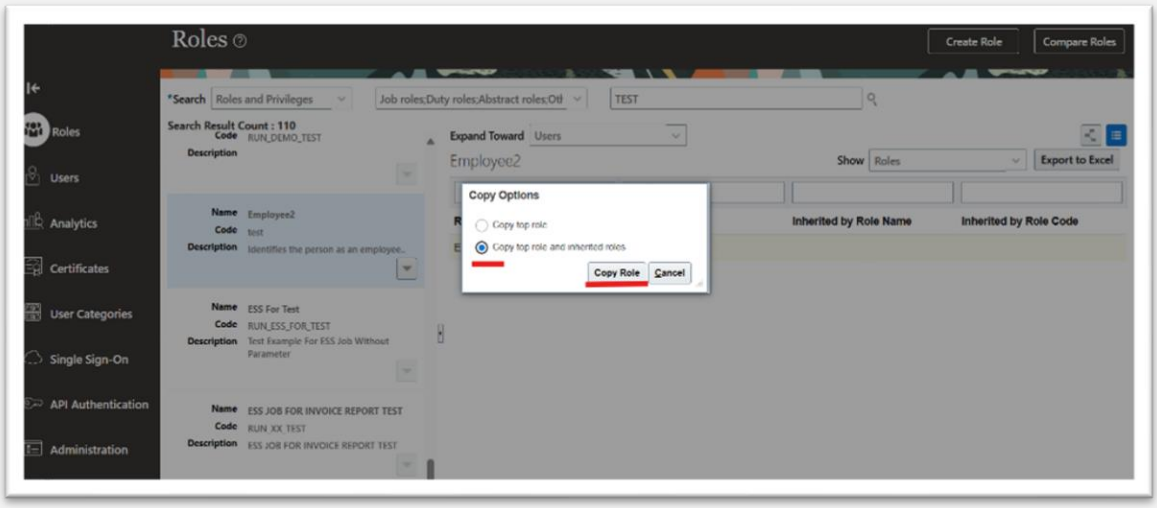
If you determine you must make changes, navigate back to the appropriate page and do so. If you're satisfied with the role, select Save and Close.



Role Copying or Editing



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're copying a role, select one of two options in a Copy Option dialog:

- **Copy top 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 top 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. Essentially, you follow the same process in editing a role as you would follow 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 can't:

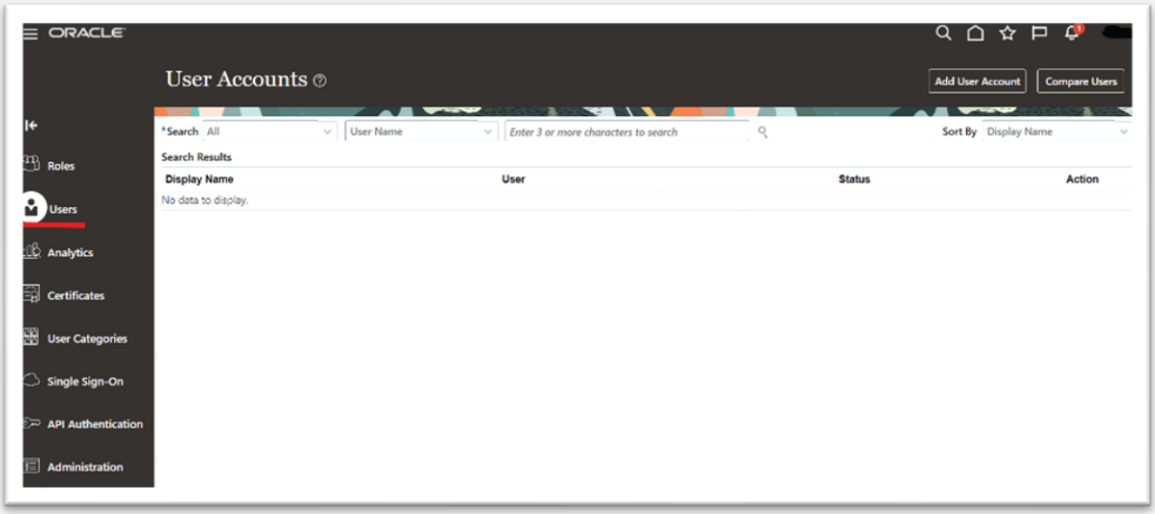
- Modify, add, or remove function security policies.
- Modify or remove data security policies provided by Oracle.
- Modify the role hierarchy.

The **Predefined role** check box is cleared if you're editing a custom role or if you have copied a role. In that case, you can make any changes to role components.

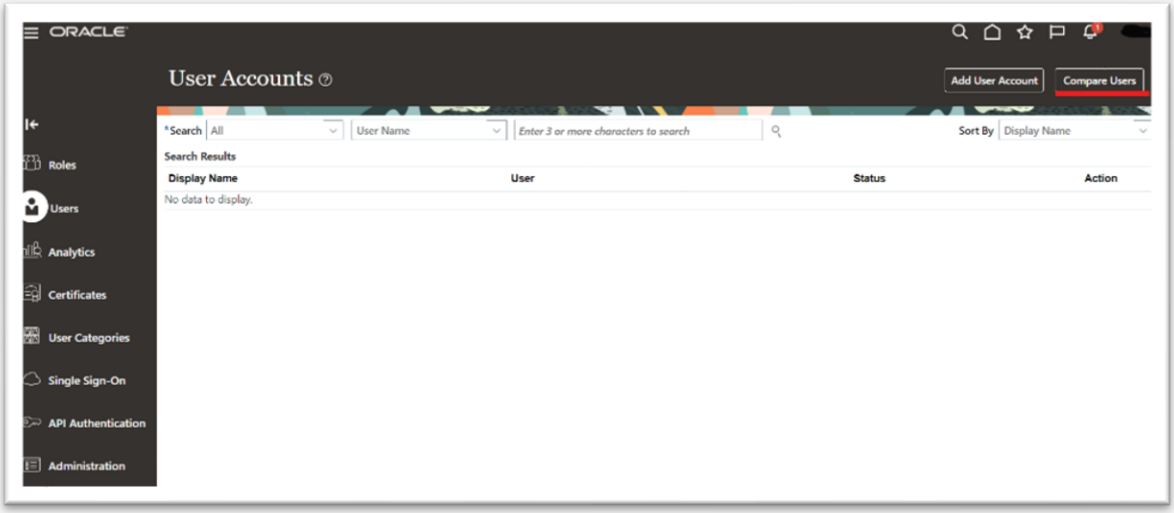
- By default, the name and code of a copied role match the source role's, except a prefix, suffix, or both are appended. In the Roles Administration page, you can configure the default prefix and suffix for each value.
- A copied role can't inherit users from a source job or abstract role. You must select 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 Status tab of the Administration page.

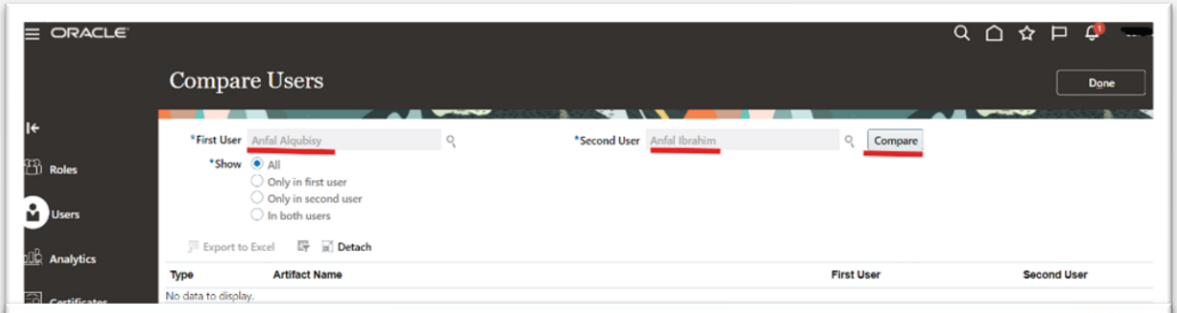
Compare Users



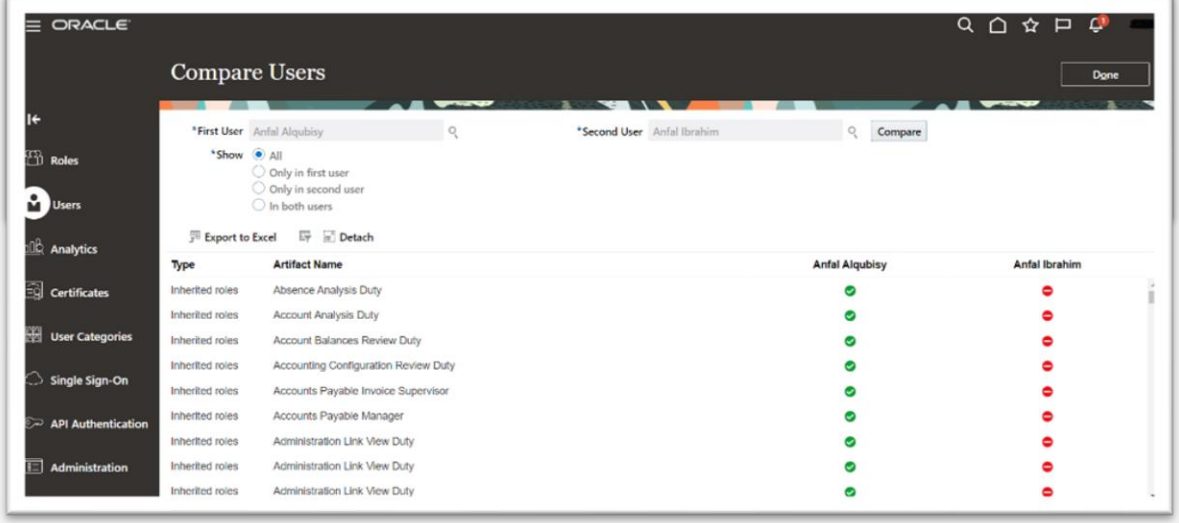
On the Security Console, click Users.



Click **Compare Users**.



Search for and select both users one after another.



Click **Compare**.
All the details of both the users are displayed.

Identify roles that grant access to Navigator menu items and privileges required for that access

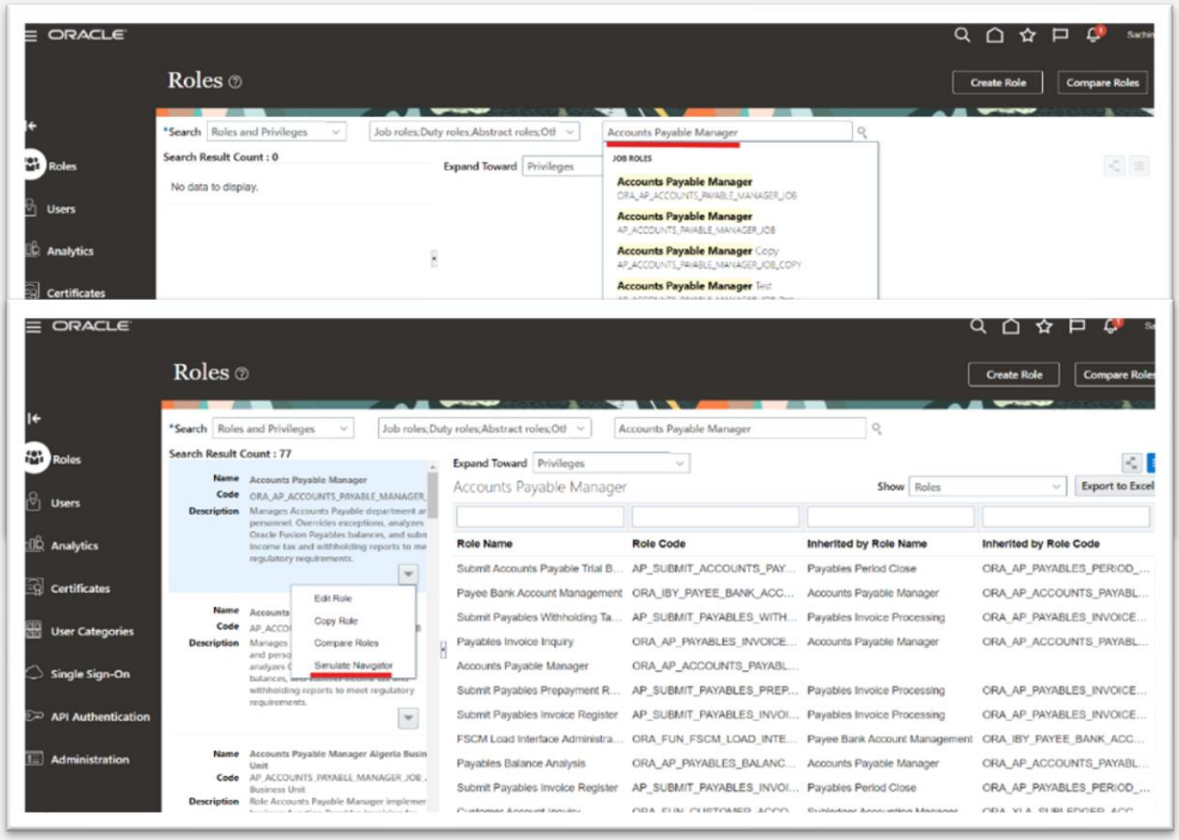
Simulate Navigator

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

Select the Roles tab in **the Security Console**.

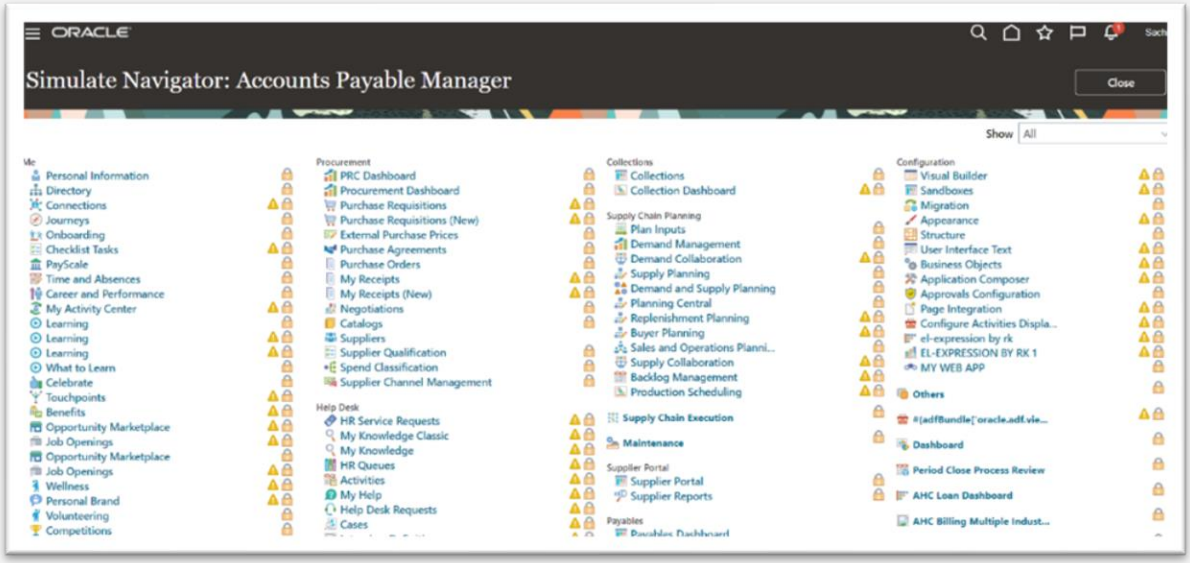
Select

Simulate Navigator



In a Simulate Navigator page:

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



In either view:

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

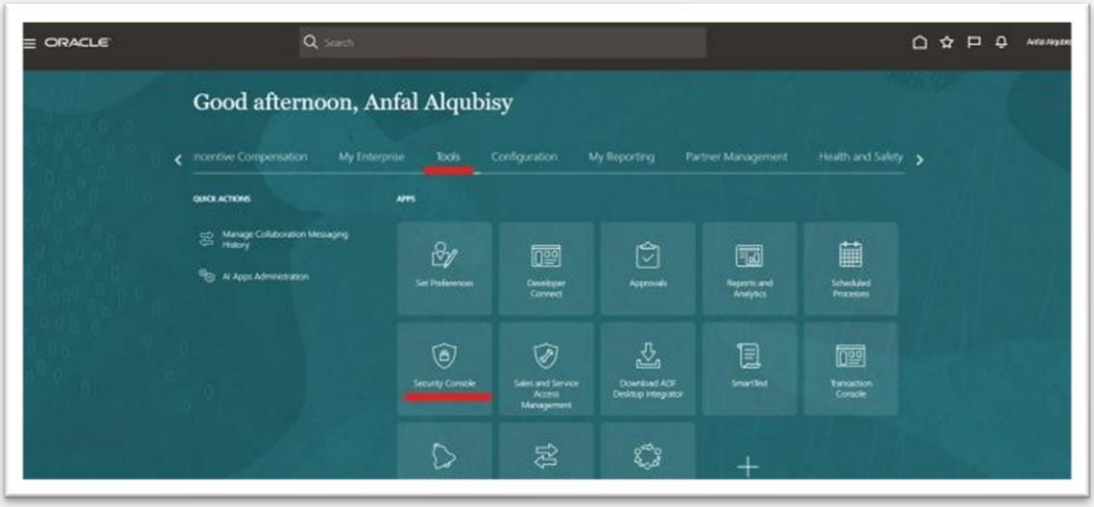
To plan how this authorization may be altered

1. Click any menu item on the Simulate Navigator page.
2. Select either of the two options:
    - **View Roles That Grant Access**: Lists roles that grant access to the menu item.
    - **View Privileges Required for Menu**: Lists privileges required for access to the menu item. Lists privileges required for access to the task panel items.

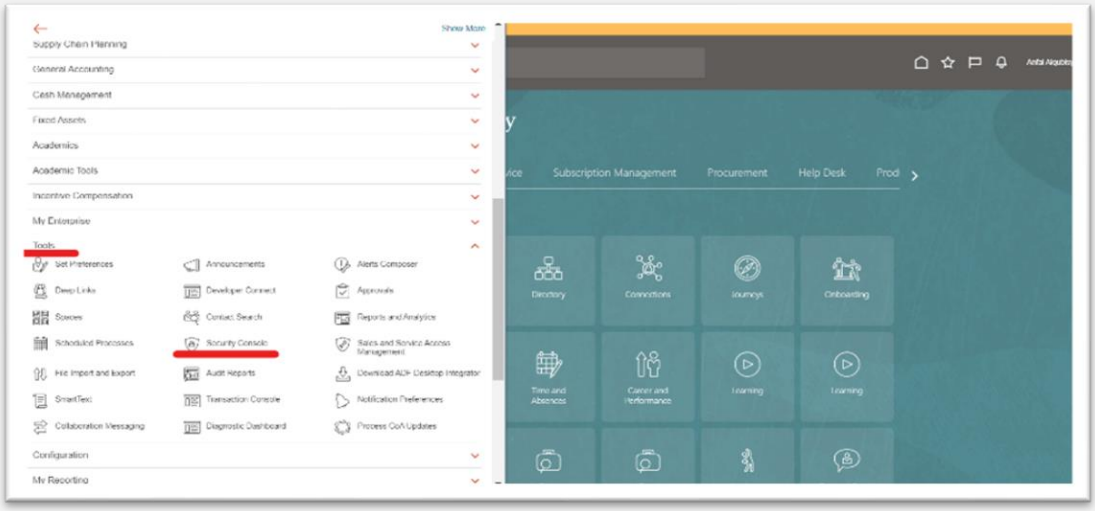
Users

Create user accounts.

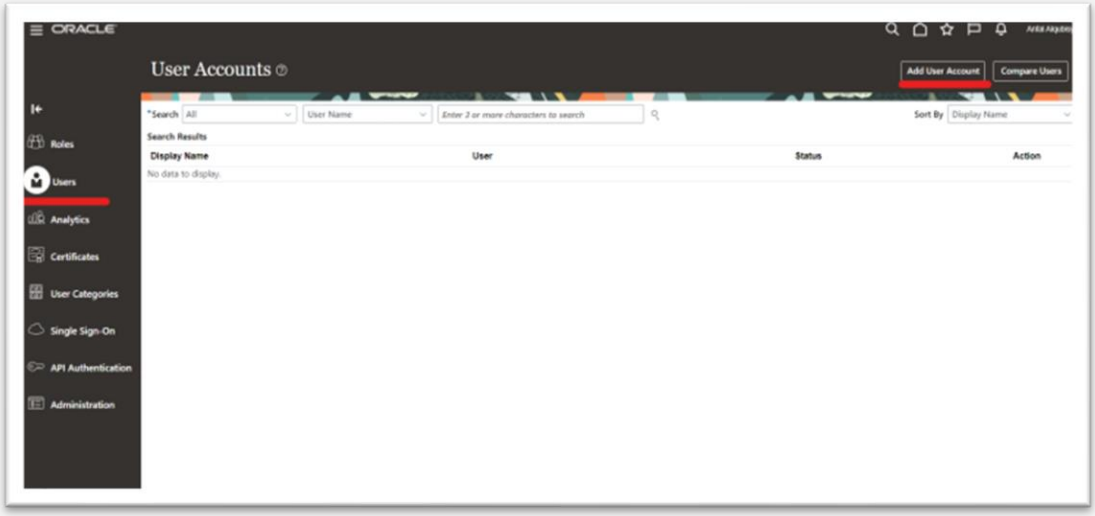
Home Page >> Tools >> Security Console



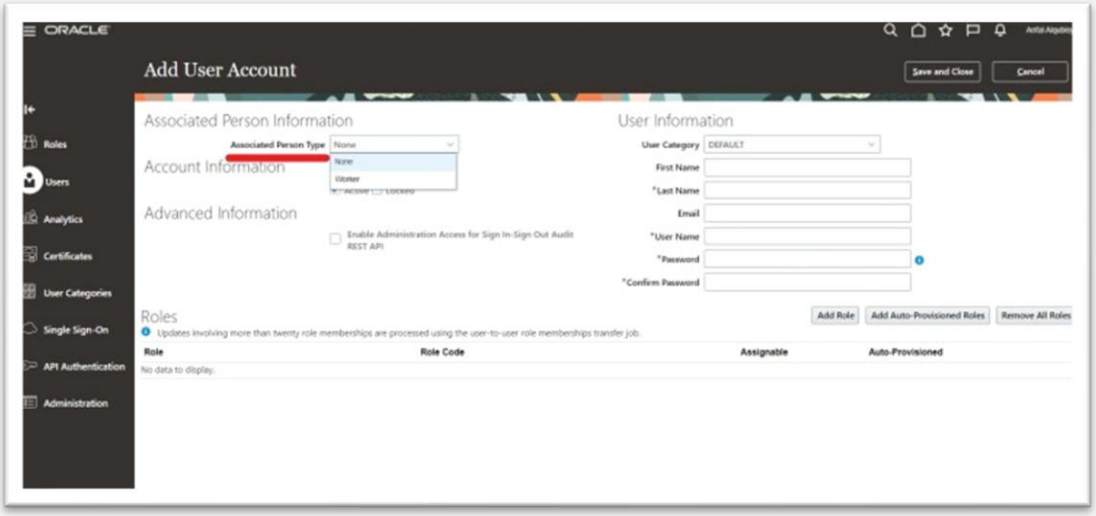
Or: Navigator>> Tools >> Security Console



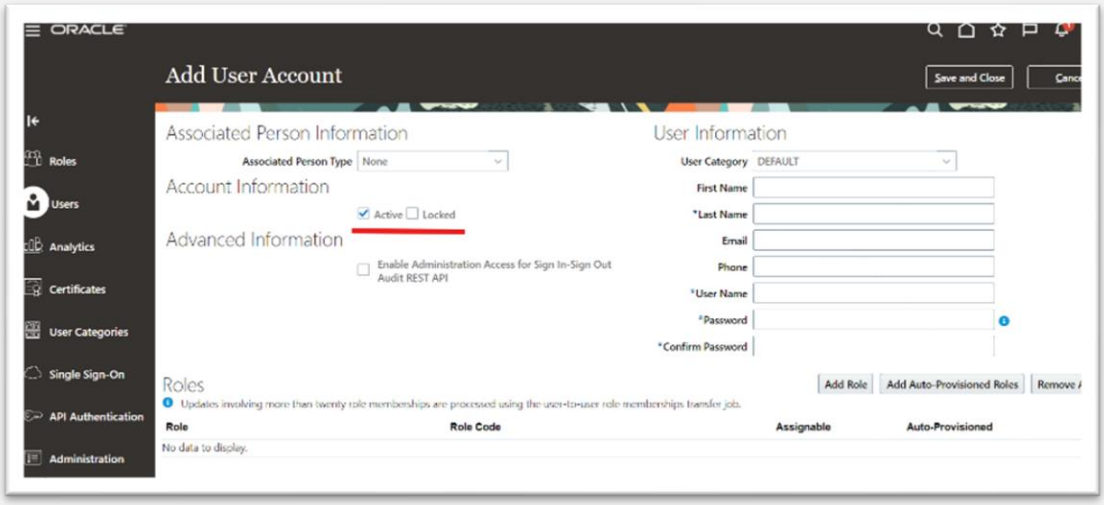
In the Security Console, click the Users tab.



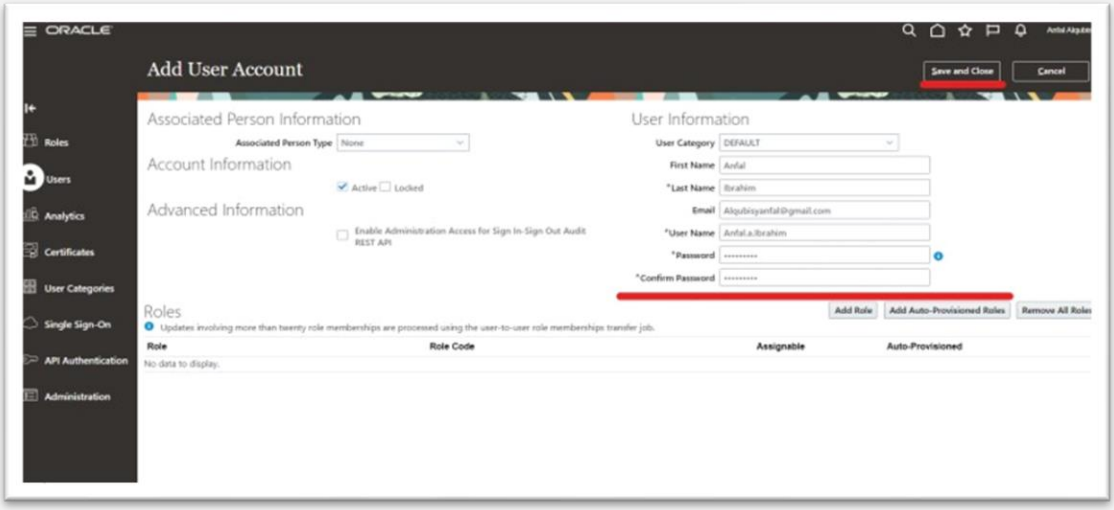
On the User Accounts page, click the Add User Account button.



From the **Associated Person Type** list, select **Worker** to link this account to a worker record in HCM. Otherwise, leave it as **None**.



In the Account Information section, change the default settings if you don't want the account to be active or unlocked.



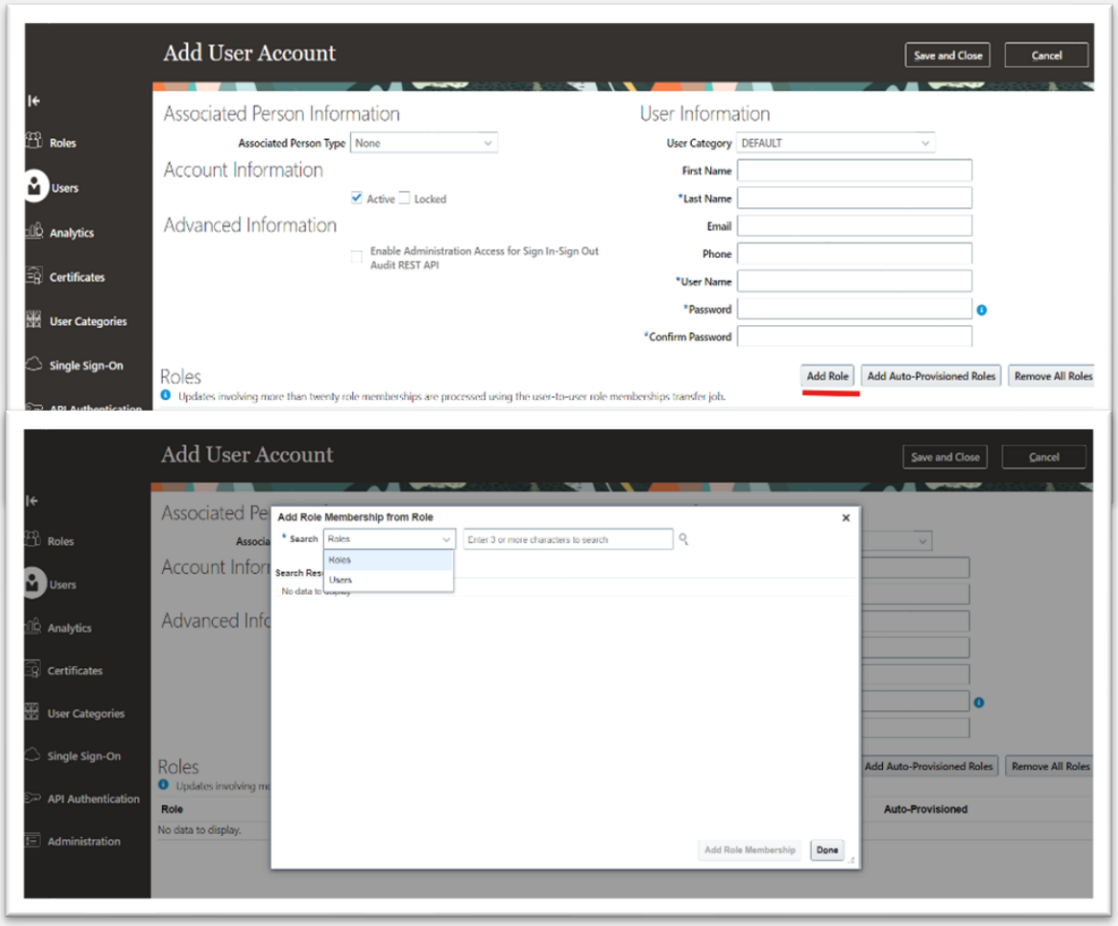
Fill in the User Information section.

- Select the user category that you want to associate the user with. The user category includes a password policy and a rule that determines how the user name is automatically generated.
- Enter the user's first name only if the rule from the selected user category makes use of the first name or the first name initial to generate user names.
- Enter a password that conforms to the password policy from the selected user category.

Assign roles to user accounts

Add Role to User

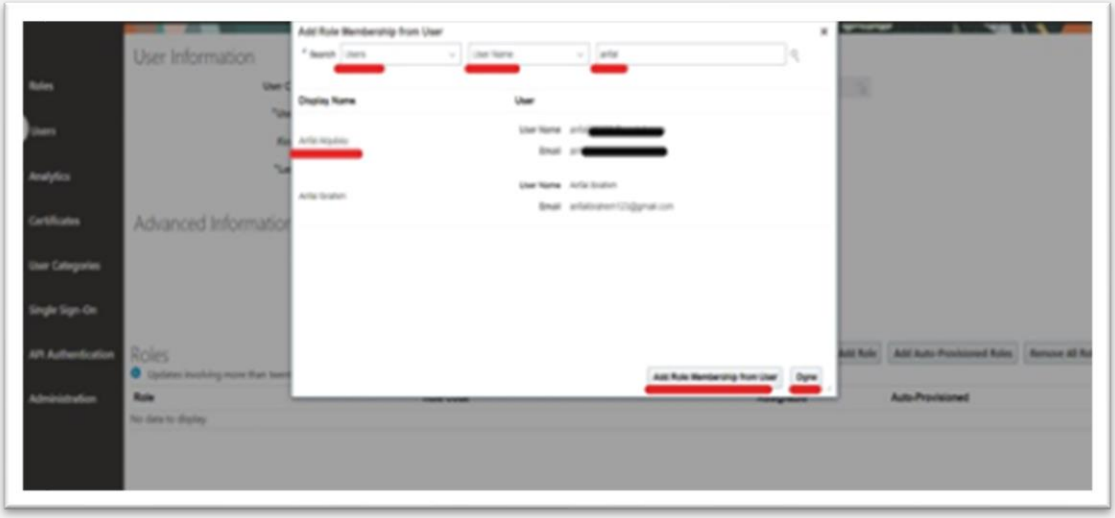
In the Roles section, click the Add Role button.



Search for the role that you want to assign to the user and the click Add Role Membership button. The role is added to the list of existing roles.

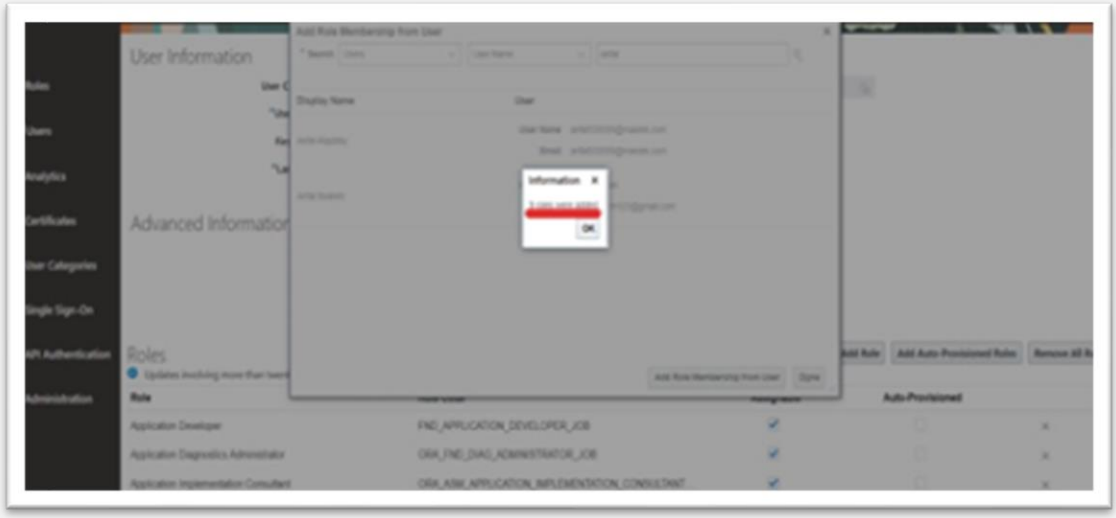
Repeat the previous step to add more roles if required, or just click Done.

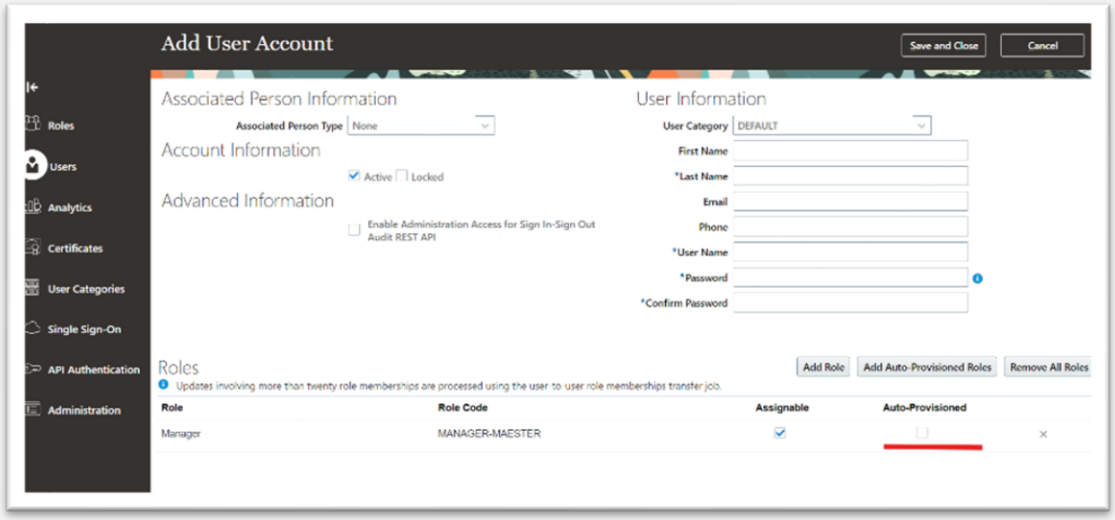
Copy Roles from One User to Another



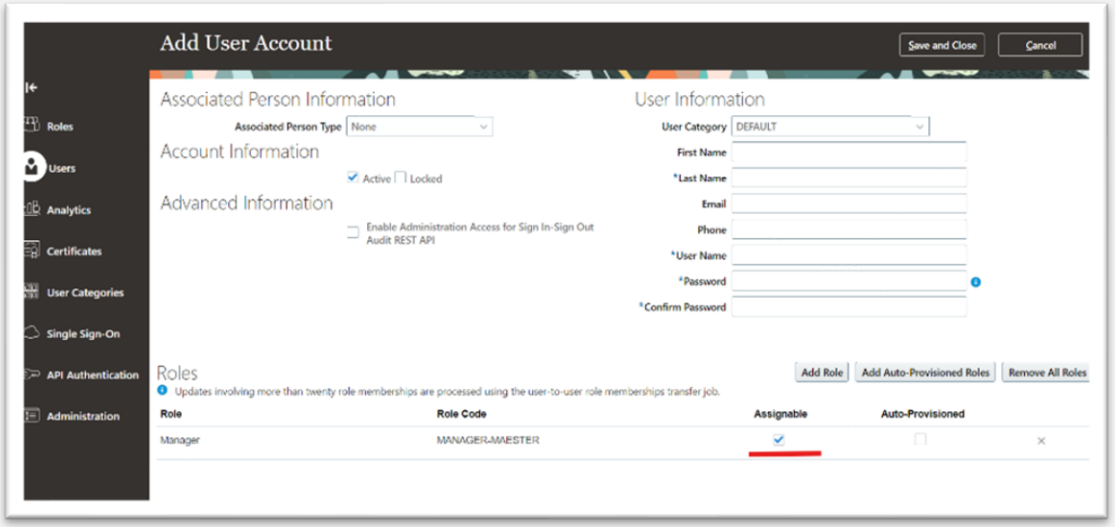
Select Users from the Search drop-down list and search for the user from which you want to copy the roles.

Select the user and click Add Role Membership from User. A confirmation message appears. Click OK and click Done.

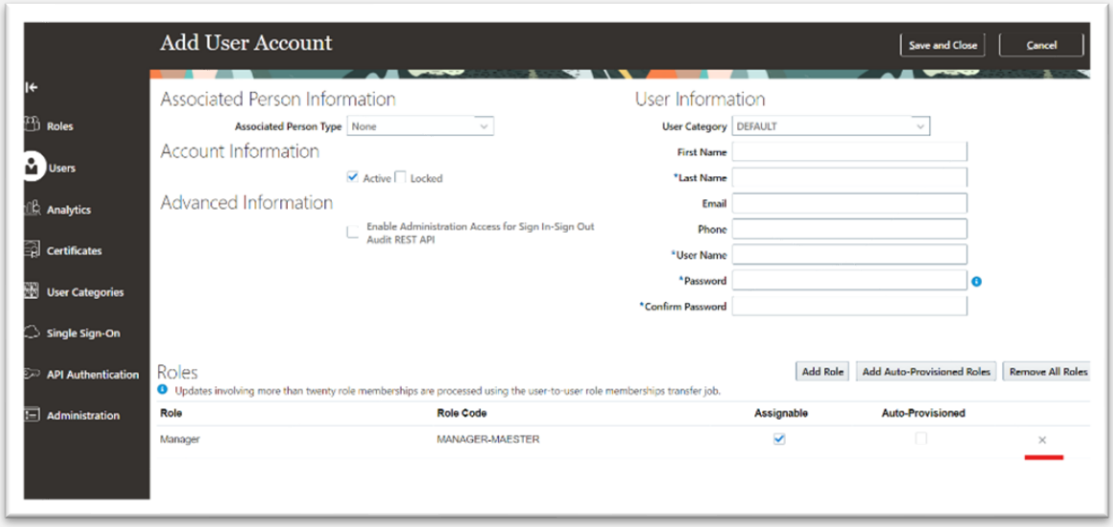




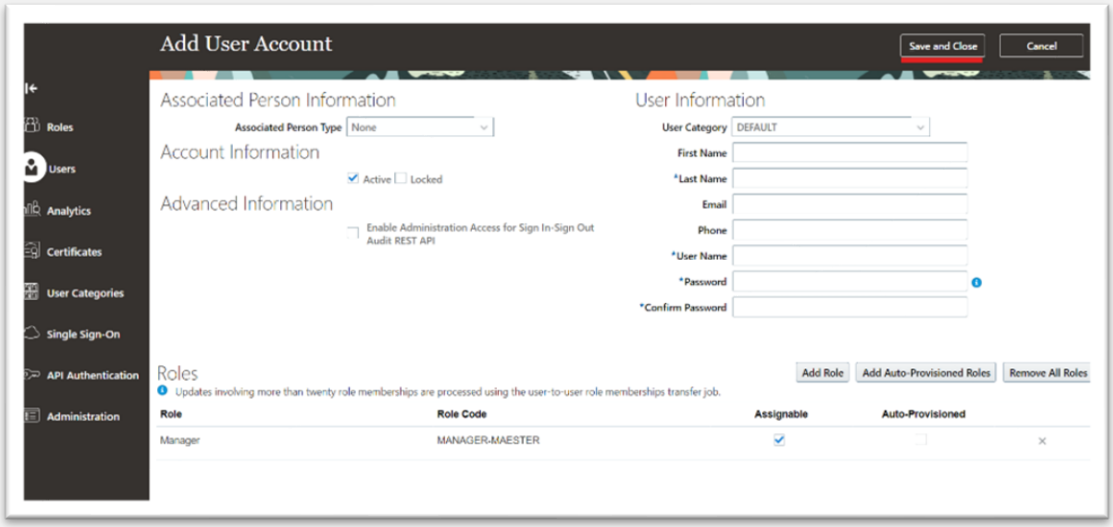
Click the Add Auto-Provisioned Roles button to add any roles that the user is eligible for, based on role provisioning rules. If nothing happens, that means there aren't any roles to autoprovision. You can add auto-provisioned roles only to users who have associated worker information.



In the Roles table, click the Assignable check box for any role that can be delegated to another user. The Auto-Provisioned column displays a tick mark if the user has roles that were assigned through autoprovisioning.



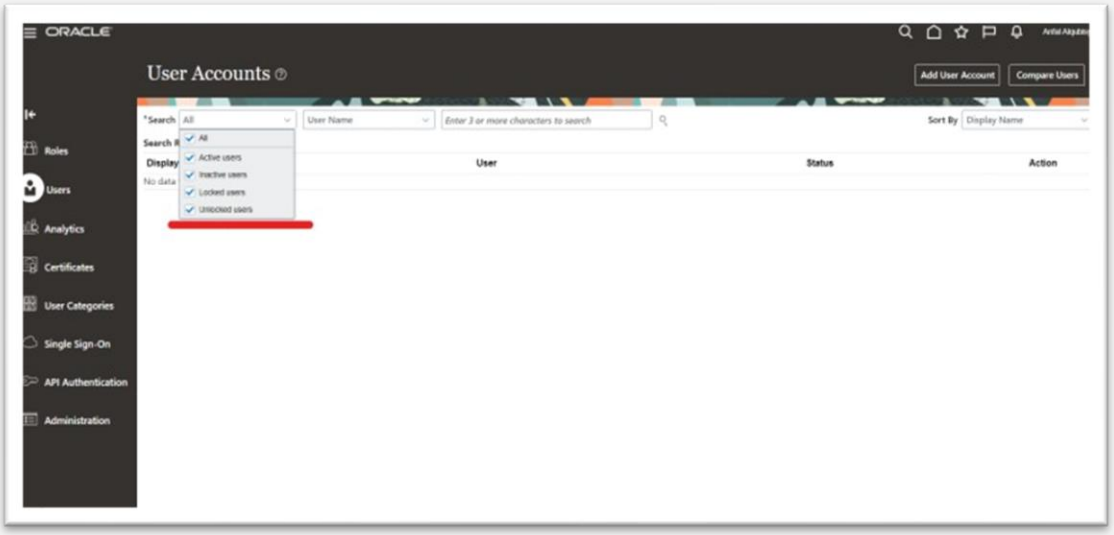
Click the Delete **icon to unassign any role.**



Click **Save** and Close.

Assign Roles to an Existing User

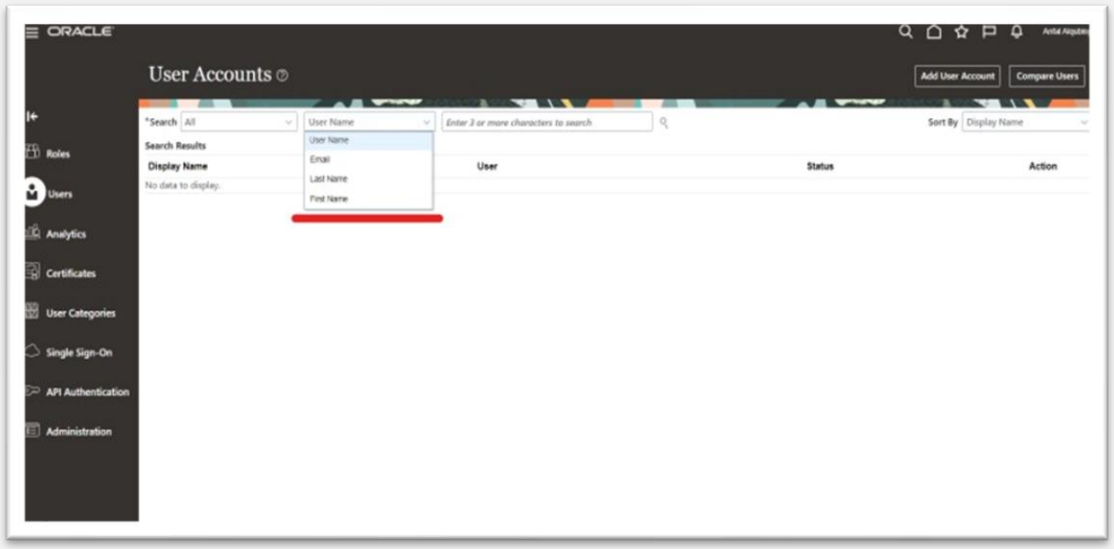
Search user



Search in

Type user:

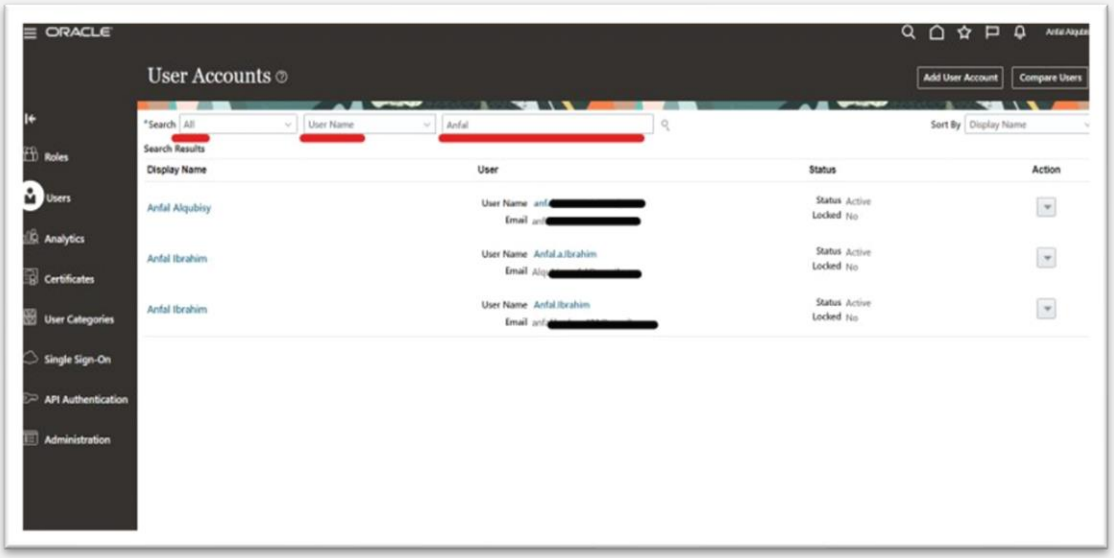
- Active users
- Inactive users
- Locked users
- Unlocked users



Select search in

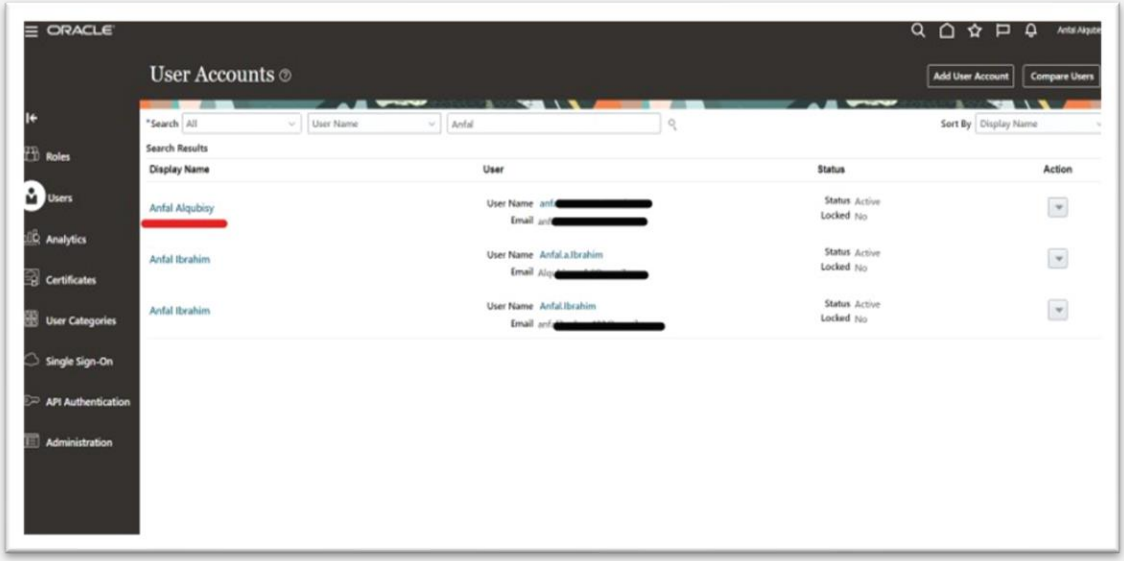
- Username
- Email
- Last Name
- First Name

Result search

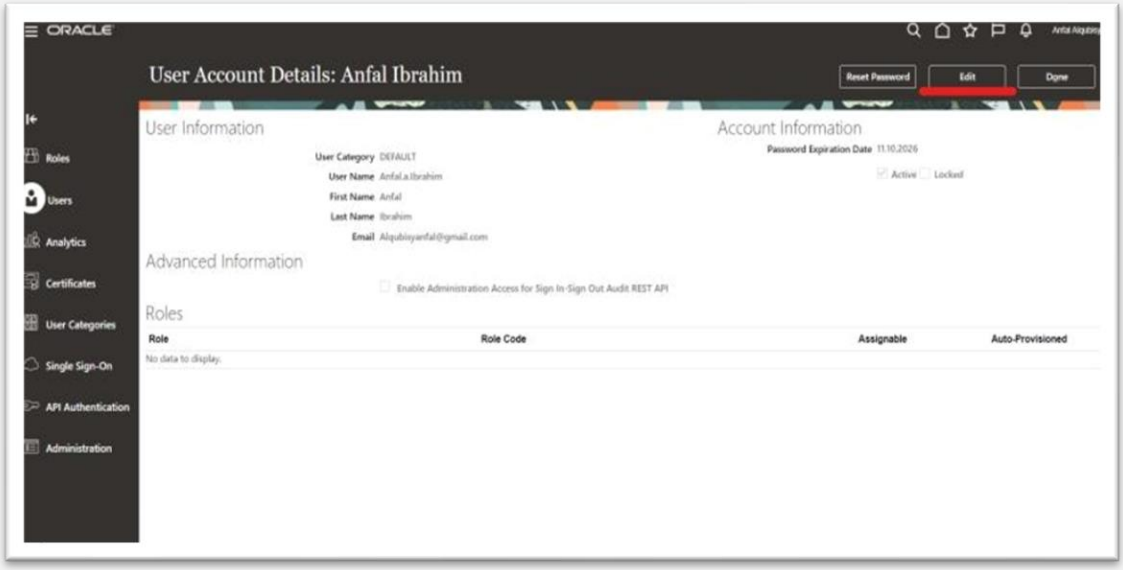


In the Security Console, click the Users tab.

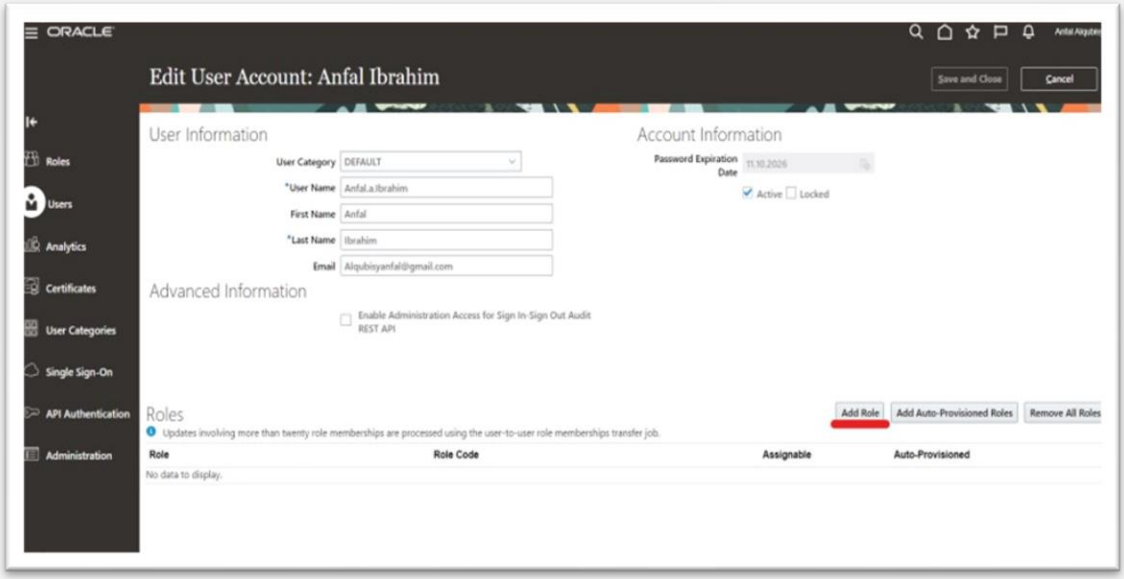
Search for and select the user you want to assign roles to



On the User Account Details page, click the **Edit** button.



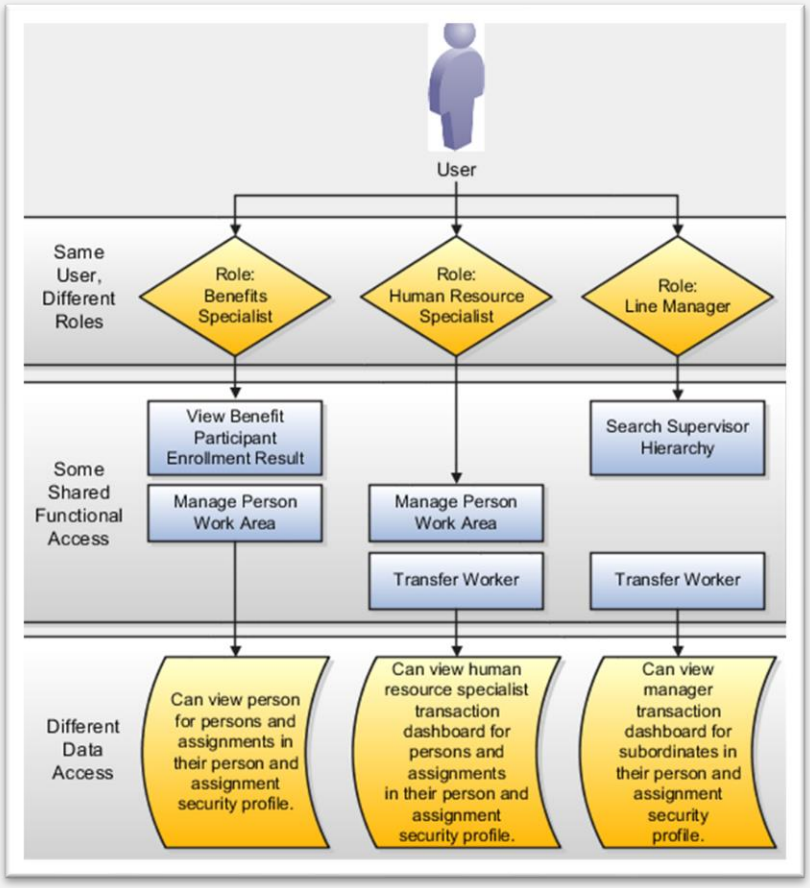
In the Roles section, click the **Add Role** button.



User With Multiple Roles

A user who fills multiple roles in the organization should be provisioned with multiple roles for security reasons so changes in responsibility can be quickly applied. The user's functional and data access is the union of grants provided by the provisioned roles.

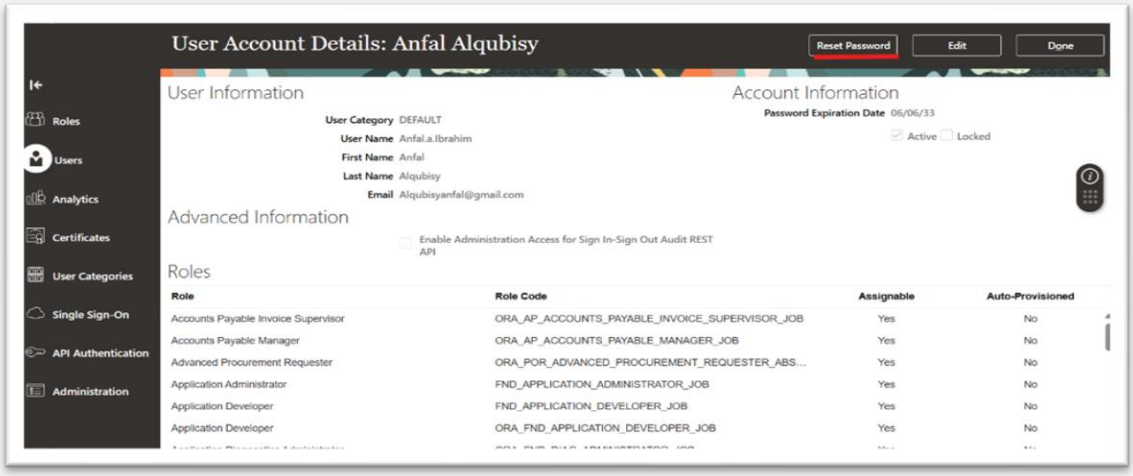
For example, a user can be provisioned with the Benefits Specialist, Human Resources Specialist, and Line Manager roles. These roles grant different, though partially overlapping, functional access, and differing data access.



Reset users' passwords

In the Security Console, click the **Users** tab.

On the User Accounts page, search for the user whose password you want to change.



In the **Reset Password** dialog box, select whether to generate the password automatically or change it manually.

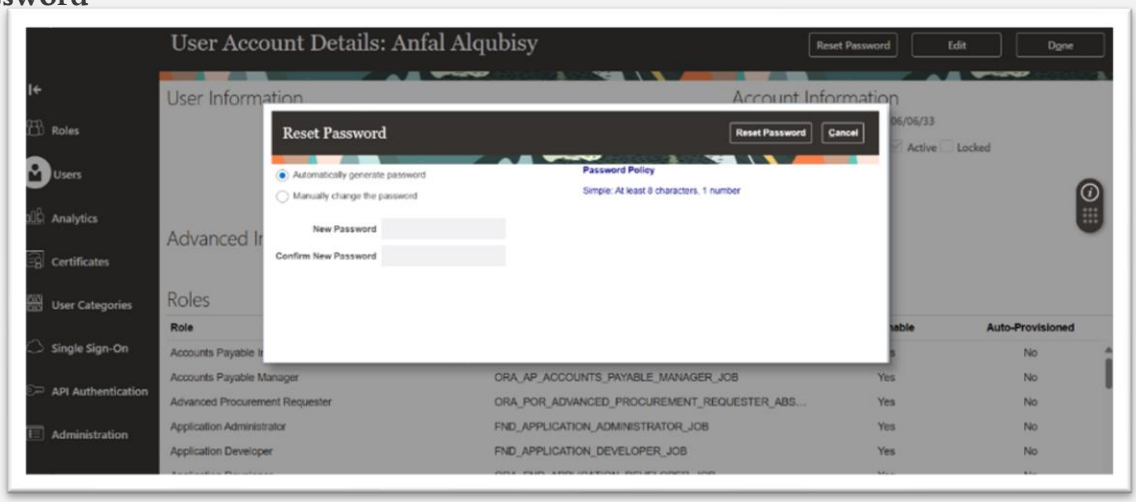
For a manual change, enter a new password.

Reset Password

- Automatically generate password
- Manually change the password

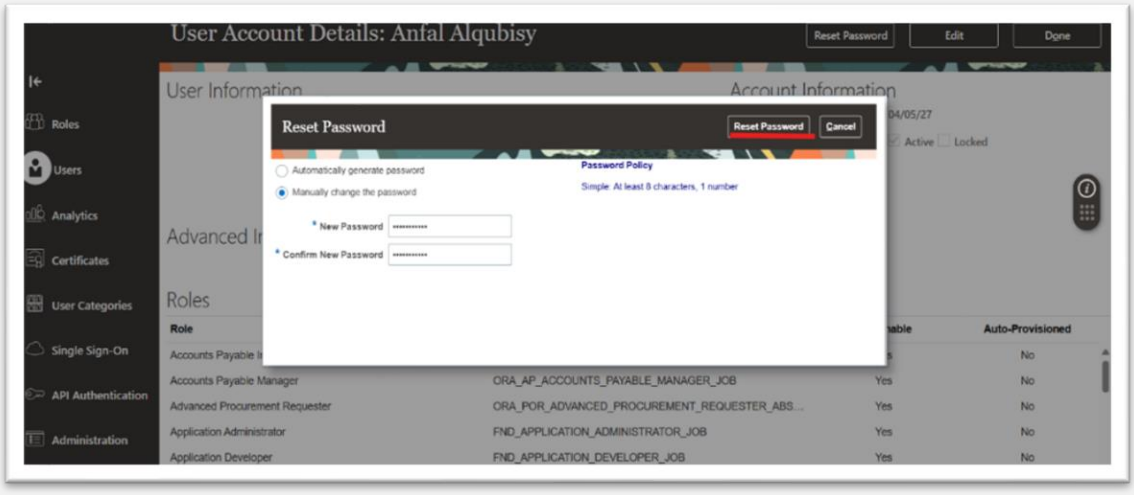
Automatically generate password

Enter the new password and click on Reset Password button



Manually change the password

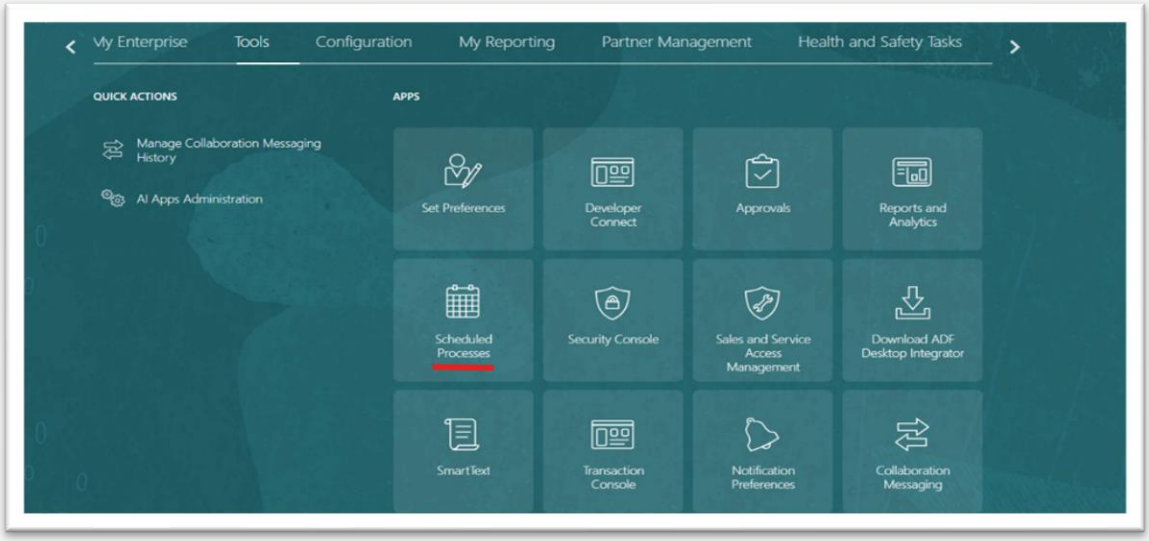
Enter the new password and click on Reset Password button

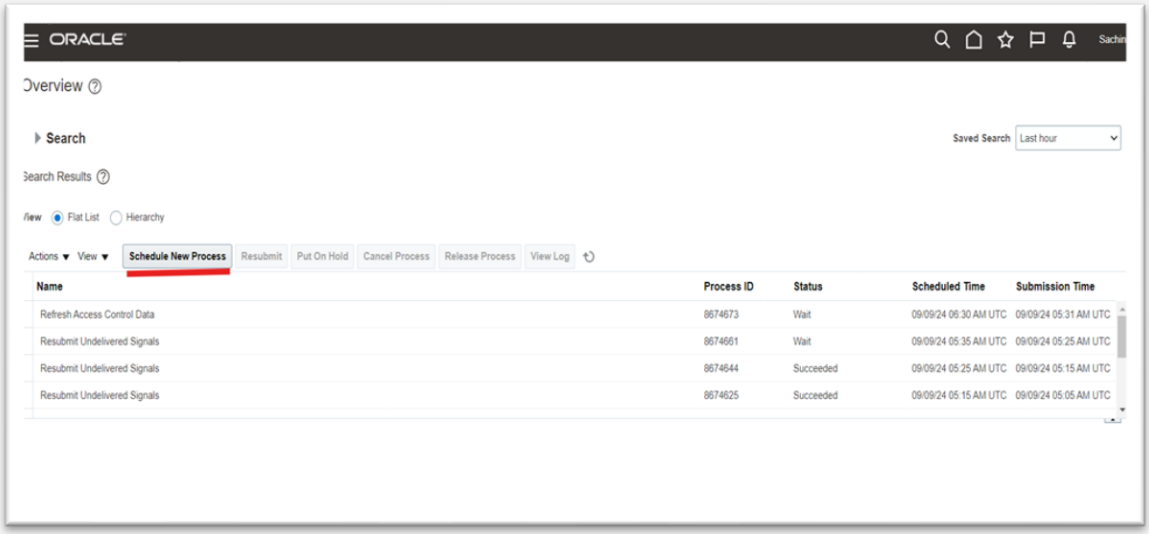


Password Expiry Report

The Password Expiry Report sends the password expiration warning and password expired notifications. You must schedule this report to run daily to help users know when their passwords have to be reset.

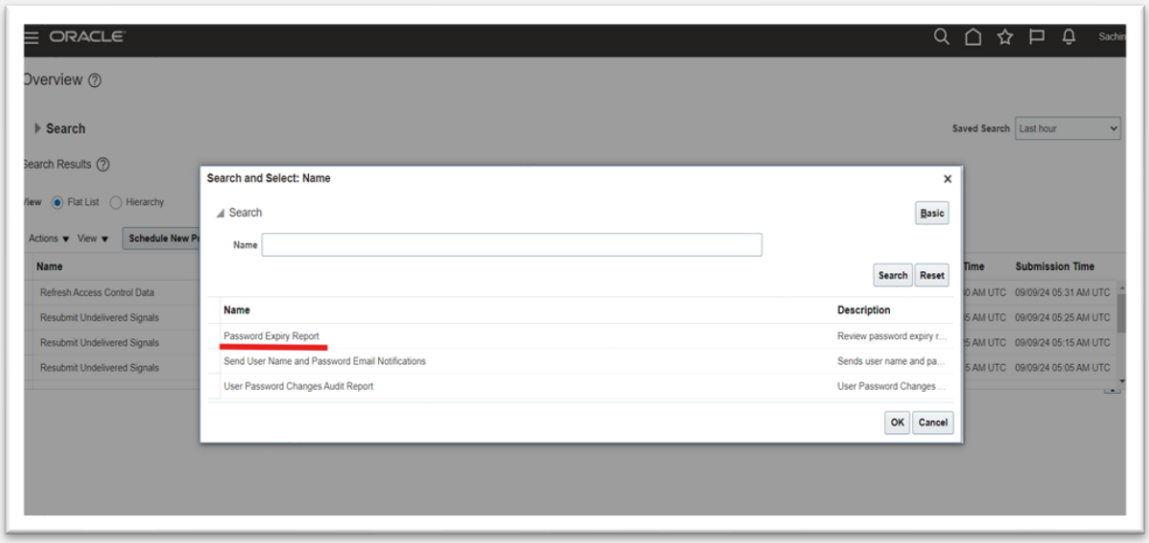
In the Scheduled Processes work area, click **Schedule New Process**.



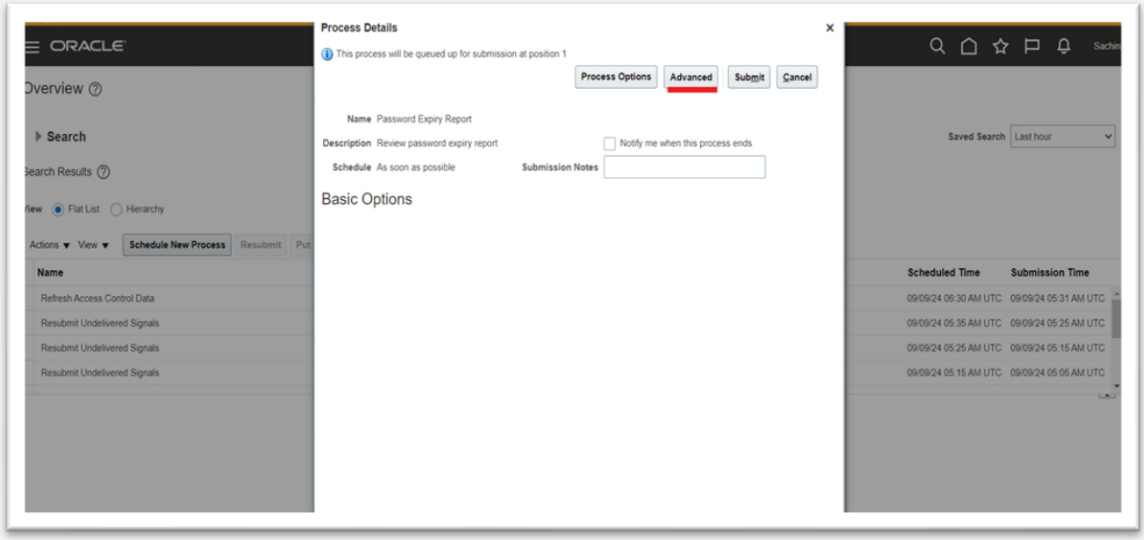


In the Schedule Process dialog box, search for and select the **Password Expiry Report** process.

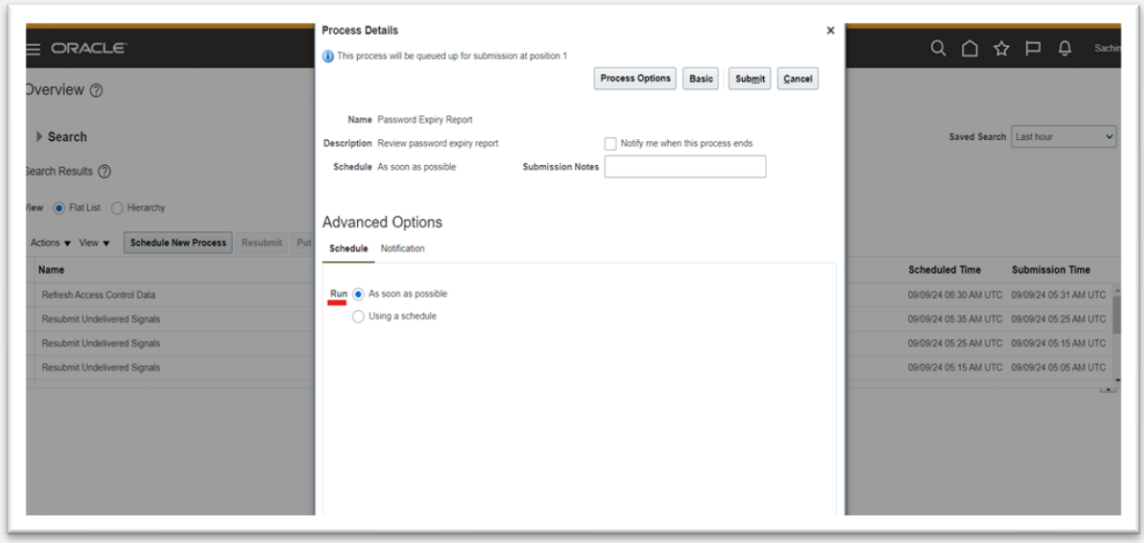
Click **OK**.



In the Process Details dialog box, click **Advanced**.



On the Schedule tab, set **Run** to **Using a schedule**.



Select a **Frequency** value. For example, select **Daily**.

Select a start date and time.

Click **Submit**.