CAMPTRA TECHNOLOGIES

DYNAMIC SOLUTIONS, TRUSTED SERVICE

2024

Security Admin Guide

Camptra Technologies
1309 W 15th Street
Suite 240
Plano, TX 75075

info@camptratech.com

V1

Camptra Technologies

1/1/2024

Guide Usage and Disclosures 2
Guide Information 2
How To Use This Guide 2
Overall Process Flow 2
Glossary of Terms 3
Day to Day Operations Guide 5
Overview 5
Navigation 5
User Page 7
Create User Accounts 7
Manage User Accounts 9
Assign Roles To Existing User Accounts 10
Remove Roles For Existing User Accounts 14
Reset User Password 16

Guide Usage and Disclosures

Guide Information

This guide is designed based on the Oracle Cloud HCM delivered setups; some fields may differ from your instance configurations. For example, some fields may be required in this guide that are not required in your instance. Additionally, some of the training topics discussed in this guide may not apply to your organization, but we know you'll find it helpful. If you would like a custom guide for your organization, please contact Megan Ketter at mketter@camptratech.com.

How To Use This Guide

This guide is intended to assist Admin users with their day-to-day tasks in Oracle Cloud. A few notes before you begin:

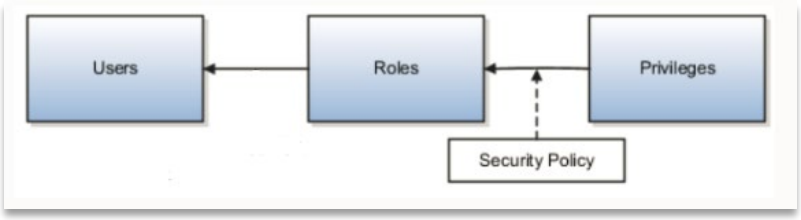
1. Any fields with an asterisk are required fields.
2. Based on your configurations, approval workflows may in place for the training topics below; those tasks would need to be approved before the additions or updates are visible in your instance.
3. You may have specific flexfields in your instance that require inputs; this guide is a generic tool and will not include those specific flexfields. You will see those fields as a context segment or not visible at all in our Oracle instance.

Overall Process Flow

Before we begin with the training content, It's important to understand the overall process flow of information in Oracle Cloud for the Security Console.

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.



Glossary of Terms

Here we've included common terms associated to the Security Console. Please review the terms below to familiarize yourself with the Oracle Cloud terms used throughout this guide.

Abstract Role

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

Application Role

- A role specific to applications and stored in the policy store.

Data Role

- A role for a defined set of data describing the job a user does within that defined set of data. A data role inherits job or abstract roles and grants entitlement to access data within a specific dimension of data based on data security policies. A type of enterprise role.

Data Role Template

- A template used to generate data roles by specifying which base roles to combine with which dimension values for a set of data security policies.

Data Security

- The control of access to data. Data security controls what action a user can taken against which data.

Data Security Policy

- A grant of entitlement to a role on an object or attribute group for a given condition

Duty Role

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

Enterprise Role

- Abstract, job, and data roles are shared across the enterprise. An enterprise role is an LDAP group. An enterprise role is propagated and synchronized across Oracle Fusion Middleware, where it is considered to be an external role or role not specifically defined within applications.

Function Security

- The control of access to a page or a specific widget or functionality within a page. Function security controls what a user can do.

HCM Data Role

- A job role, such as benefits administrator, associated with specified instances of Oracle Fusion Human Capital Management (HCM) data, such as one or more positions or all persons in a department.

Job Role

- A role for a specific job consisting of duties, such as an accounts payable manager or application implementation consultant. A type of enterprise role.

Role

- Controls access to application functions and data.

Role Deprovisioning

- The automatic or manual removal of an abstract role, a job role, or a data role from a user.

Role Hierarchy

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

Role Mapping

- A relationship between one or more job roles, abstract roles, and data roles and one or more conditions. Depending on role-mapping options, the role can be provisioned to or by users with at least one assignment that matches the conditions in the role mapping.

Role Provisioning

- The automatic or manual allocation of an abstract role, a job role, or a data role to a user.

Security Profile

- A set of criteria that identifies one or more human capital management (HCM) objects of a single type for the purposes of securing access to those objects. Security profiles can be defined for persons, organizations, positions, countries, LDGs, document types, payrolls, and payroll flows.

Day to Day Operations Guide

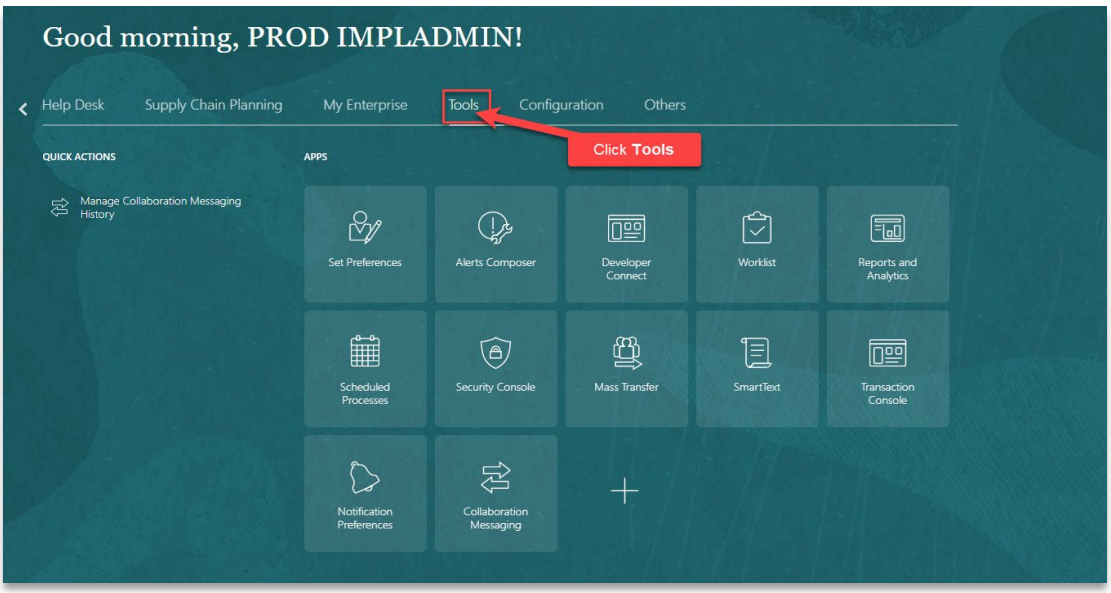
Overview

We use Security Console to manage application security in the instance. One can do tasks related to role management, role analysis, user-account management, and certificate management. You must have the IT Security Manager role to use and manage the Security Console.

Navigation

Navigation: Tools>Security Console

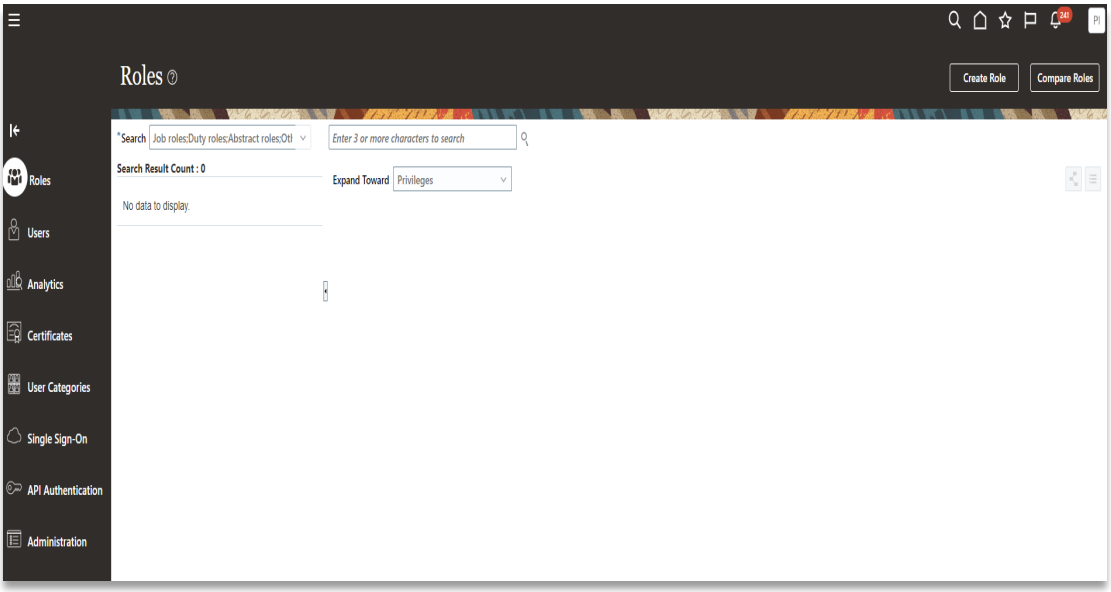
From the home screen, click **Tools**



Next, click **Security Console.** As a note, if we do not see the **Security Console** option, we do not have the applicable Security Roles to manage the Security Console and will need these roles added to our user to access the Security Console.

This is the **Security Console** work area. In the **Roles** page, you can do the following:

- Create Job, Abstract, and Duty Roles
- Edit Custom Roles
- Copy Roles
- Compare Roles
- Visualize Role Hierarchies and Assignment to Users
- Identify Roles that grant access to items and privileges for access



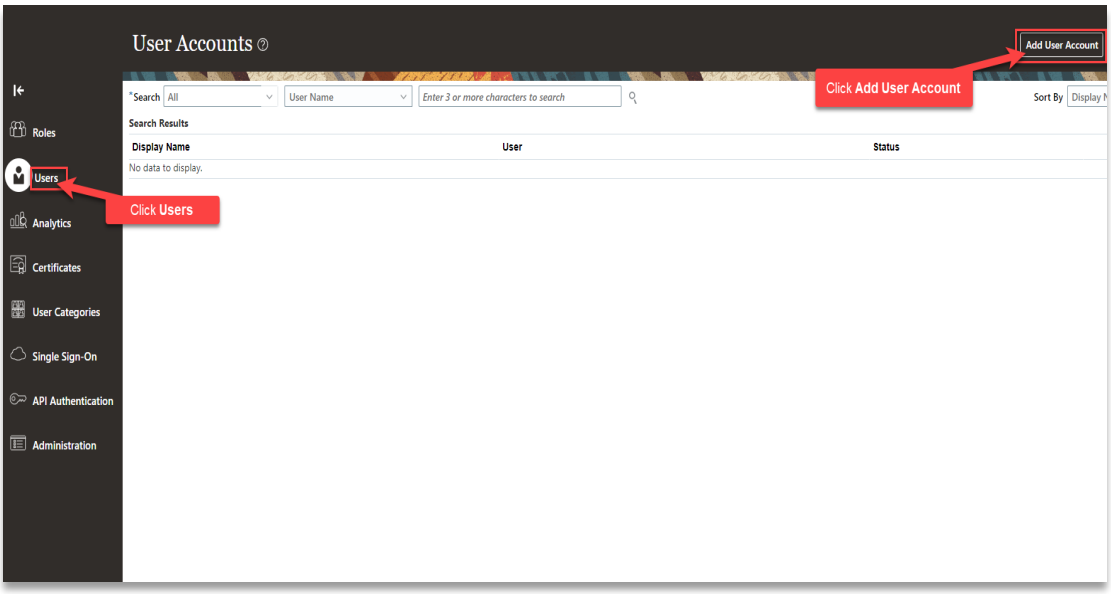
User Page

Create User Accounts

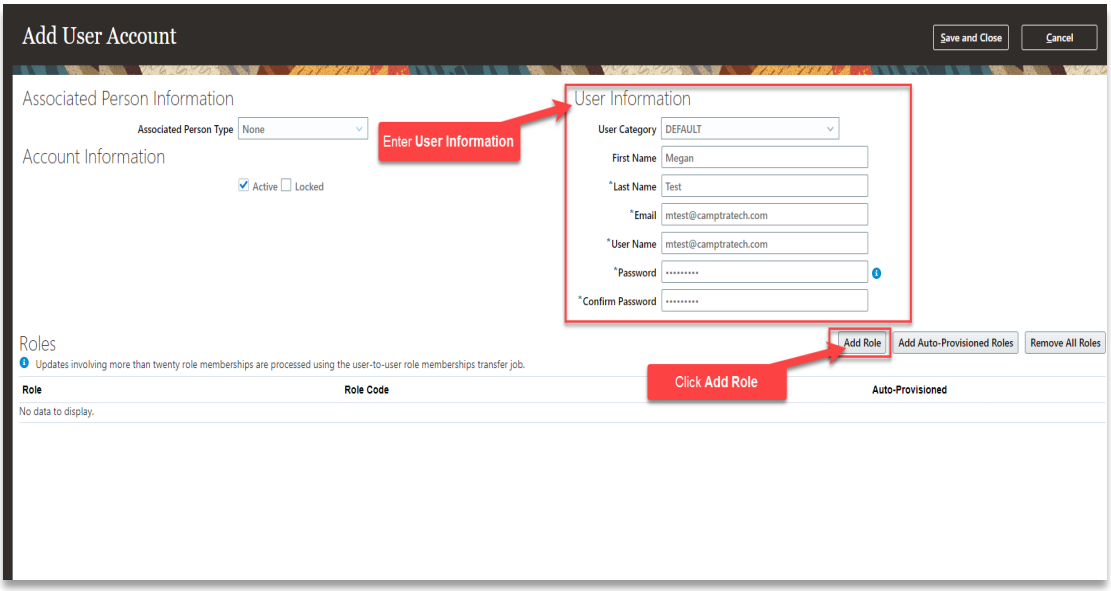
Note: User Account creation is not required for all new hires. Oracle will automatically create the user account and provision the roles. Creating a User Account is only required when the user is not an employee and needs Oracle Cloud Access.

Navigation: Tools>Security Console>Users Tab>Add User Account>Save and Close

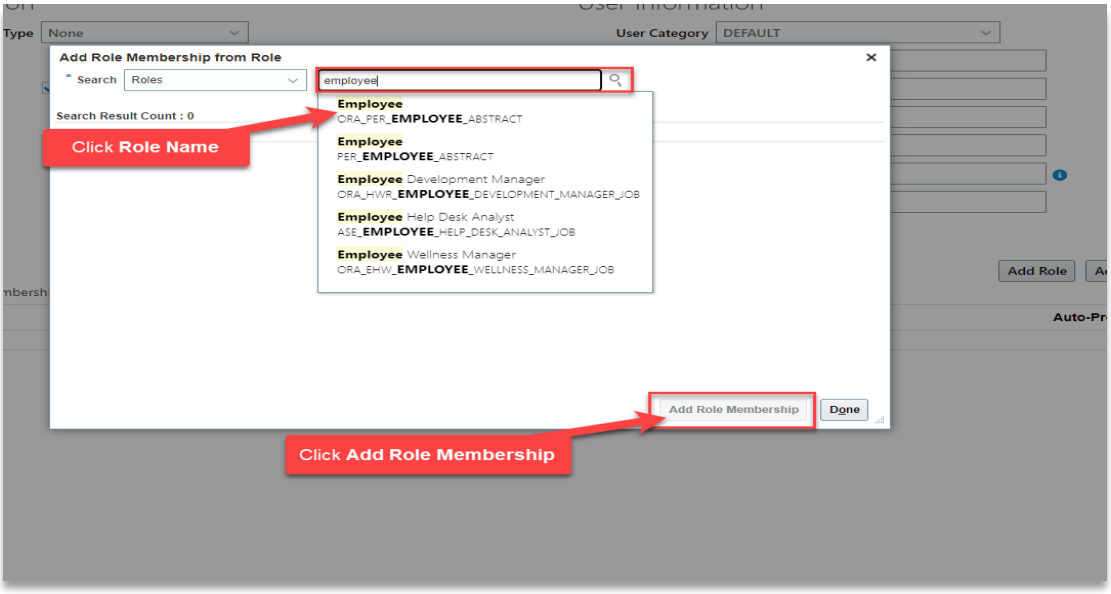
To create a user account, Select the **Users** tab and click **Add User Account**



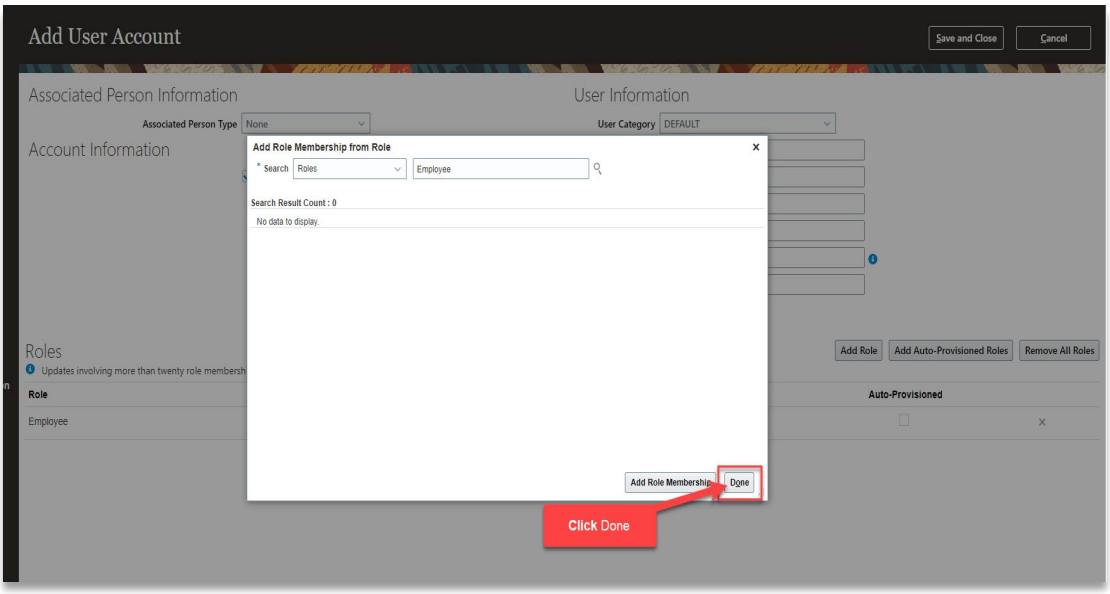
Enter the user information and click **Add Roles** to add the required roles to this user.



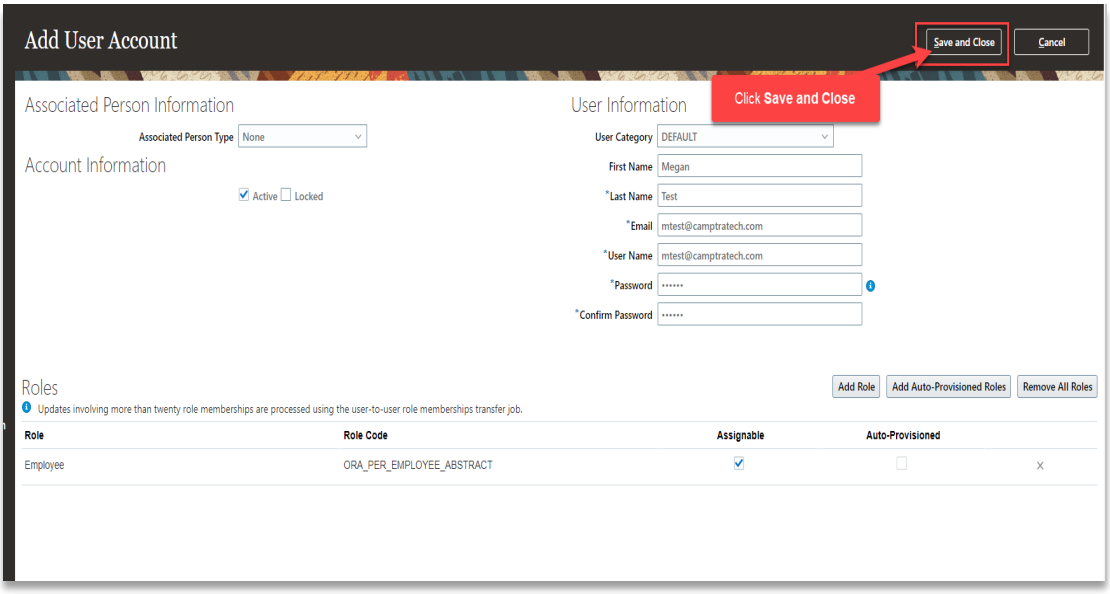
Search for the required role and select the role. Click **Add Role Membership**



Next, once all the roles have been added, click **Done**



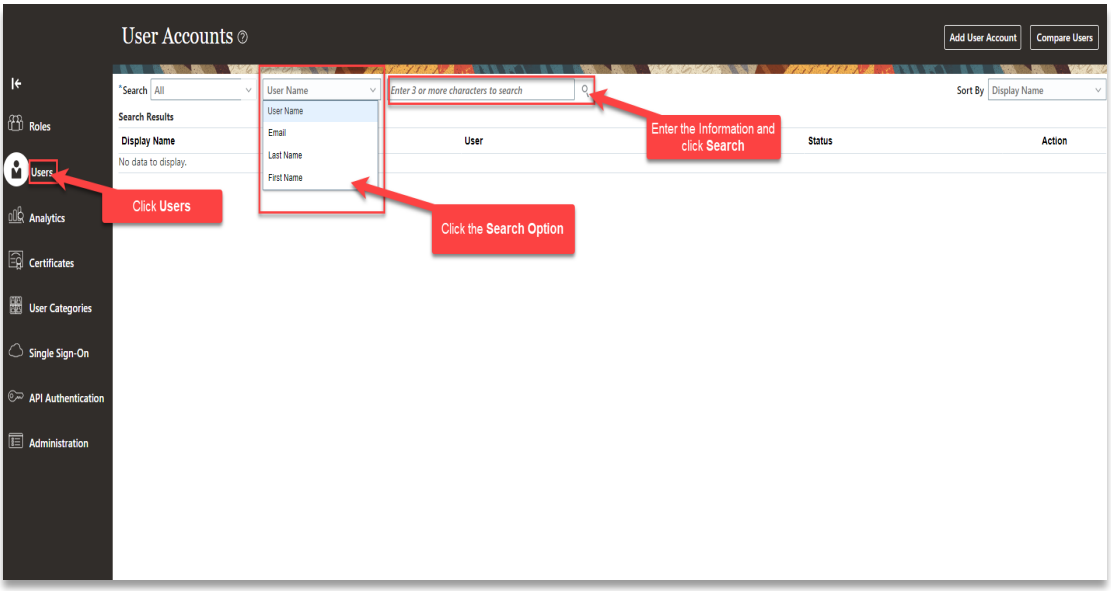
Click **Save and Close** to create the User Account



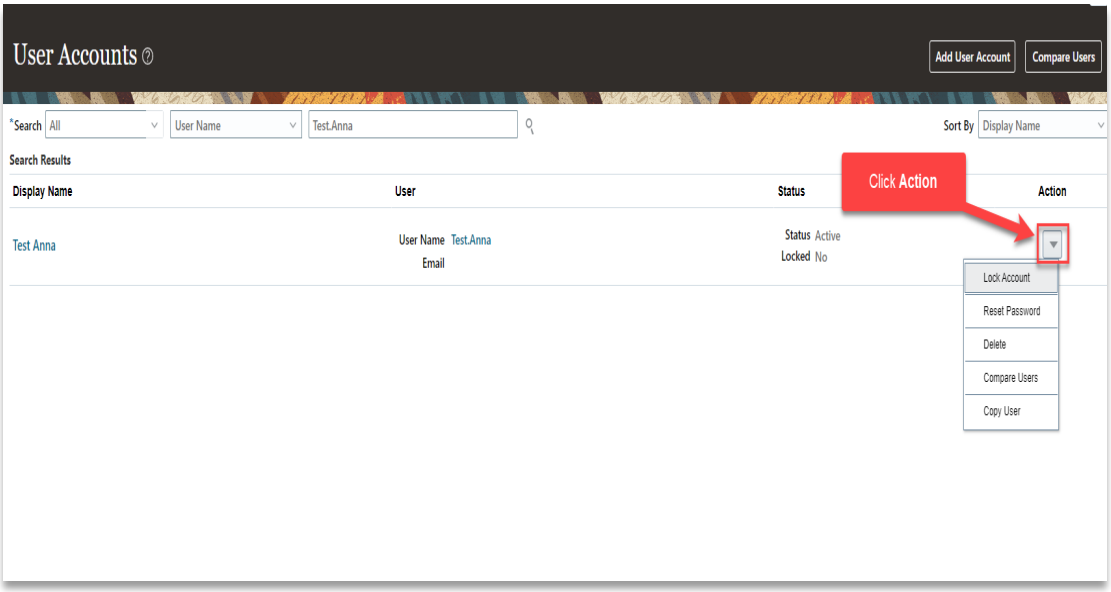
Manage User Accounts

Navigation: Tools>Security Console>Users Tab>Search User>Actions

From **Users** tab, search for the existing user accounts by username, First Name, Last Name, or Email. Select the **Search Option** from the dropdown and enter the Information and click **Search**



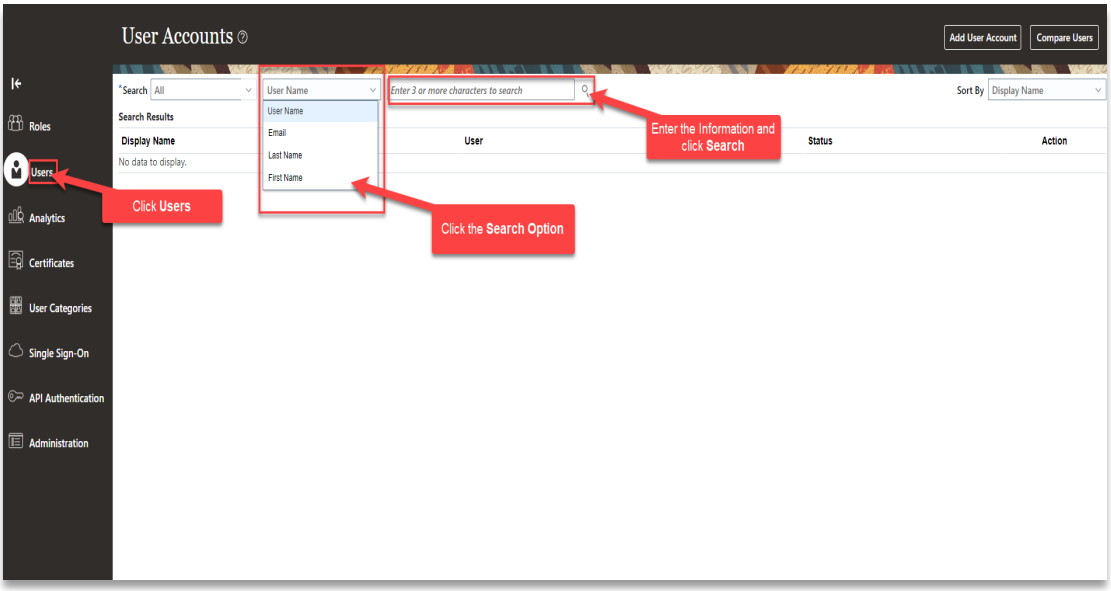
Using the **Actions** dropdown, we can **Lock Account**, **Reset Password**, **Delete**, **Compare Users**, or **Copy User**



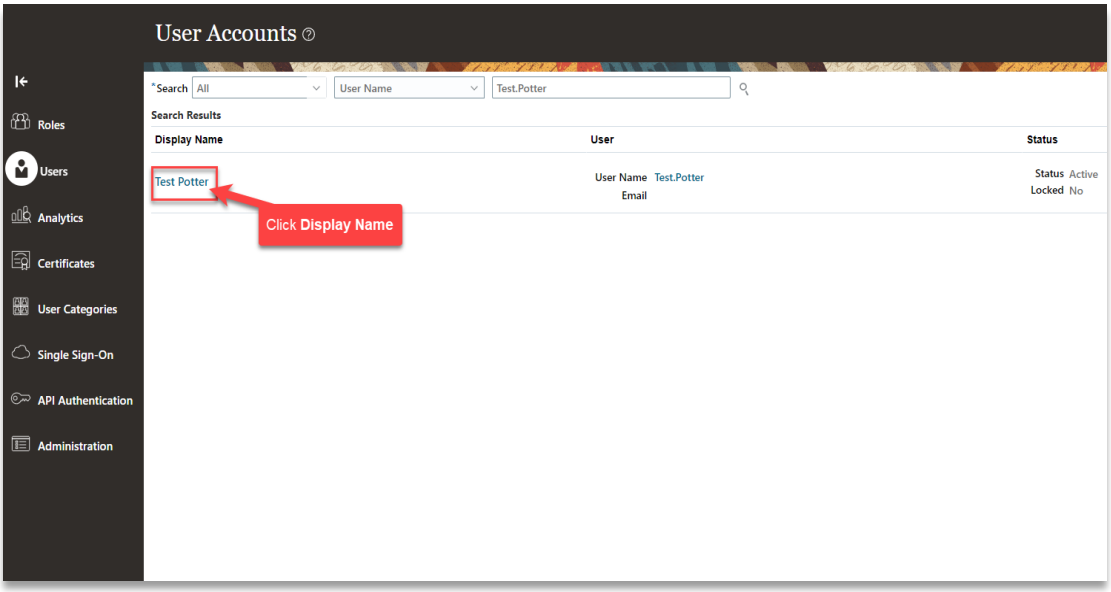
Assign Roles To Existing User Accounts

Navigation: Tools>Security Console>Users Tab>Search User>Edit>Add Role>Search Role>Done>Save and Close

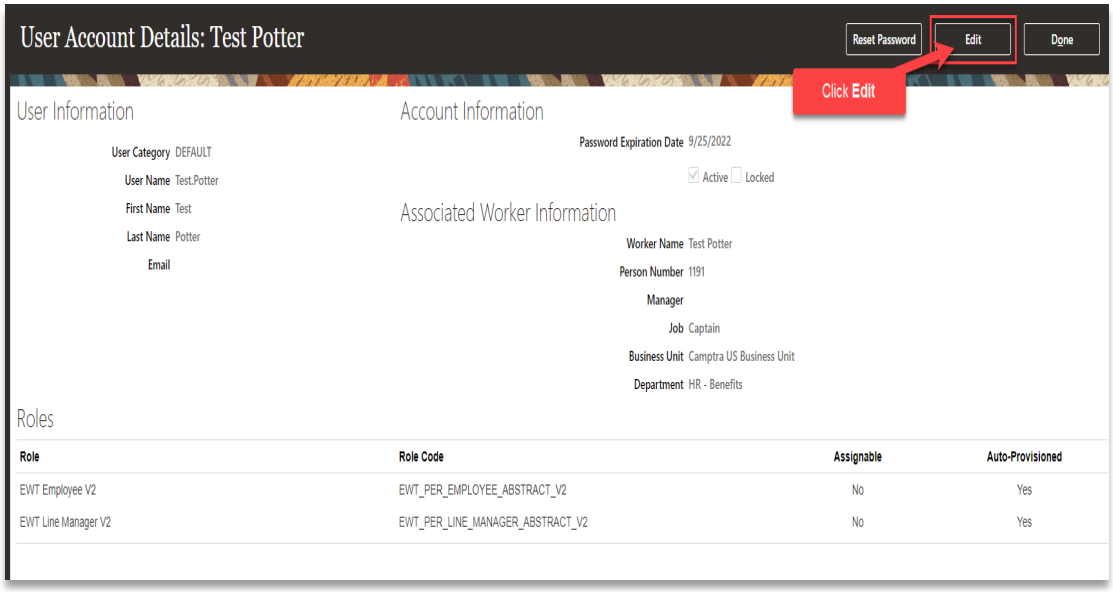
From **Users** tab, search for the existing user accounts by username, First Name, Last Name, or Email. Select the **Search Option** from the dropdown and enter the Information and click **Search**



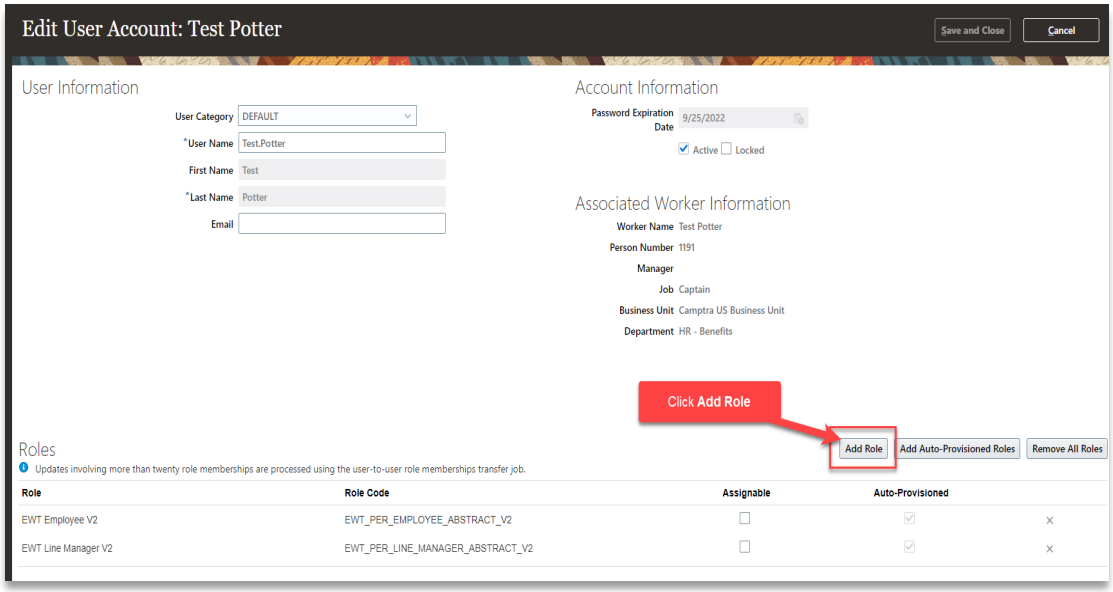
Click **Display Name**



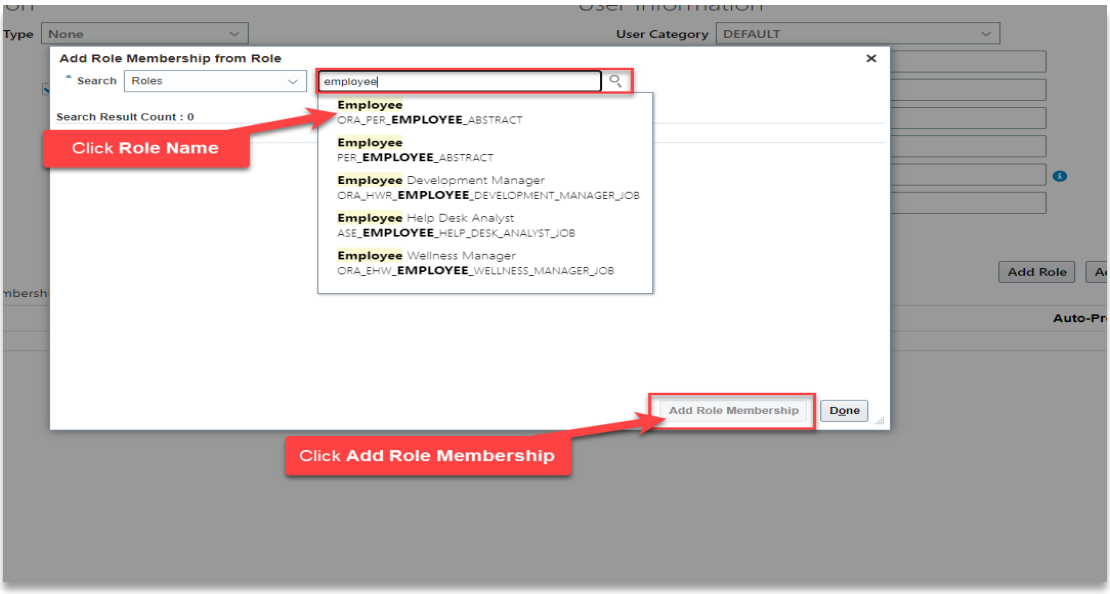
Click **Edit**



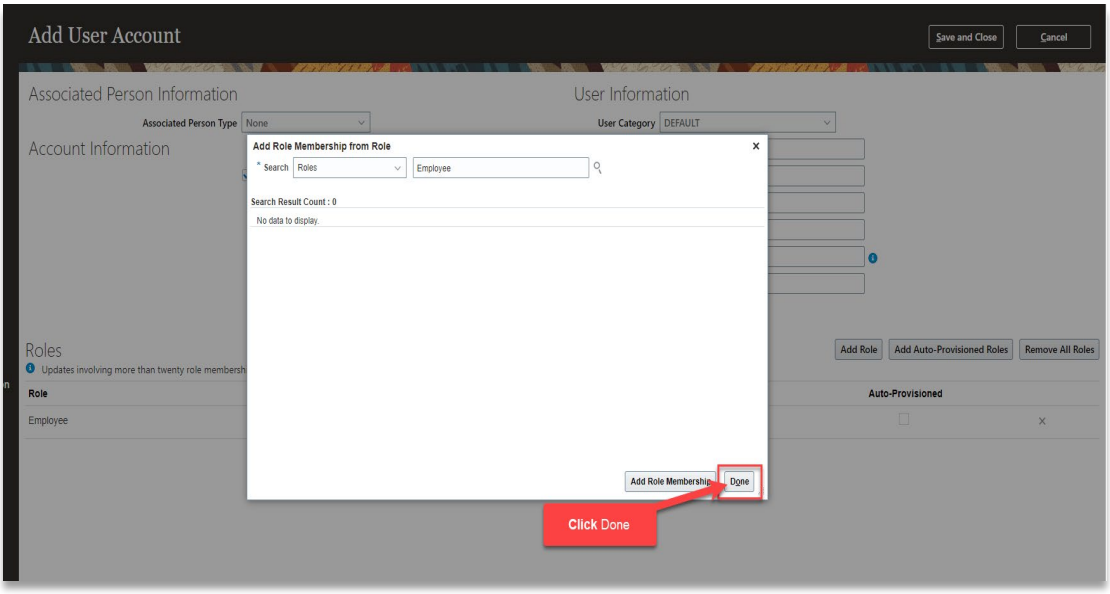
Click **Add Role**



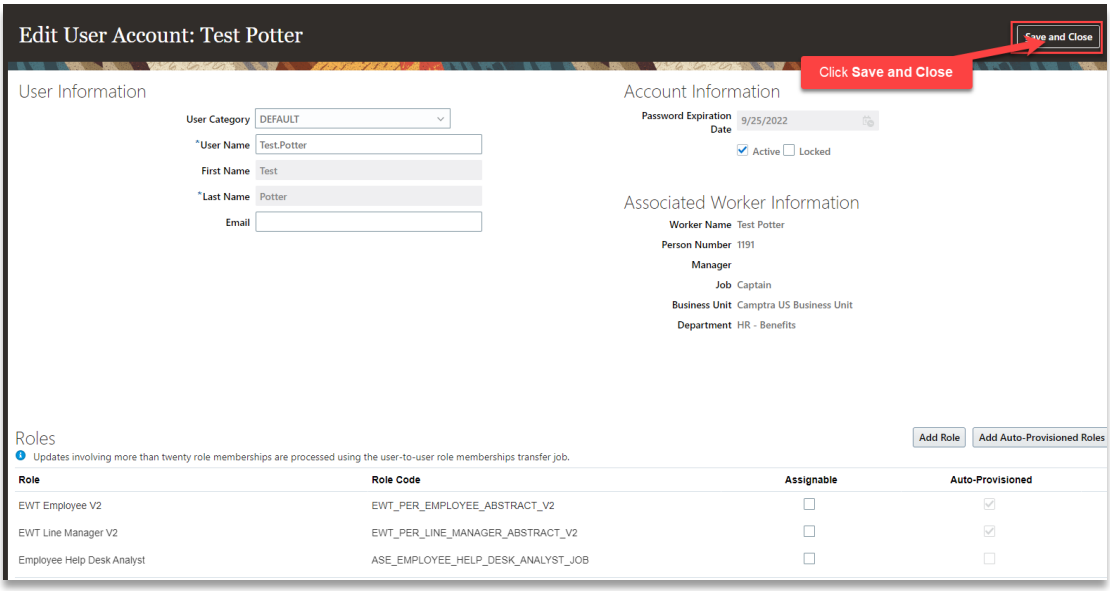
Search for the required role and select the role. Click **Add Role Membership**



Next, once all the roles have been added, click **Done**



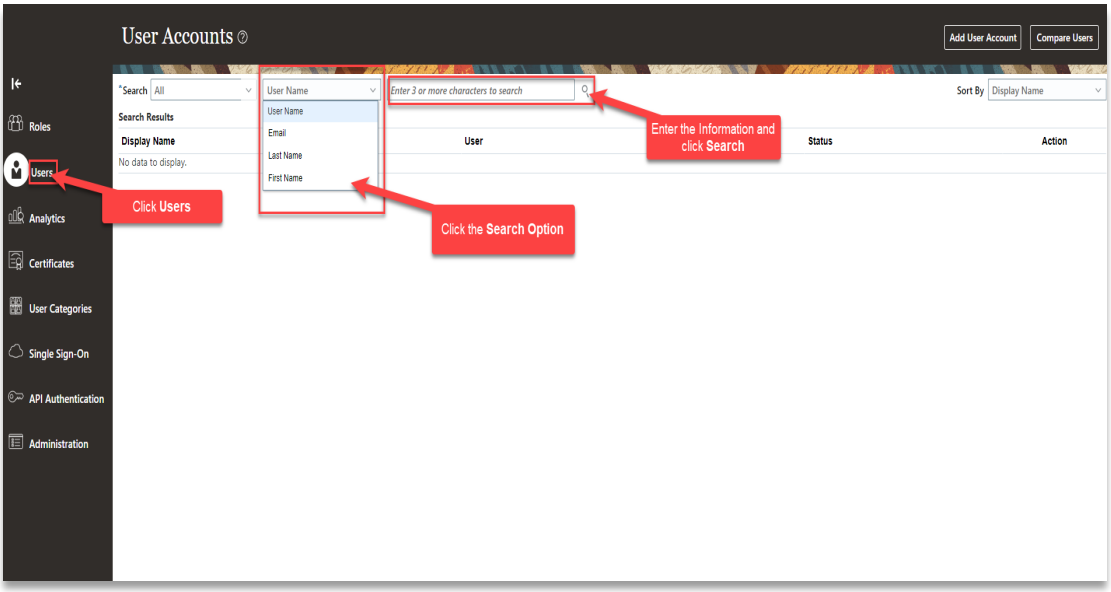
Click **Save and Close**



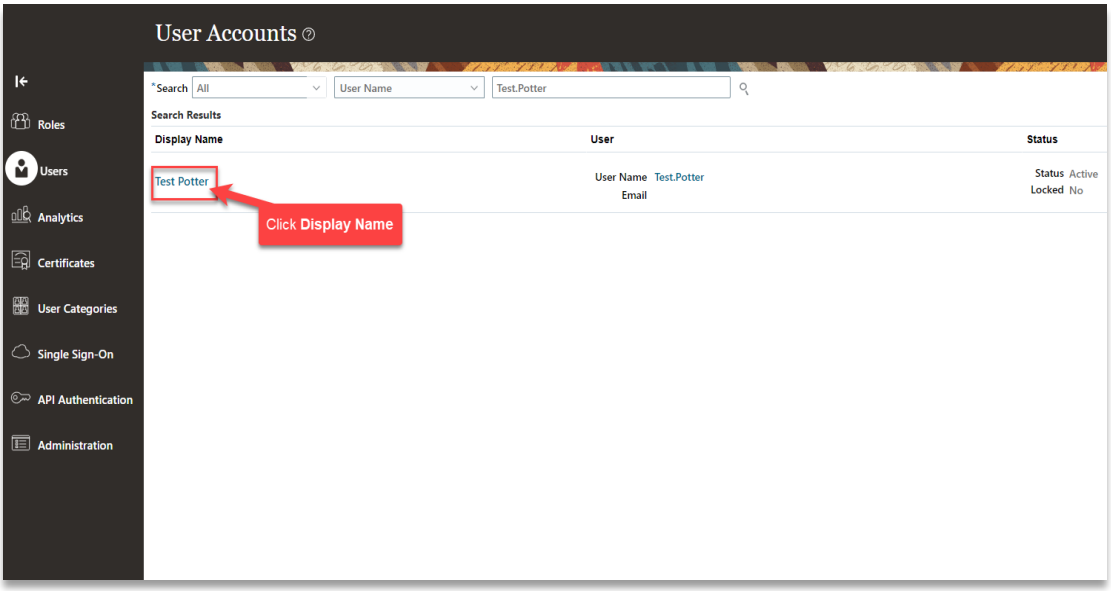
Remove Roles For Existing User Accounts

Navigation: Tools>Security Console>Users Tab>Search User>Edit>Remove Role> Save and Close

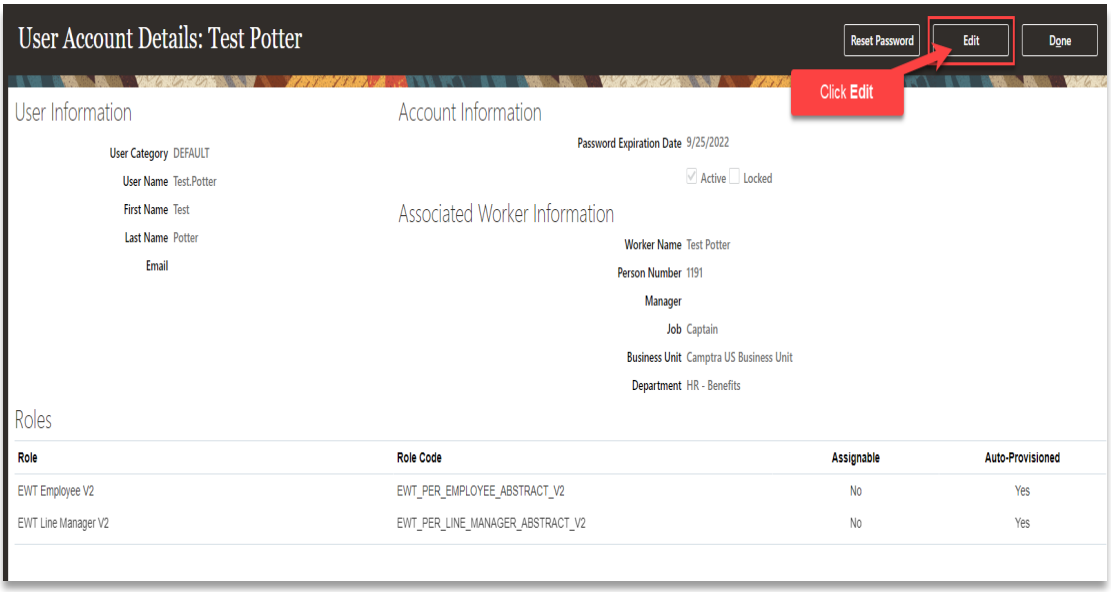
From **Users** tab, search for the existing user accounts by username, First Name, Last Name, or Email. Select the **Search Option** from the dropdown and enter the Information and click **Search**



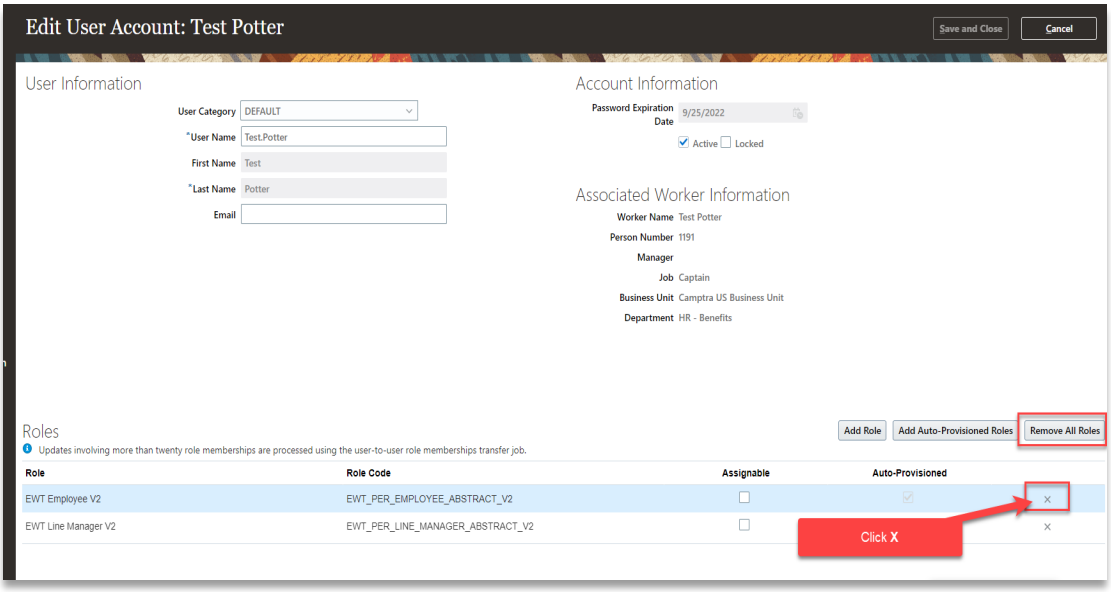
Click **Display Name**



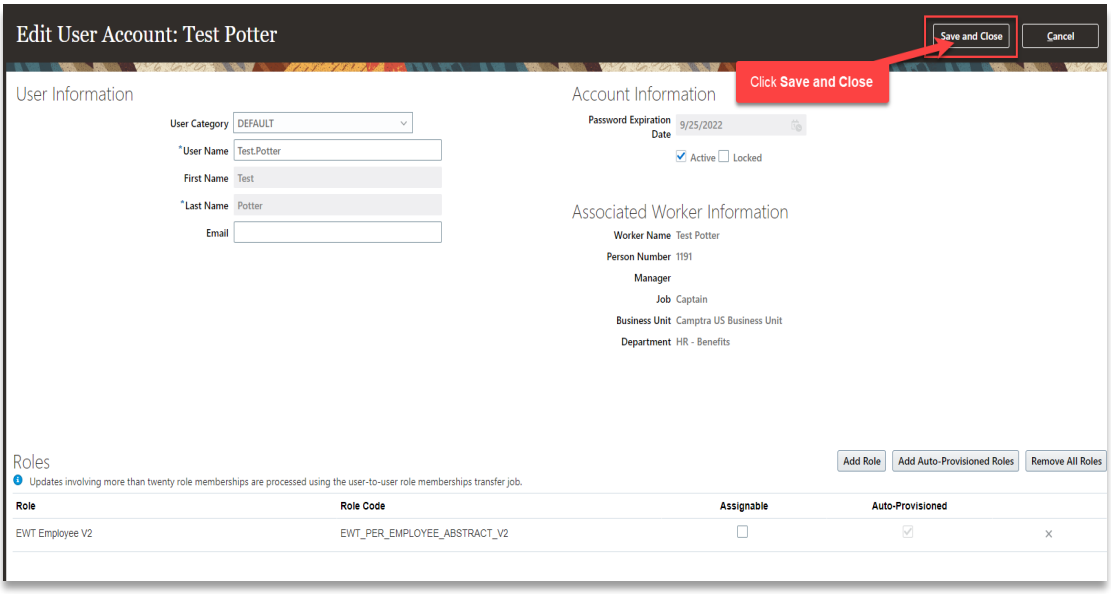
Click **Edit**



Click **X** across from the role name to **Remove** the Role. You can also select **Remove All Roles**, if applicable.



Click **Yes**, then **Save and Close**

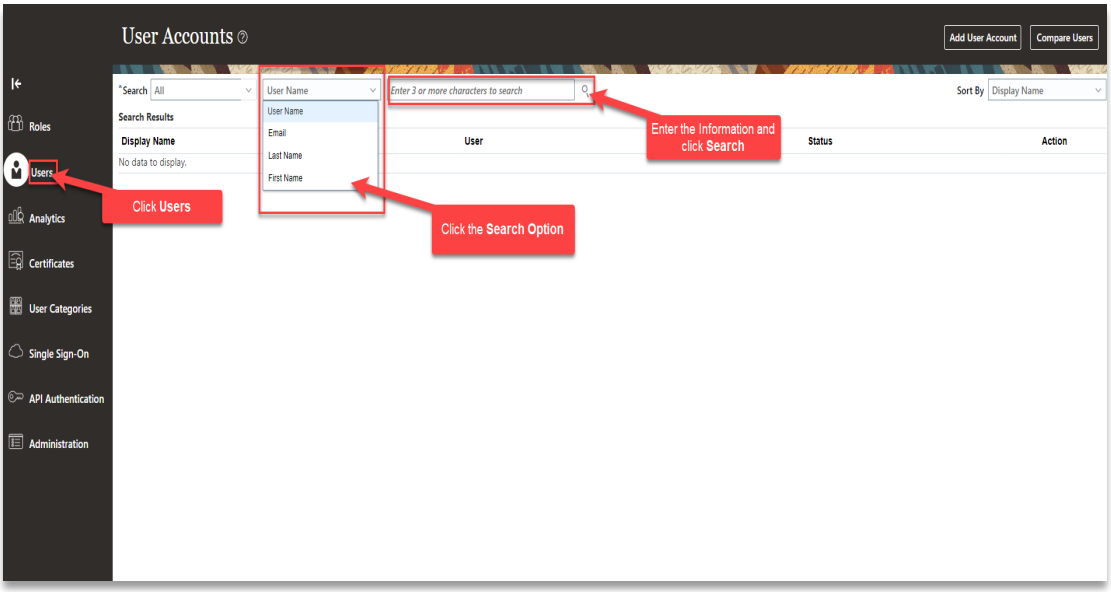


Reset User Password

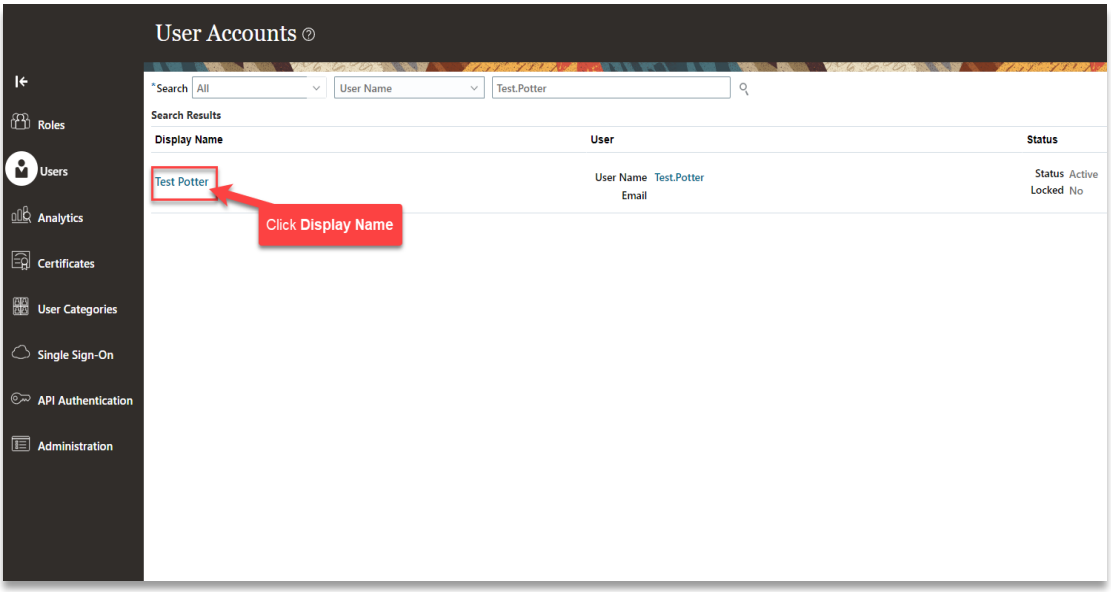
Note: If the organization is using Single Sign On (SSO), the password should not be reset in Oracle Cloud; the password should be reset in the system managing the SSO, for example, Azure. If the user doesn't have an email account with the organization, the password should be reset through Oracle Cloud.

Navigation: Tools>Security Console>Users Tab>Search User>Reset Password>Done

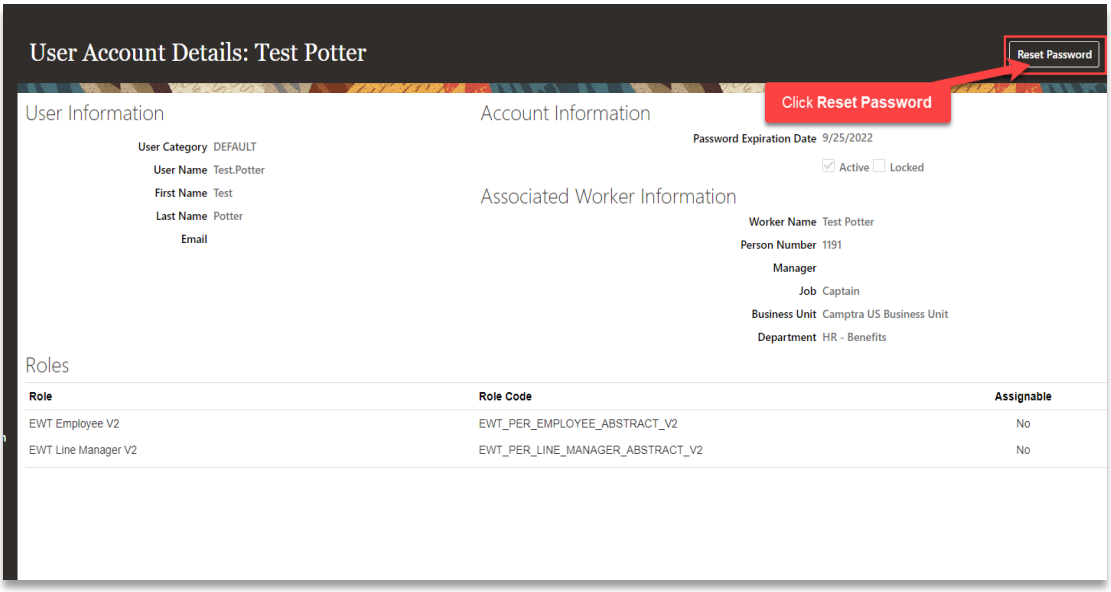
From **Users** tab, search for the existing user accounts by username, First Name, Last Name, or Email. Select the **Search Option** from the dropdown and enter the Information and click **Search**



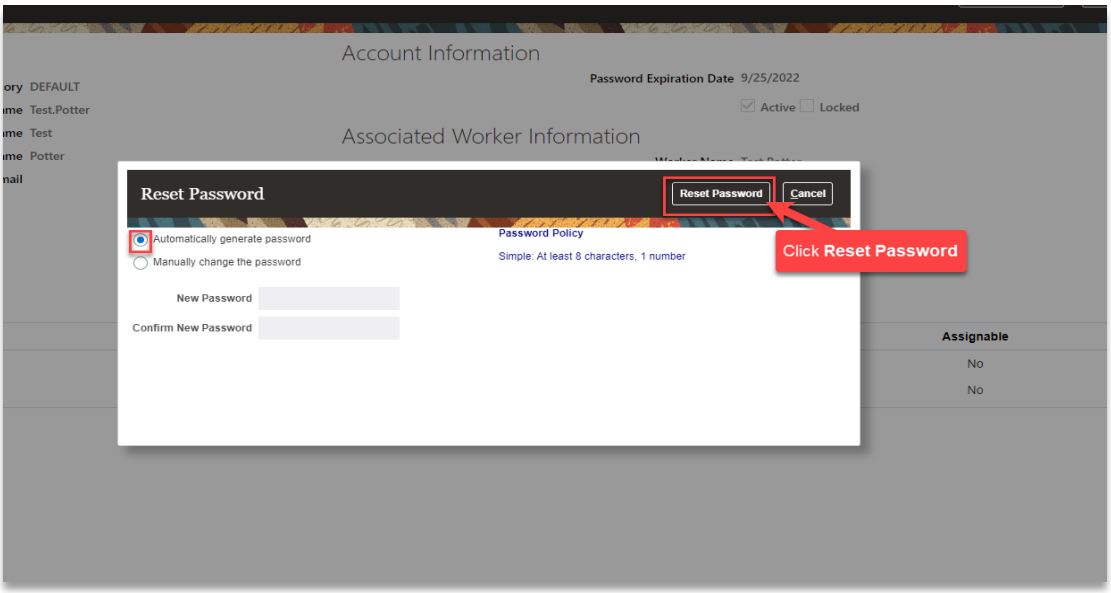
Click **Display Name**



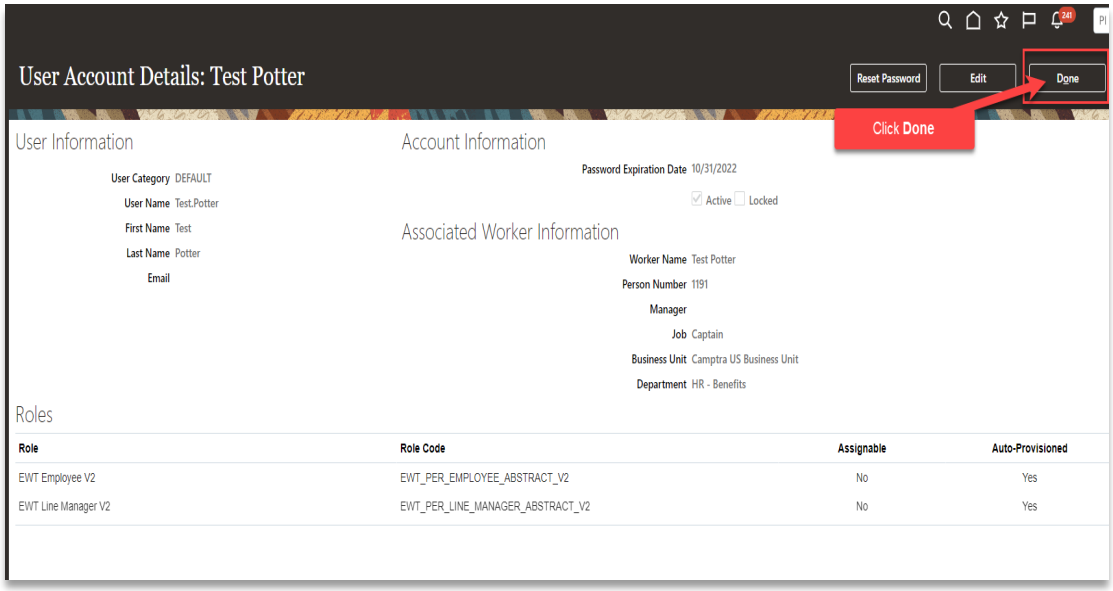
Click **Reset Password**



Click **Automatically Generate Password** to generate a password. Click **Manually Change The Password** to manually add a password for the user. Click **Reset Password**



Click **Done.** The user will receive an email with the password information.



Thank you for reviewing and using our guide; we hope you have found it helpful. If you have any questions on the content included in this guide, please contact our Training & Learning team at learn@camptratech.com

Version History	Revision Date	Author	Changes
Version 1.0		Megan Ketter	Initial Version