

How to Create a Custom Role in Oracle Fusion

Oracle Fusion provides a set of predefined (seeded) roles that cover most standard job functions, but many organizations need to adjust the menus and privileges attached to these roles to match their own business requirements. This guide walks you through how to create a custom role in Oracle Fusion by copying a standard role through the Security Console, modifying its privileges and data security policies, configuring its role hierarchy, assigning it to users, and verifying the results.

Prerequisites

Before you begin, make sure you understand the following:

- Oracle provides many seeded roles, but you should never edit these standard roles directly.
- To meet specific business requirements, you must copy a standard role and tailor the copy instead.
- You will need access to the **Security Console** in Oracle Applications.
- You should identify in advance which standard role you want to base your custom role on, and which menus or privileges need to be removed or modified.

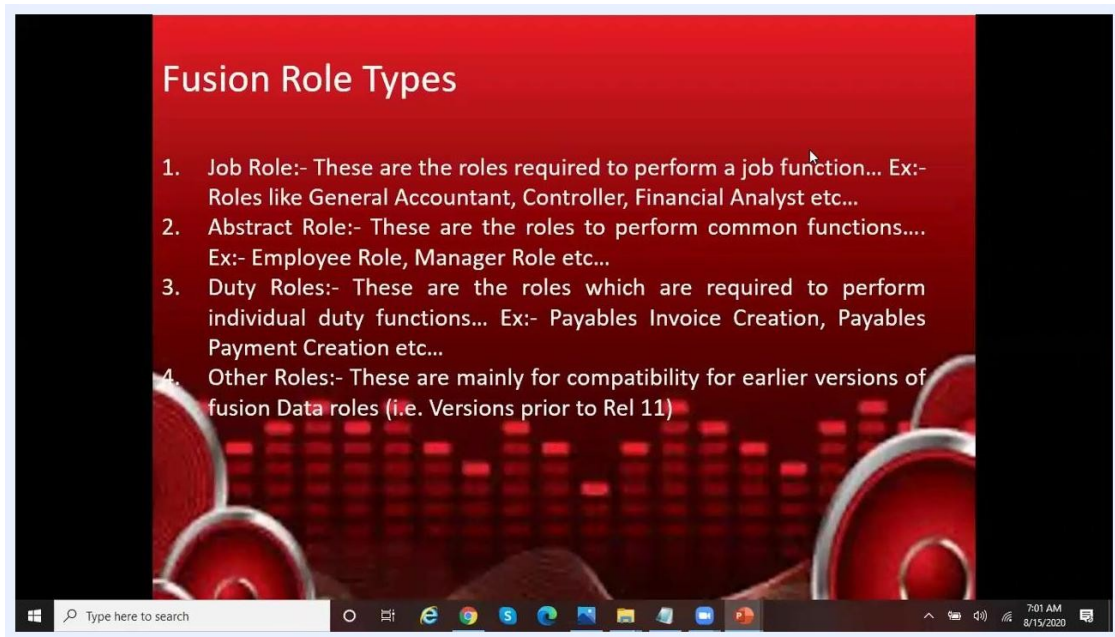
Understanding Fusion role types

1. Review the four main types of roles available in Oracle Fusion

Oracle Fusion organizes security around four role types:

- **Job Role:** Required to perform a specific job function. Example roles include General Accountant, Controller, and Financial Analyst.
- **Abstract Role:** Used to perform common functions across the organization. Example roles include Employee Role and Manager Role.
- **Duty Role:** Required to perform individual duty functions. Example duties include Payables Invoice Creation and Payables Payment Creation.

- **Other Roles:** Mainly provided for compatibility with earlier versions of Fusion Data roles (prior to Release 11).



PowerPoint slide listing and describing the four Fusion Role Types: Job Role, Abstract Role, Duty Role, and Other Roles. The slide is titled "Fusion Role Types" and includes examples for each type.

2. Prepare to create a custom role

Before opening the Security Console, identify the standard role you want to base your custom role on. Then determine which menus or privileges need to be removed or modified to meet your business requirements.

Accessing the Security Console

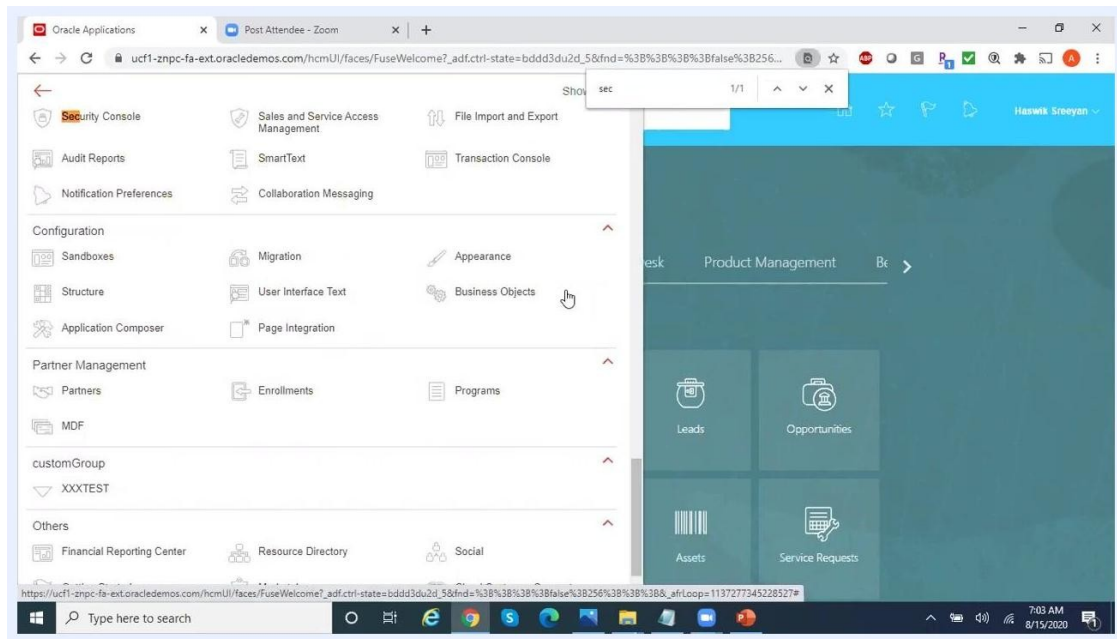
3. Access the main navigation menu

Open Oracle Applications and access the main navigation menu. Scroll through the menu to locate the **Security Console** option.

If you cannot find the **Security Console** by scrolling, use the search function instead:

- Click into the search bar at the top of the menu.
- Type "Security Console" to filter and locate the option.

The **Security Console** is found under the section with options like "Audit Reports," "Notification Preferences," and "Configuration."



Oracle Applications navigation menu open, with the user searching for "Security Console". Various modules and options are visible, including Configuration, Partner Management, and others.

Click on **Security Console** to open it.

4. Open the Roles tab

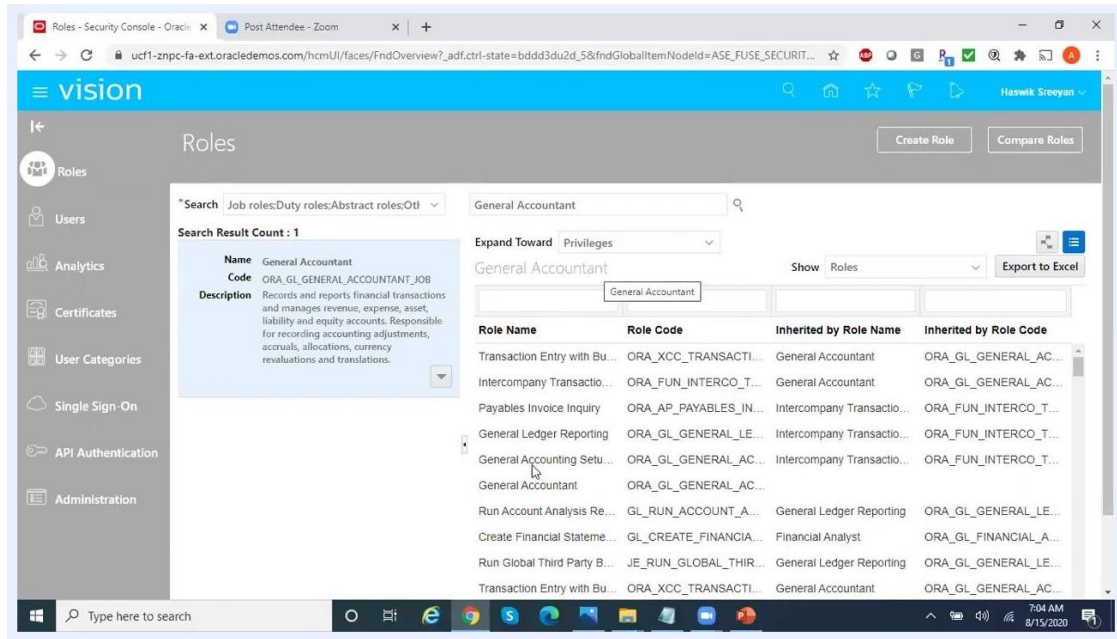
In the **Security Console**, select the **Roles** tab from the left sidebar.

5. Filter the roles list

Use the search and filter options to view different types of roles:

- Click the filter dropdown next to the search bar.
- Ensure that **Job roles**, **Duty roles**, **Abstract roles**, and **Other roles** are checked.

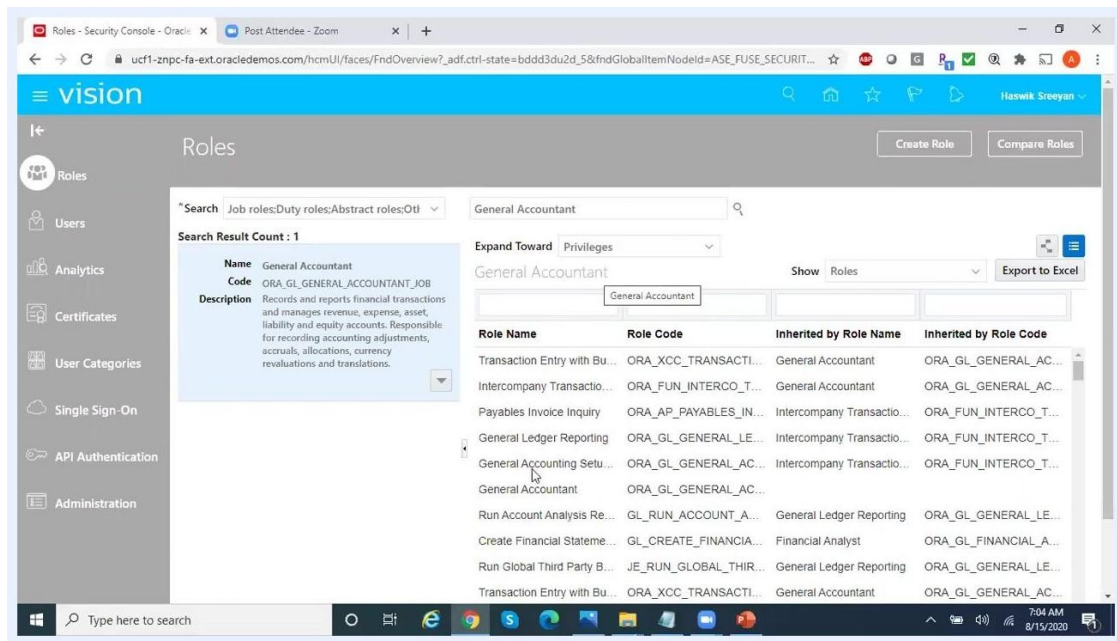
- You can also filter by **Privileges** and **Aggregate privileges** if needed.



Security Console Roles screen with filter dropdown open, showing options for Job roles, Duty roles, Abstract roles, Other roles, Privileges, and Aggregate privileges.

6. Search for the standard role to base your custom role on

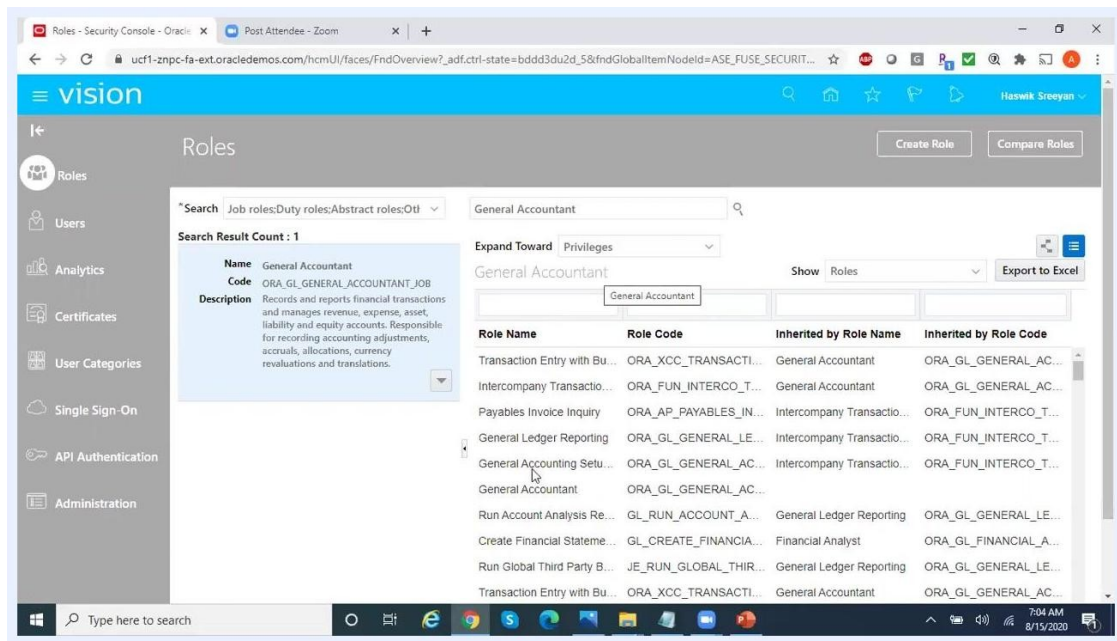
In the search bar, enter the name of the standard role you want to use as a starting point. For this example, type **General Accountant** and select the matching role from the search results under **Job Roles**.



Security Console Roles screen with "General Accountant" typed in the search bar, showing matching job and duty roles in the dropdown.

7. Review the standard role's details

Confirm the **Name** (General Accountant), **Code** (ORA_GL_GENERAL_ACCOUNTANT_JOB), and **Description**. Review the list of privileges and inherited roles associated with this role.



Security Console displaying the details for the "General Accountant" role, including its code, description, and a list of associated privileges and inherited roles.

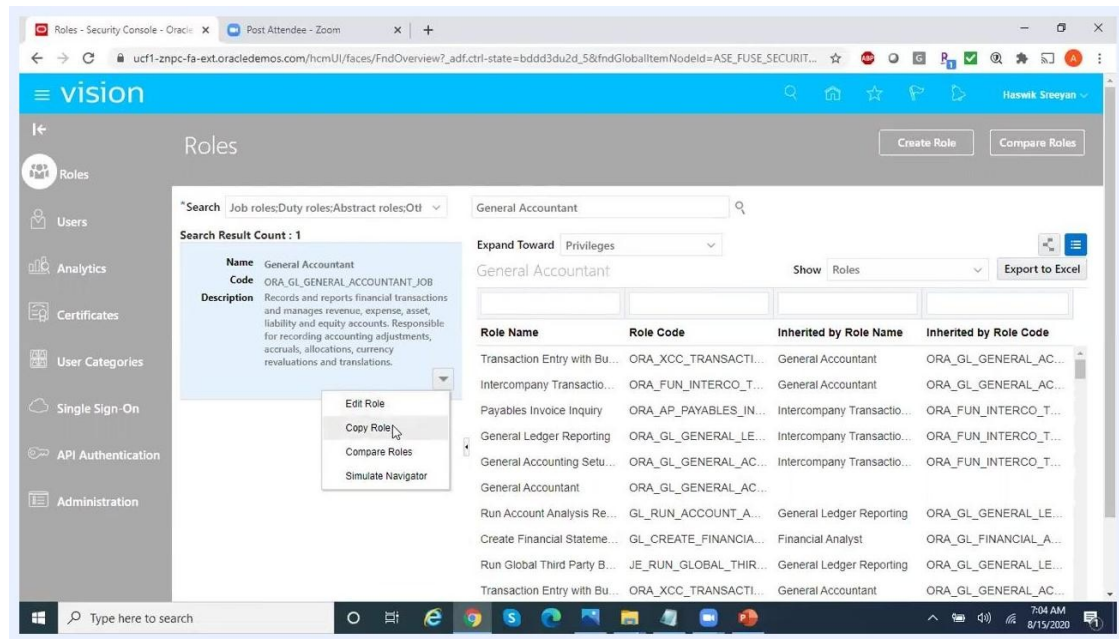
Copying the standard role

8. Copy the role instead of editing it

Business requirements may require you to remove certain menus or privileges from a standard role. Because standard roles should never be edited directly, you instead copy the role and create a custom version tailored to your needs, then assign that custom role to users as required.

To start, click the dropdown arrow next to the standard role's name and select **Copy Role** from the menu.

Do not select "Edit Role" for standard roles — always use **Copy Role** to create a custom version.



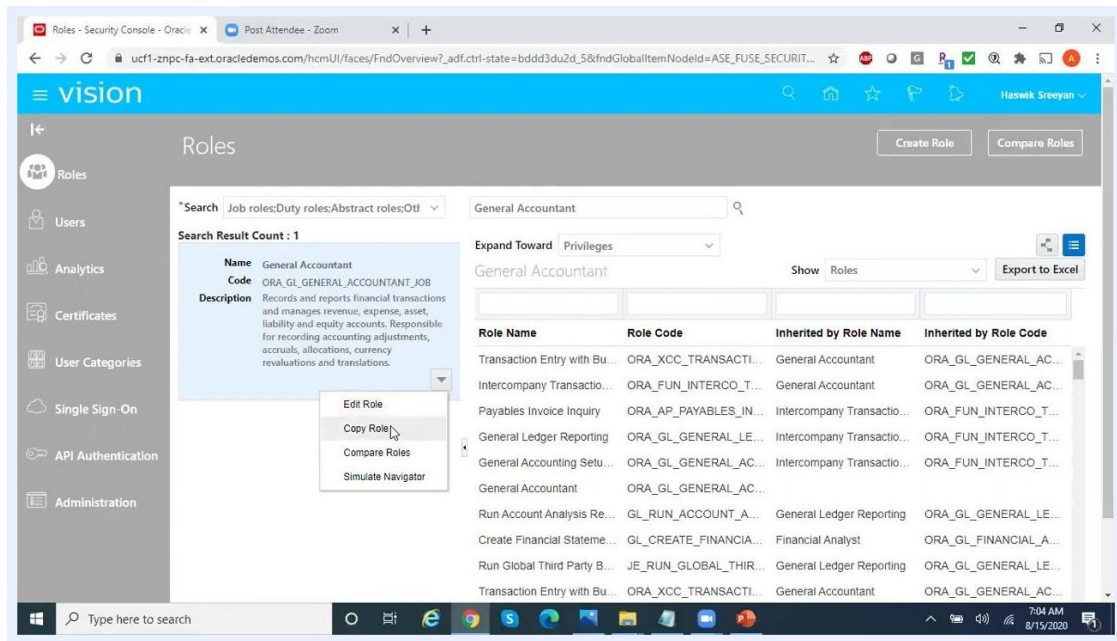
Security Console with the dropdown menu open for the "General Accountant" role, showing options: Edit Role, Copy Role, Compare Roles, Simulate Navigator. "Copy Role" is highlighted.

9. Enter the custom role's basic details

In the **Copy Role** wizard, enter the following details:

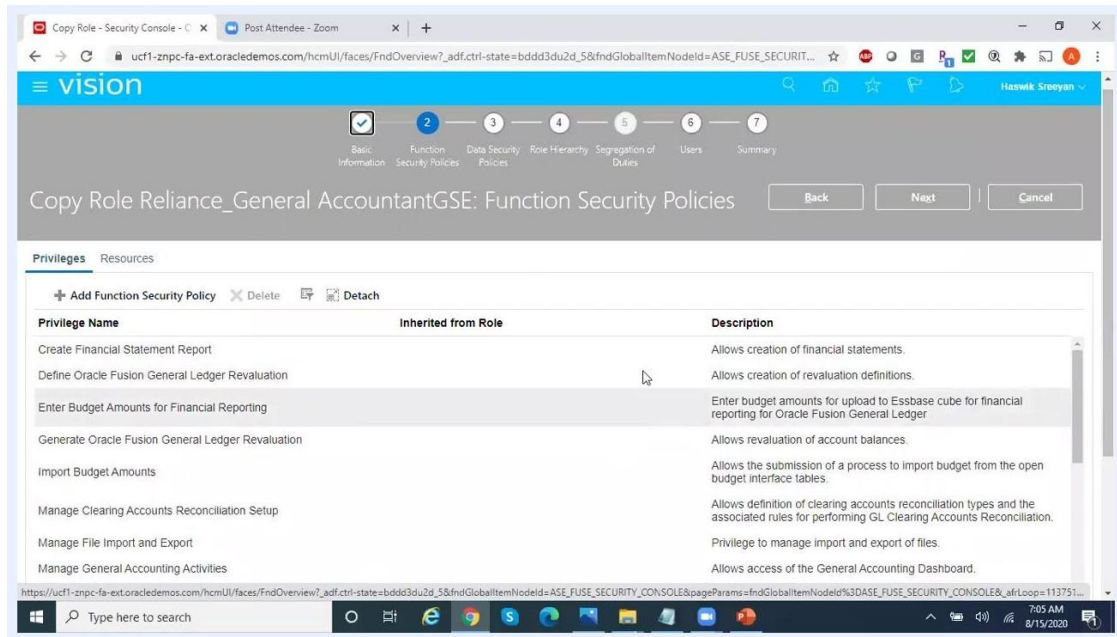
- **Role Name:** Reliance_General AccountantGSE
- **Role Code:** RELIANCE_GL_GENERAL_ACCOUNTANT_JOB_GSE
- **Role Category:** Financials - Job Roles (auto-filled)
- **Predefined Role:** Leave this checkbox unchecked, since this is a custom role rather than a predefined one.

- **Description:** Auto-filled from the standard role, though you may edit it as needed. For example: "Records and reports financial transactions and manages revenue, expense, asset, liability and equity accounts. Responsible for recording accounting adjustments, accruals, allocations, currency revaluations and translations."



Copy Role wizard in Oracle Fusion Security Console, with fields filled for Role Name (Reliance_General AccountantGSE), Role Code (RELIANCE_GL_GENERAL_ACCOUNTANT_JOB_GSE), Role Category (Financials - Job Roles), Predefined Role (unchecked), and Description.

Verify that the **Predefined Role** checkbox remains unchecked to confirm you are creating a custom role, not a seeded one. The fields should display the Role Name, Role Code, Role Category, and Description shown above.



Copy Role wizard showing Role Name, Role Code, Role Category, Predefined Role (unchecked), and Description fields for the custom role.

Click **Next** to proceed to the Function Security Policies step.

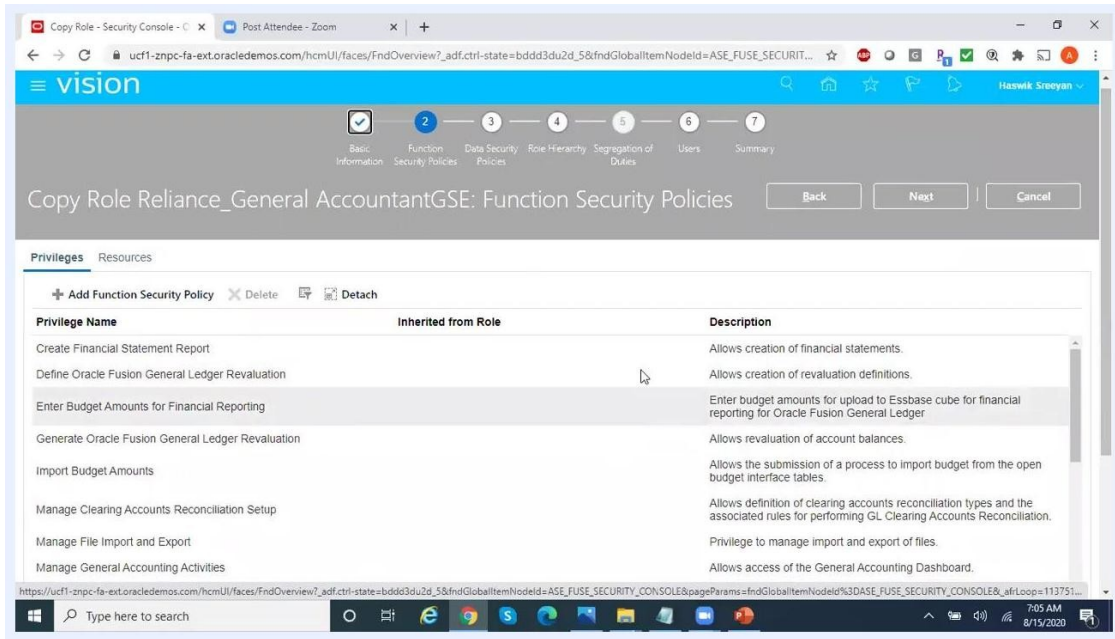
Adjusting function security policies

10. Review the inherited privileges

The **Function Security Policies** page lists all privileges inherited from the standard "General Accountant" role, including:

- Create Financial Statement Report
- Define Oracle Fusion General Ledger Revaluation
- Enter Budget Amounts for Financial Reporting
- Generate Oracle Fusion General Ledger Revaluation
- Import Budget Amounts
- Manage Clearing Accounts Reconciliation Setup
- Manage File Import and Export

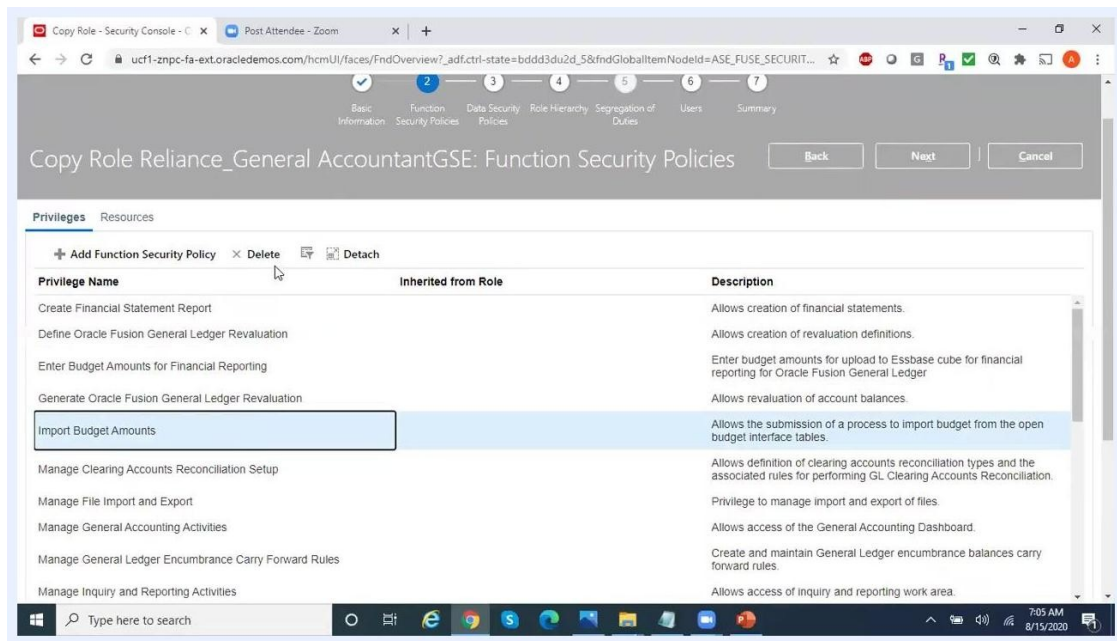
- Manage General Accounting Activities



Function Security Policies screen showing a list of privileges, including "Enter Budget Amounts for Financial Reporting" and "Import Budget Amounts".

11. Remove budget-related privileges

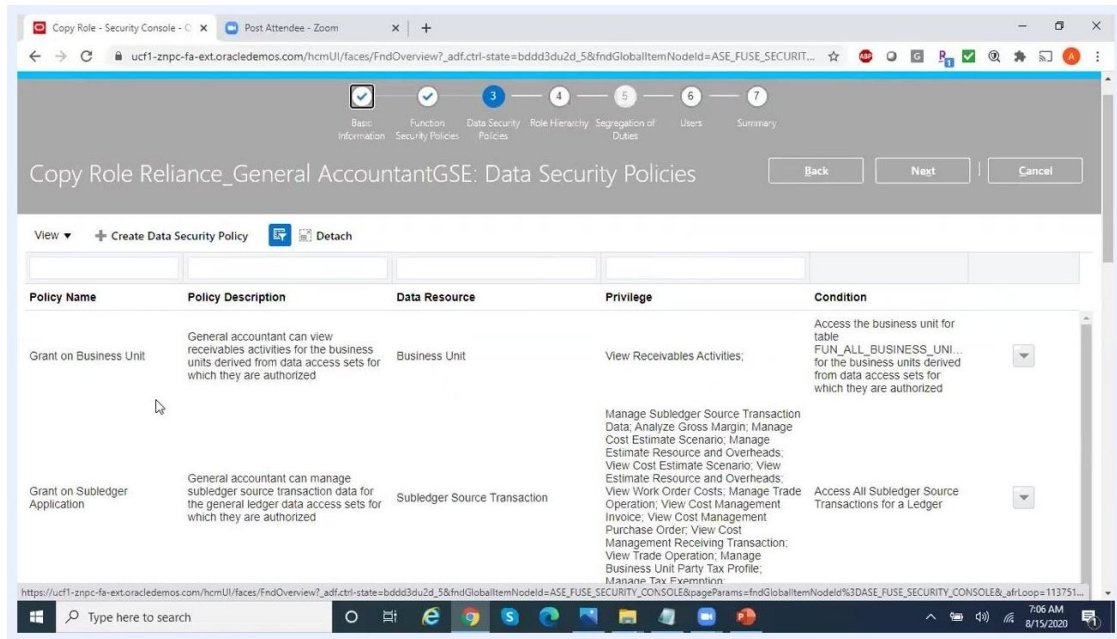
Identify privileges related to budgets, such as **Enter Budget Amounts for Financial Reporting** and **Import Budget Amounts**. Select each budget-related privilege by clicking on it, then click the **Delete** button to remove it.



Privilege "Import Budget Amounts" selected, with the Delete button highlighted, ready to remove the privilege.

12. Remove component functionality privileges

Scroll through the list and identify any privileges related to component functionalities that should not be included. Select the privilege — for example, "Run Encumbrance Year End Carry Forward Program in Final Mode" — and click **Delete** to remove it.



Component-related privilege "Run Encumbrance Year End Carry Forward Program in Final Mode" selected, ready for deletion.

Click **Next** to proceed to the Data Security Policies step.

Adjusting data security policies

13. Review the inherited data security policies

The **Data Security Policies** page lists policies such as:

- **Grant on Business Unit:** General accountant can view receivables activities for the business units derived from data access sets for which they are authorized.
- **Grant on Subledger Application:** General accountant can manage subledger source transaction data for the general ledger data access sets for which they are authorized.

The table columns include **Policy Name**, **Policy Description**, **Data Resource**, **Privilege**, and **Condition**.

Copy Role Reliance_General AccountantGSE: Data Security Policies

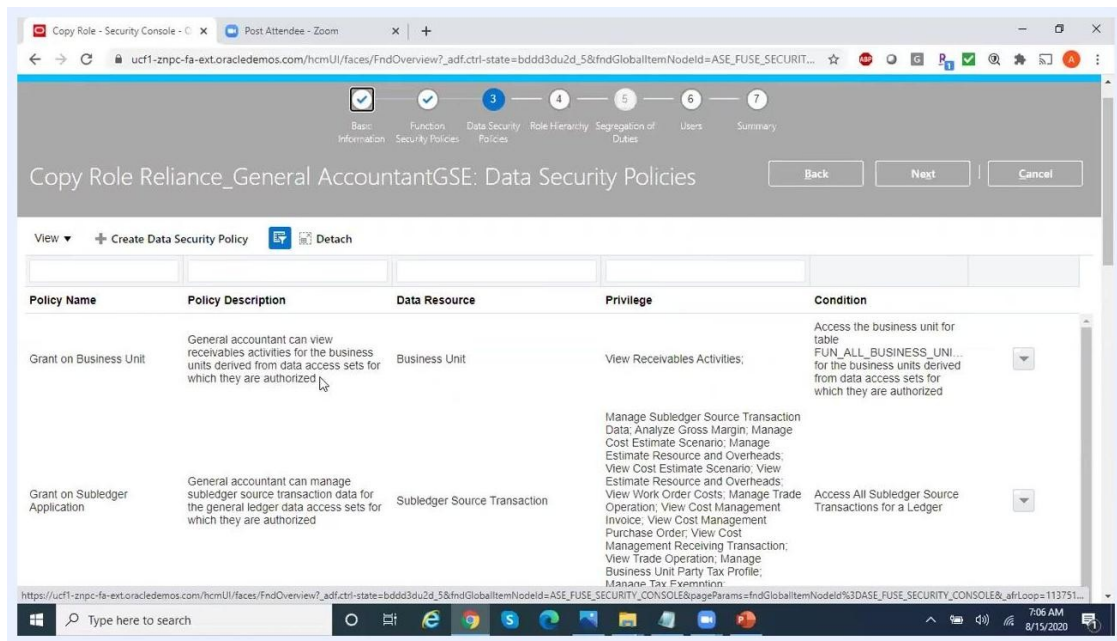
View

Policy Name	Policy Description	Data Resource	Privilege	Condition
Grant on Business Unit	General accountant can view receivables activities for the business units derived from data access sets for which they are authorized	Business Unit	View Receivables Activities;	Access the business unit for table FUN_ALL_BUSINESS_UNI... for the business units derived from data access sets for which they are authorized
Grant on Subledger Application	General accountant can manage subledger source transaction data for the general ledger data access sets for which they are authorized	Subledger Source Transaction	Manage Subledger Source Transaction Data; Analyze Gross Margin; Manage Cost Estimate Scenario; Manage Estimate Resource and Overheads; View Cost Estimate Scenario; View Estimate Resource and Overheads; View Work Order Costs; Manage Trade Operation; View Cost Management Invoice; View Cost Management Purchase Order; View Cost Management Receiving Transaction; View Trade Operation; Manage Business Unit Party Tax Profile; Manage Tax Exemption	Access All Subledger Source Transactions for a Ledger

Data Security Policies screen showing "Grant on Business Unit" and "Grant on Subledger Application" policies, with privileges and conditions listed.

14. Remove unwanted data security policies

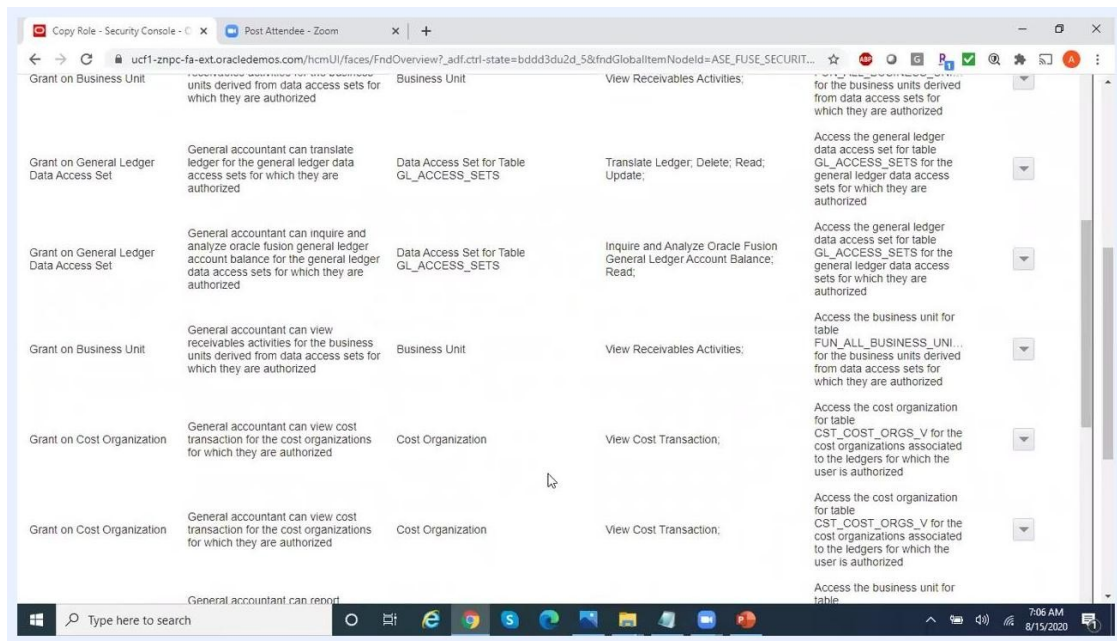
If you do not want the custom role to have access to a specific data security policy — for example, "View Receivables Activities" for business units — select the relevant policy. Click the **Delete** or **Remove Data Security Policy** button, then confirm the deletion when prompted by clicking **Yes**.



Data Security Policies screen with "Grant on Business Unit" policy selected, ready for removal.

15. Locate a data security policy to edit

Scroll through the list of data security policies to identify the one you want to edit. For example, locate the "Grant on Cost Organization" policy, which allows a general accountant to view cost transactions for authorized cost organizations. The policy details appear in columns for Policy Name, Policy Description, Data Resource, Privilege, and Condition.



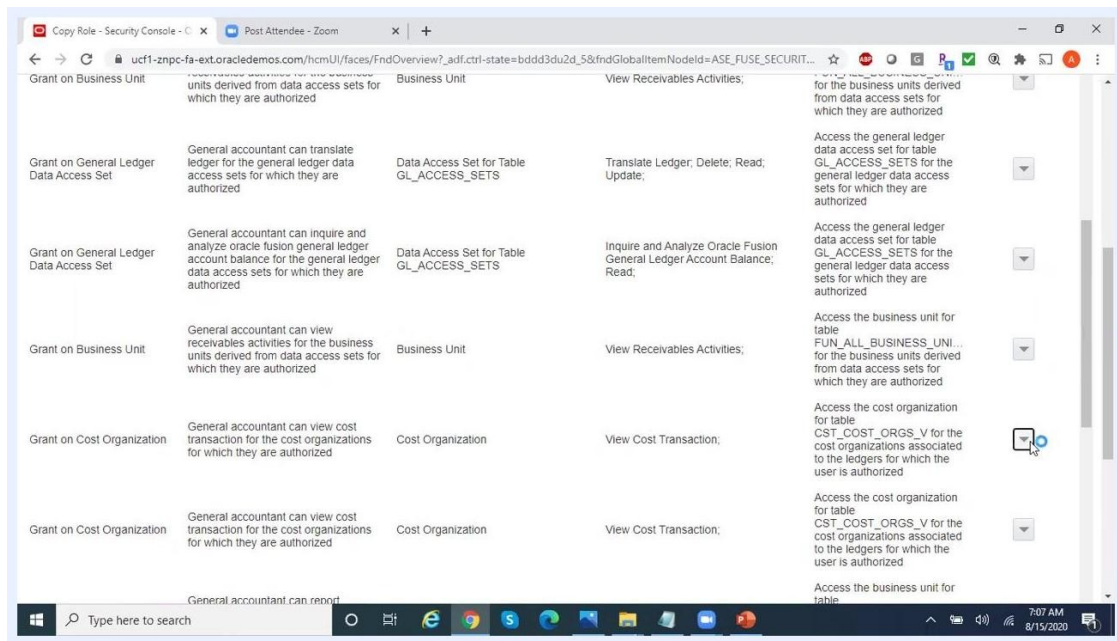
Policy Name	Policy Description	Data Resource	Privilege	Condition
Grant on Business Unit	General accountant can translate ledger for the general ledger data access sets for which they are authorized	Business Unit	Translate Ledger; Delete; Read; Update;	Access the general ledger data access set for table GL_ACCESS_SETS for the business units derived from data access sets for which they are authorized
Grant on General Ledger Data Access Set	General accountant can inquire and analyze oracle fusion general ledger account balance for the general ledger data access sets for which they are authorized	Data Access Set for Table GL_ACCESS_SETS	Inquire and Analyze Oracle Fusion General Ledger Account Balance; Read;	Access the general ledger data access set for table GL_ACCESS_SETS for the general ledger data access sets for which they are authorized
Grant on Business Unit	General accountant can view receivables activities for the business units derived from data access sets for which they are authorized	Business Unit	View Receivables Activities;	Access the business unit for table FUN_ALL_BUSINESS_UNI... for the business units derived from data access sets for which they are authorized
Grant on Cost Organization	General accountant can view cost transaction for the cost organizations for which they are authorized	Cost Organization	View Cost Transaction;	Access the cost organization for table CST_COST_ORGS_V for the cost organizations associated to the ledgers for which the user is authorized
Grant on Cost Organization	General accountant can view cost transaction for the cost organizations for which they are authorized	Cost Organization	View Cost Transaction;	Access the cost organization for table CST_COST_ORGS_V for the cost organizations associated to the ledgers for which the user is authorized

List of data security policies with columns for Policy Name, Policy Description, Data Resource, Privilege, and Condition. Example entries include "Grant on Cost Organization" with privileges like "View Cost Transaction".

Click the edit icon next to the policy you want to modify. The **Edit Data Security Policy** dialog opens, showing the current privileges — for example, the "Actions" dropdown may show "View Cost Transaction." The dialog also includes options for selecting additional privileges such as "View Estimate Costs," "View Planning Cost Organizations," and "View Standard Costs."

16. Add additional privileges to the policy

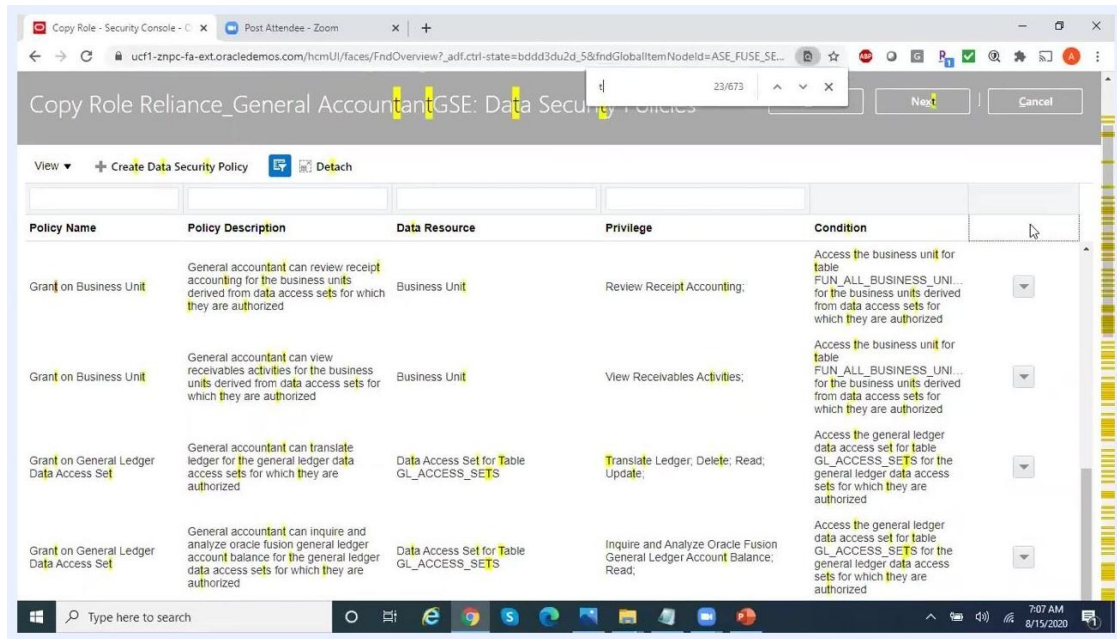
In the **Edit Data Security Policy** dialog, scroll through the list of available privileges and select the ones you need. For example, check both "View Cost Transaction" and "View Item Cost" to allow the role to view both types of data. Make sure the "Policy Description" field accurately reflects the updated privileges, then click **OK** to save your changes.



Edit Data Security Policy dialog with multiple privileges being selected, such as "View Cost Transaction" and "View Item Cost".

17. Confirm the updated policy

After saving, the updated policy appears in the list. Confirm that the new privileges are reflected under the "Privilege" column for the edited policy. You can use the search or filter fields at the top to quickly locate specific policies or privileges.

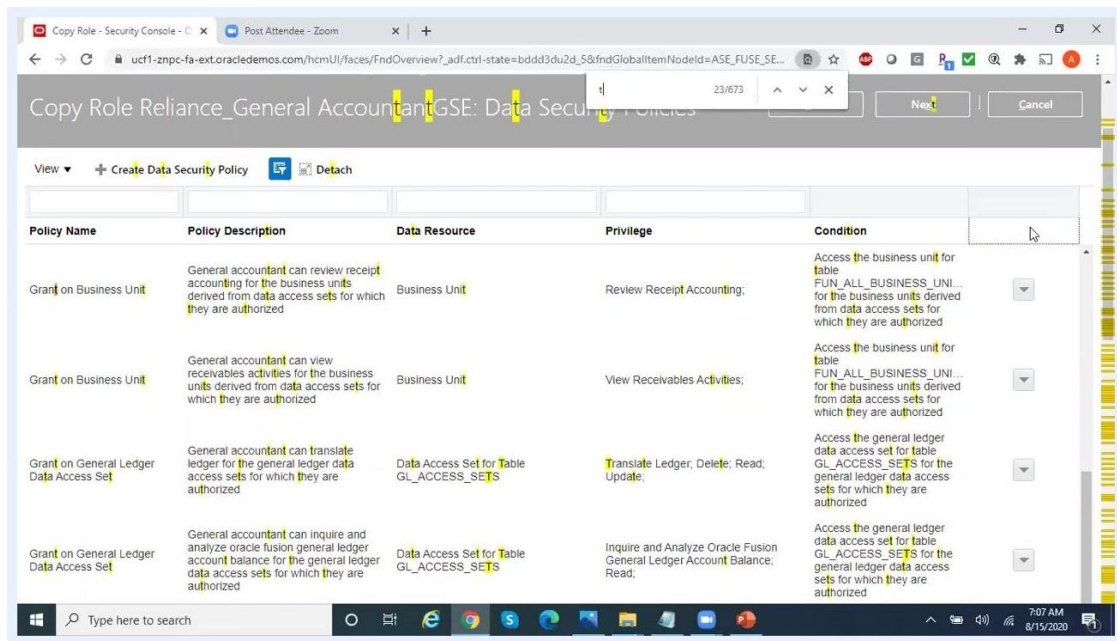


Policy Name	Policy Description	Data Resource	Privilege	Condition
Grant on Business Unit	General accountant can review receipt accounting for the business units derived from data access sets for which they are authorized	Business Unit	Review Receipt Accounting;	Access the business unit for table FUN_ALL_BUSINESS_UNI... for the business units derived from data access sets for which they are authorized
Grant on Business Unit	General accountant can view receivables activities for the business units derived from data access sets for which they are authorized	Business Unit	View Receivables Activities;	Access the business unit for table FUN_ALL_BUSINESS_UNI... for the business units derived from data access sets for which they are authorized
Grant on General Ledger Data Access Set	General accountant can translate ledger for the general ledger data access sets for which they are authorized	Data Access Set for Table GL_ACCESS_SETS	Translate Ledger; Delete; Read; Update;	Access the general ledger data access set for table GL_ACCESS_SETS for the general ledger data access sets for which they are authorized
Grant on General Ledger Data Access Set	General accountant can inquire and analyze oracle fusion general ledger account balance for the general ledger data access sets for which they are authorized	Data Access Set for Table GL_ACCESS_SETS	Inquire and Analyze Oracle Fusion General Ledger Account Balance; Read;	Access the general ledger data access set for table GL_ACCESS_SETS for the general ledger data access sets for which they are authorized

Updated list of data security policies showing new privileges under the "Privilege" column.

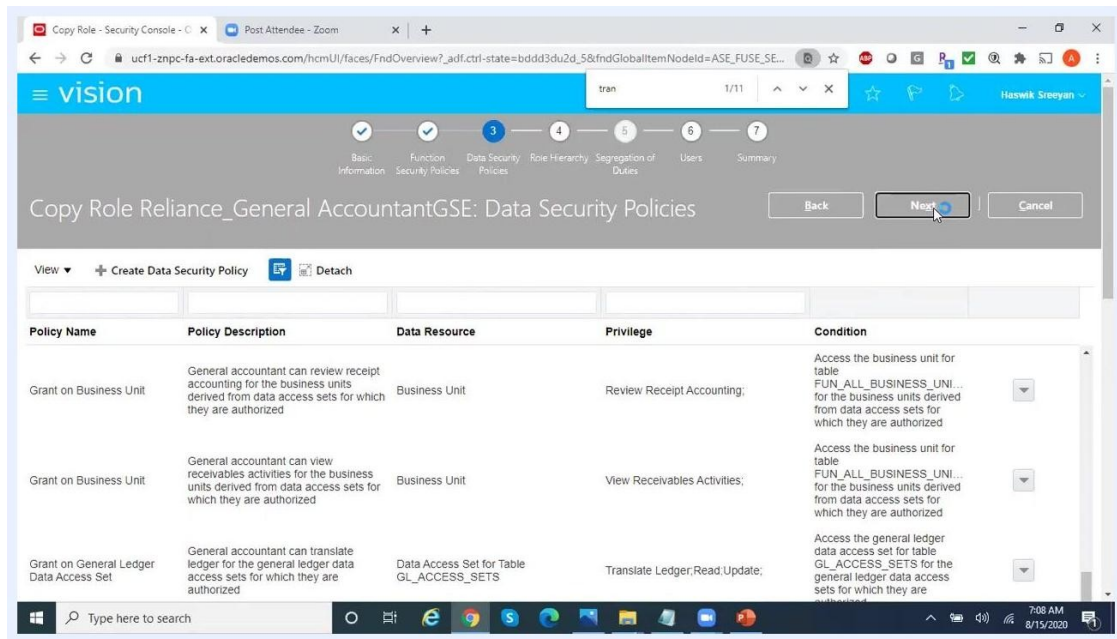
18. Edit privileges for other policies (optional)

If you need to modify privileges for other policies — for example, removing the "Delete" privilege from a translation data policy — locate the relevant policy. Click the edit icon and uncheck the "Delete" privilege, leaving only "Read" and "Update" if required. Save your changes and verify the update in the policy list.



Policy list with a focus on a policy where privileges like "Translate Ledger; Delete; Read; Update" are shown, and the "Delete" privilege is being considered for removal.

Once all necessary edits and additions are complete, click the **Next** button at the top right to continue to the next step in the role setup process.

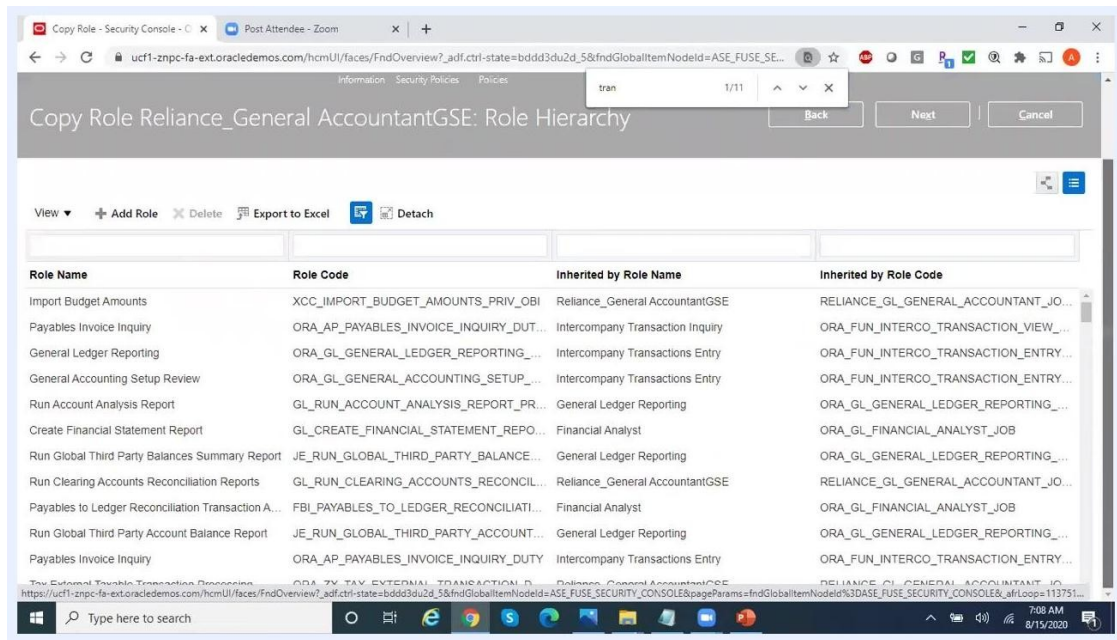


User clicking the "Next" button to proceed after editing data security policies.

Configuring role hierarchy

19. Review the role hierarchy screen

On the "Copy Role Reliance_General AccountantGSE: Role Hierarchy" screen, you see a list of roles with columns for Role Name, Role Code, Inherited by Role Name, and Inherited by Role Code. Common actions available include **Add Role**, **Delete**, **Export to Excel**, and **Detach**.

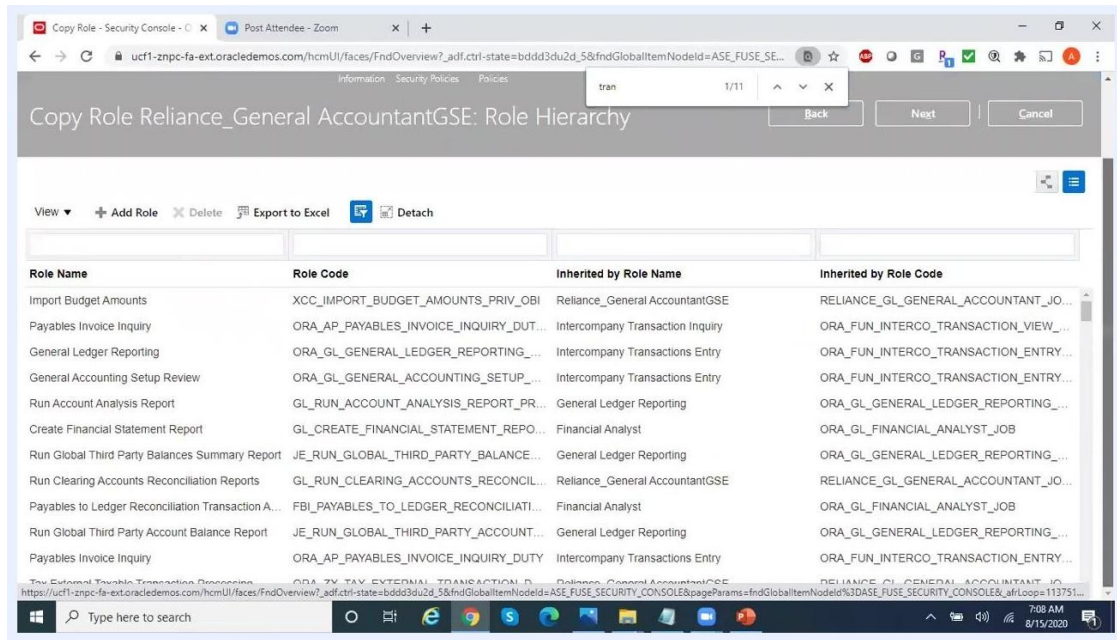


Role Name	Role Code	Inherited by Role Name	Inherited by Role Code
Import Budget Amounts	XCC_IMPORT_BUDGET_AMOUNTS_PRIV_OBI	Reliance_General AccountantGSE	RELIANCE_GL_GENERAL_ACCOUNTANT_JO...
Payables Invoice Inquiry	ORA_AP_PAYABLES_INVOICE_INQUIRY_DUT...	Intercompany Transaction Inquiry	ORA_FUN_INTERCO_TRANSACTION_VIEW...
General Ledger Reporting	ORA_GL_GENERAL_LEDGER_REPORTING_...	Intercompany Transactions Entry	ORA_FUN_INTERCO_TRANSACTION_ENTRY...
General Accounting Setup Review	ORA_GL_GENERAL_ACCOUNTING_SETUP_...	Intercompany Transactions Entry	ORA_FUN_INTERCO_TRANSACTION_ENTRY...
Run Account Analysis Report	GL_RUN_ACCOUNT_ANALYSIS_REPORT_PR...	General Ledger Reporting	ORA_GL_GENERAL_LEDGER_REPORTING...
Create Financial Statement Report	GL_CREATE_FINANCIAL_STATEMENT_REPO...	Financial Analyst	ORA_GL_FINANCIAL_ANALYST_JOB
Run Global Third Party Balances Summary Report	JE_RUN_GLOBAL_THIRD_PARTY_BALANCE...	General Ledger Reporting	ORA_GL_GENERAL_LEDGER_REPORTING...
Run Clearing Accounts Reconciliation Reports	GL_RUN_CLEARING_ACCOUNTS_RECONCIL...	Reliance_General AccountantGSE	RELIANCE_GL_GENERAL_ACCOUNTANT_JO...
Payables to Ledger Reconciliation Transaction A...	FBI_PAYABLES_TO_LEDGER_RECONCILIATI...	Financial Analyst	ORA_GL_FINANCIAL_ANALYST_JOB
Run Global Third Party Account Balance Report	JE_RUN_GLOBAL_THIRD_PARTY_ACCOUNT...	General Ledger Reporting	ORA_GL_GENERAL_LEDGER_REPORTING...
Payables Invoice Inquiry	ORA_AP_PAYABLES_INVOICE_INQUIRY_DUTY	Intercompany Transactions Entry	ORA_FUN_INTERCO_TRANSACTION_ENTRY...

Role Hierarchy screen showing a list of roles, their codes, and inheritance details. The "Add Role" button is visible.

20. Add an additional role to the hierarchy

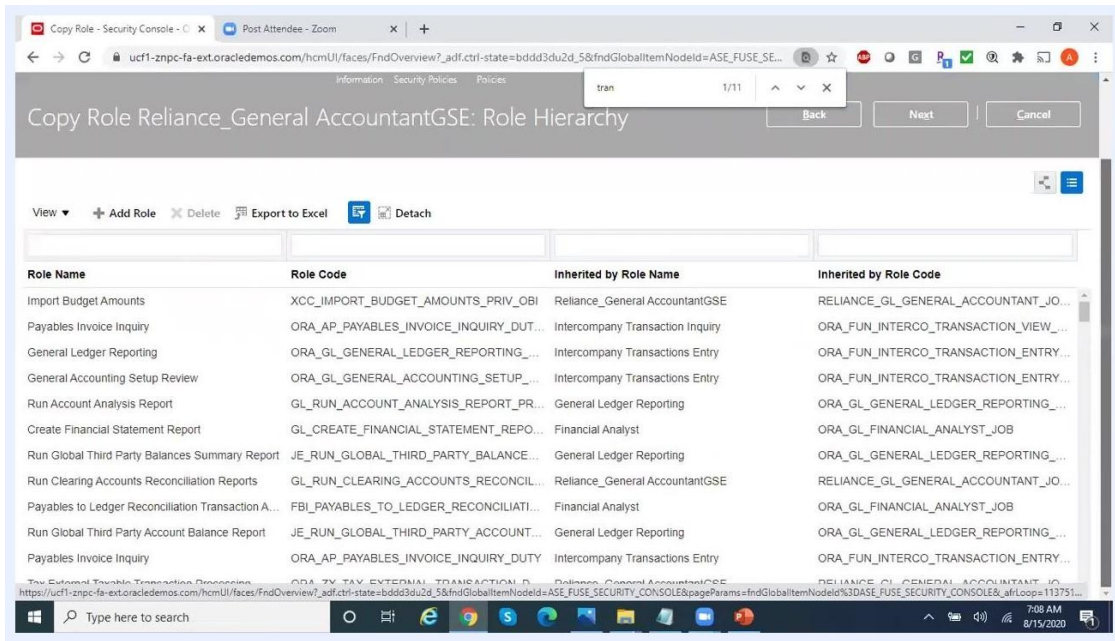
Click the **Add Role** button to open the "Add Role Membership" dialog. In the search box, type the name of the role you want to add — for example, "payables." The system displays matching duty roles and other roles, such as "Payables Administration" (ORA_AP_PAYABLES_ADMINISTRATION_DUTY). Select the role you want from the list.



Add Role Membership dialog open, searching for "payables" and displaying matching roles like "Payables Administration".

21. Proceed to the next step

After selecting the additional role, return to the Role Hierarchy screen and click the **Next** button at the top right to continue.

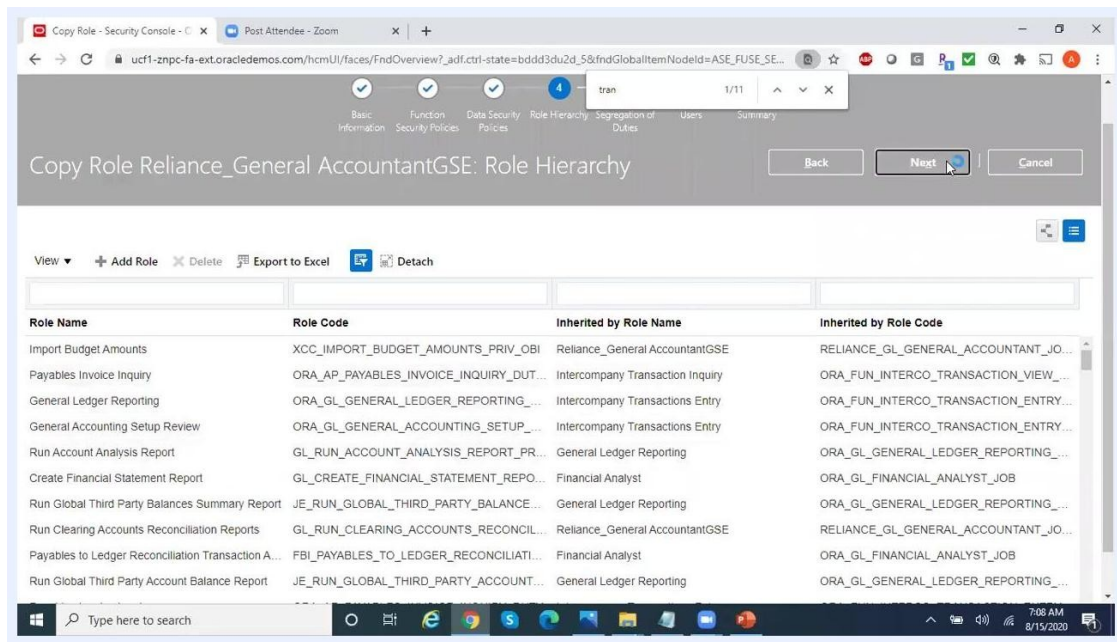


User clicking the "Next" button on the Role Hierarchy screen to proceed.

Assigning the custom role to users

22. Open the Add User dialog

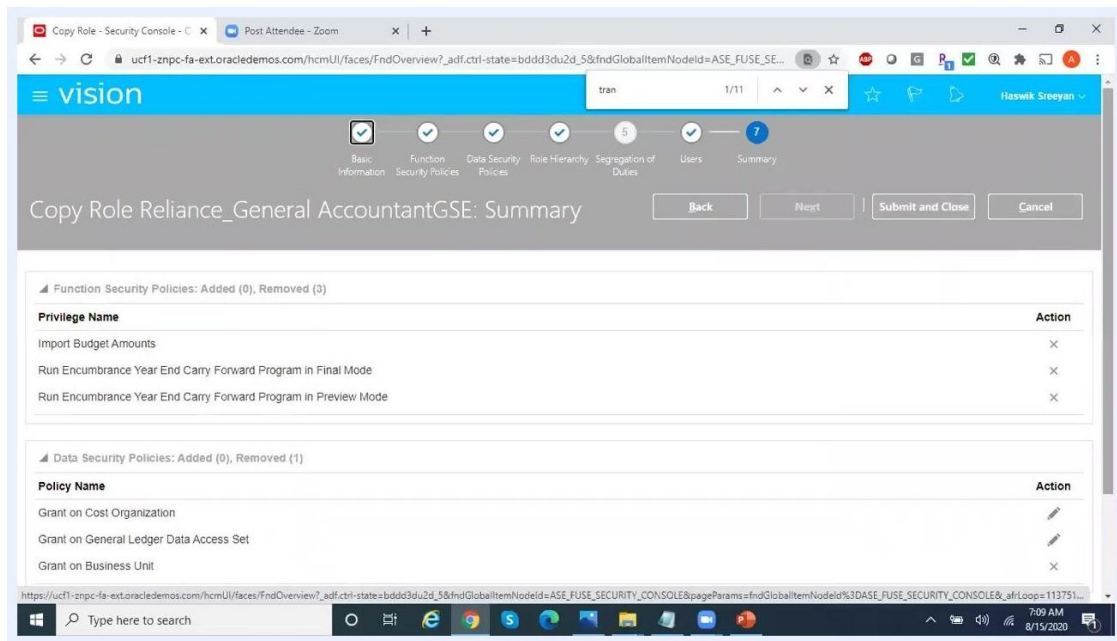
On the "Copy Role Reliance_General AccountantGSE: Users" screen, the user assignment table is initially empty, with columns for User Login, Display Name, and Description. Click the **Add User** button on the right.



Users screen with an empty user assignment table and the "Add User" button visible.

23. Search for and select the user

In the "Add User" dialog, enter the user's name or login — for example, "HSre." The system displays matching users, such as "Haswik Sreeyan" with user login "hsreeyan1." Select the appropriate user from the list.



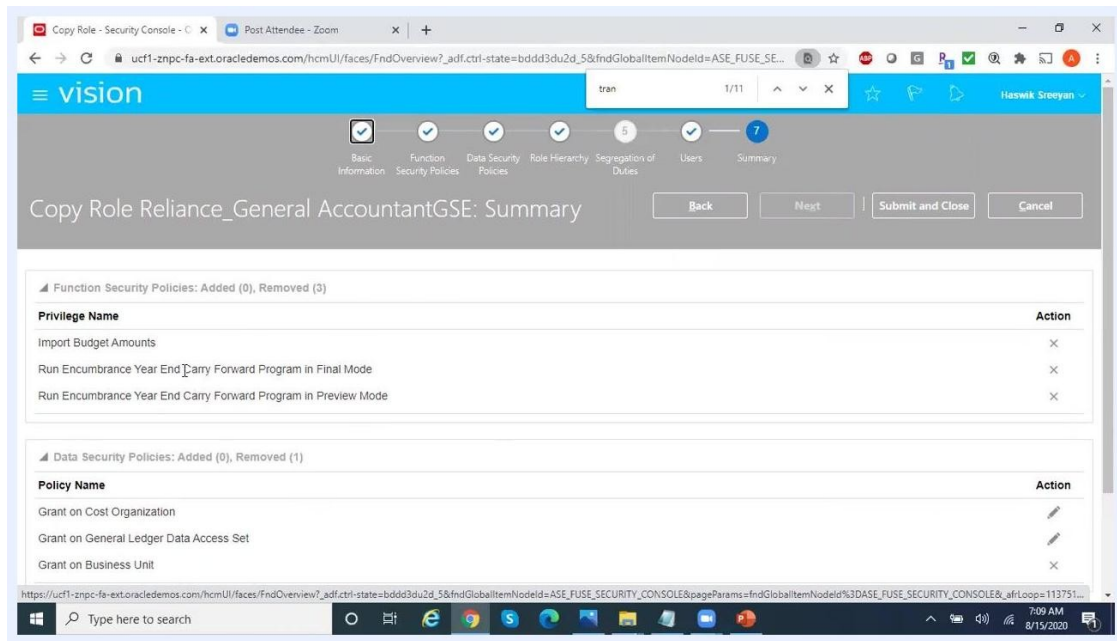
Add User dialog open, searching for "HSre" and displaying matching users.

24. Review the summary of changes

After assigning the user, the "Copy Role Reliance_General AccountantGSE: Summary" screen appears, displaying:

- **Function Security Policies:** Added or removed privileges.
- **Data Security Policies:** Added or removed policies.
- **Role Hierarchy:** Added or removed roles.
- **Users:** Added or removed users.

Review the listed changes, such as removed privileges like "Import Budget Amounts" and "Run Encumbrance Year End Carry Forward Program in Final Mode," data security policies like "Grant on Cost Organization" and "Grant on General Ledger Data Access Set," the "Payables Administration" role added to the hierarchy, and the selected user added.



Summary screen showing all changes: privileges, data security policies, role hierarchy, and users. "Submit and Close" button is visible.

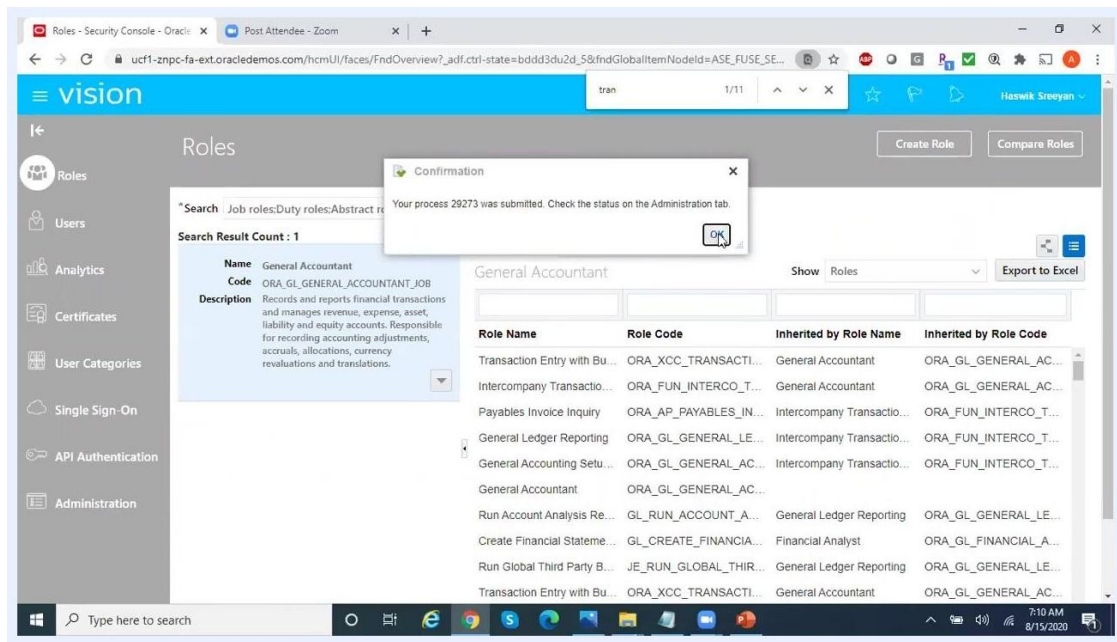
25. Submit and close

Once you have reviewed all changes and confirmed their accuracy, click the **Submit and Close** button to finalize the role configuration and assignments.

Monitoring and verifying the role copy process

26. Confirm the role copy submission

After submitting your changes, a **Confirmation** dialog appears, displaying a message such as: "Your process 29273 was submitted. Check the status on the Administration tab." Click the **OK** button to close the dialog.



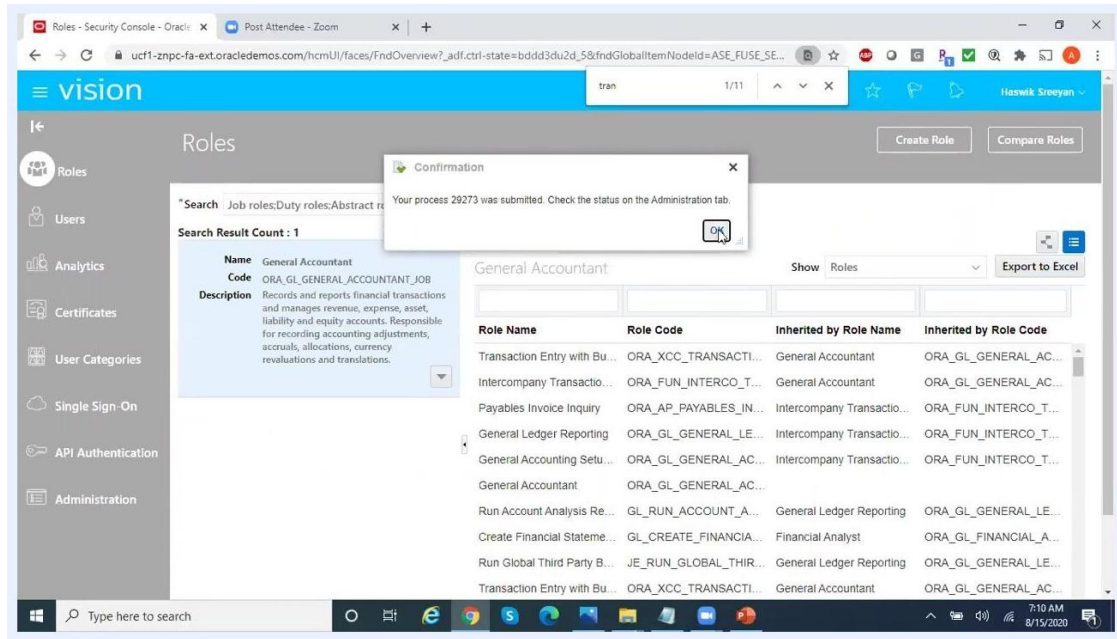
Confirmation dialog stating "Your process 29273 was submitted. Check the status on the Administration tab." with an OK button. The Roles screen is visible in the background.

27. Navigate to the Administration tab

In the left navigation pane, click **Administration**. The **Administration** screen appears, defaulting to the **Role Copy Status** tab, which lists:

- **Process:** Unique process IDs (for example, 29273).
- **Role Code:** The code of the role being copied or modified (for example, RELIANCE_GL_GENERAL_ACCOUNTANT_JOB_GSE).
- **Status:** The current status of each process (for example, Processing or Complete).

Click the **Refresh** button to update the status.



Administration screen, Role Copy Status tab, showing a list of process IDs, role codes, and their statuses. The Refresh button is highlighted.

28. Verify completion of the role copy process

Wait for the status of your process (for example, 29273) to change from **Processing** to **Complete**. Confirm that the process for your role code is now marked as **Complete** in the status column.

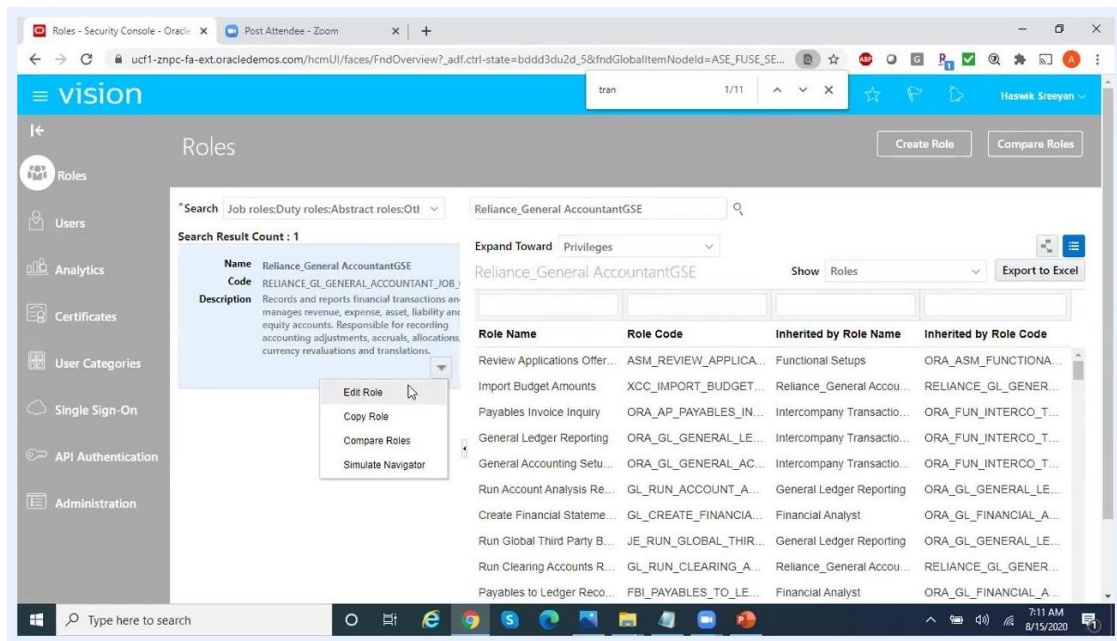
The screenshot shows the Oracle Vision Administration console. The left sidebar contains navigation links for Roles, Users, Analytics, Certificates, User Categories, Single Sign-On, API Authentication, and Administration. The main content area is titled 'Administration' and has tabs for General, Roles, Role Copy Status, and Bridge for Active Directory. The 'Role Copy Status' tab is active, displaying a table with the following data:

Process	Role Code	Status
29273	RELANCE_GL_GENERAL_ACCOUNTANT_JOB_GSE	Processing
29272	11_GL_GENERAL_ACCOUNTANT_JOB_GSE	Complete
29271	TEST_GL_FINANCIAL_ANALYST_JOB_GSE	Complete
29270	Test_AP_PAYABLES_ADMINISTRATION_DUTY_GSE	Complete
29269	Test_GL_GENERAL_ACCOUNTANT_JOB_GSE	Complete
28269	GL_GENERAL_ACCOUNTANT_FFIZER	Complete
27269	27sAP_ACCOUNTS_PAYABLE_MANAGER_JOB_GSE	Complete
26271	ZPM_CHANNEL_ACCOUNT_MANAGER_JOB_WITH_OPU	Complete
26270	ZBS_SALES_REPRESENTATIVE_JOB_WITHPARTNER33	Complete

Role Copy Status table showing process 29273 for RELIANCE_GL_GENERAL_ACCOUNTANT_JOB_GSE marked as Complete.

29. Search for users and manage user accounts

To verify user assignments or manage user accounts, click **Users** in the left navigation pane. The **User Accounts** screen appears. Use the search bar to enter at least 3 characters and search for a user by display name or user ID. The search results display matching users, their status, and available actions.

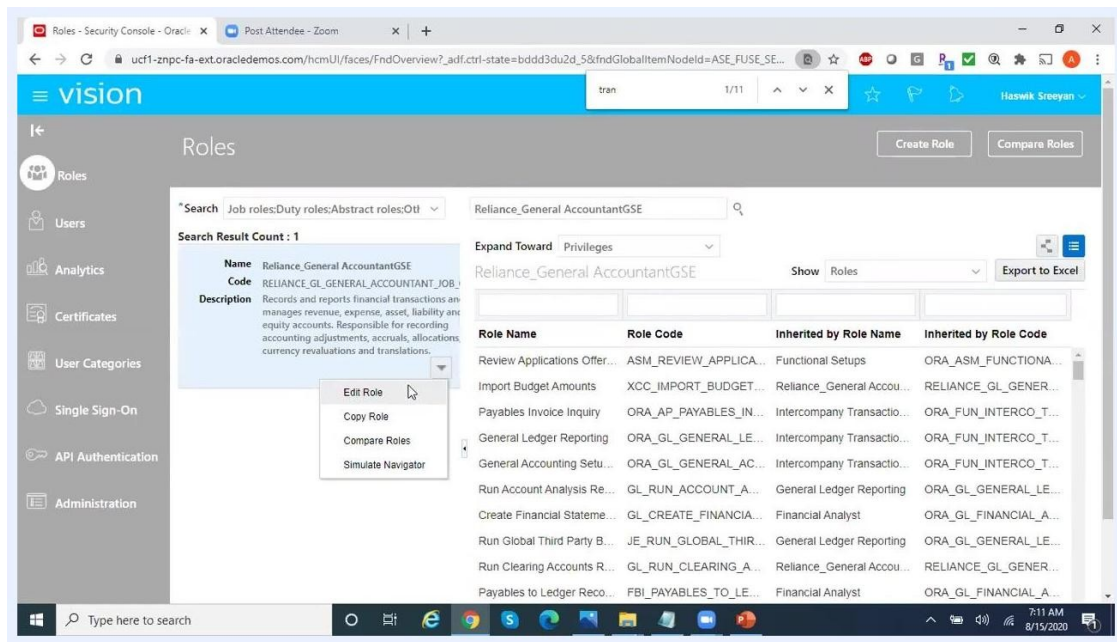


User Accounts screen with a search bar and empty results table. "Add User Account" button is visible.

Editing or comparing roles after creation

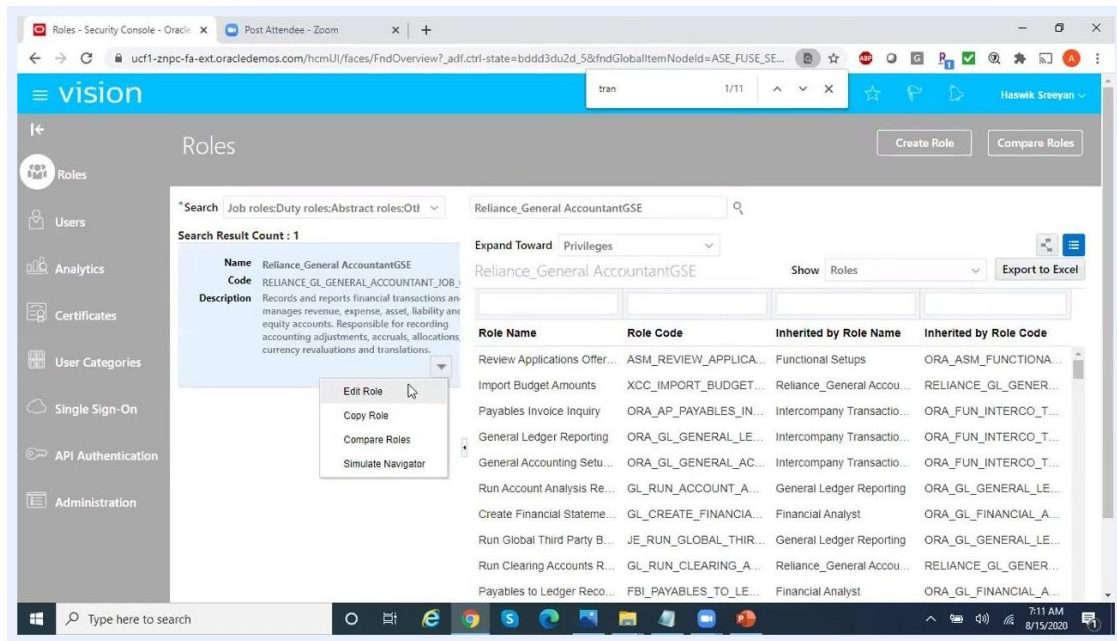
30. Edit the custom role

To make further changes to a role, return to the **Roles** section and search for the desired role — for example, Reliance_General AccountantGSE. Click the dropdown arrow next to the role name and select **Edit Role**.



Roles screen with the dropdown menu open for Reliance_General AccountantGSE, showing options: Edit Role, Copy Role, Compare Roles, Simulate Navigator.

The **Edit Role** wizard opens, where you can review and modify **Function Security Policies** (privileges and resources), and navigate through steps such as Data Security Policies, Role Hierarchy, Segregation of Duties, Users, and Summary. Use the **Back**, **Next**, or **Cancel** buttons to navigate or exit.

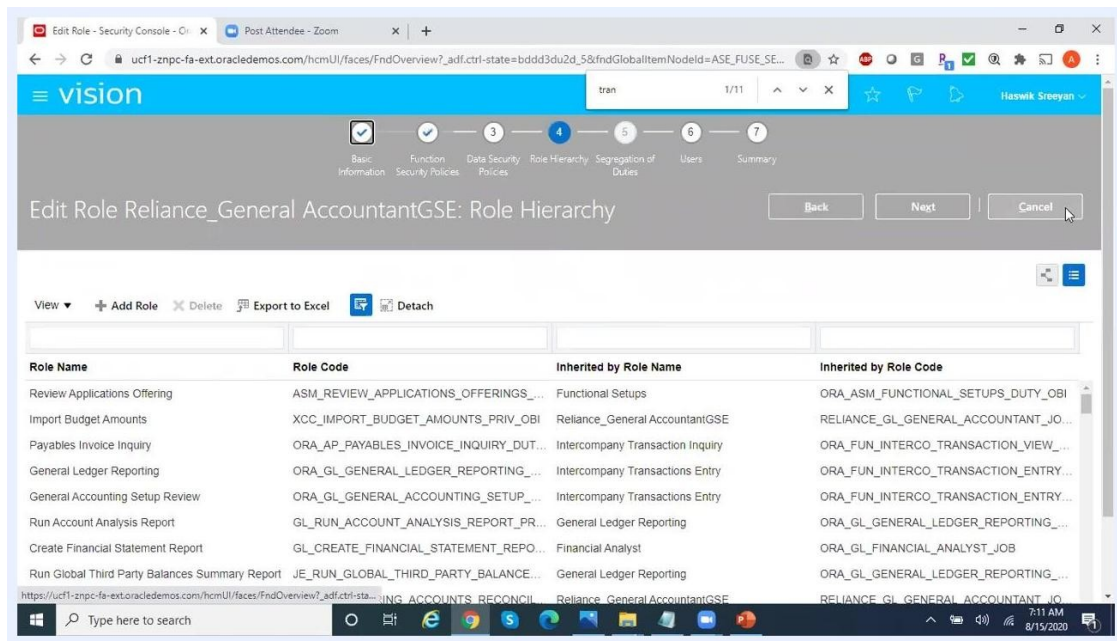


Edit Role wizard open at Function Security Policies step, listing privileges and descriptions. Navigation steps are visible at the top.

To compare the current role with another, select **Compare Roles** from the dropdown menu instead.

31. Review and modify the role hierarchy

In the Edit Role wizard, navigate to the **Role Hierarchy** step to review the list of inherited roles, their codes, and relationships. Use options such as **Add Role**, **Delete**, **Export to Excel**, or **Detach** as needed.

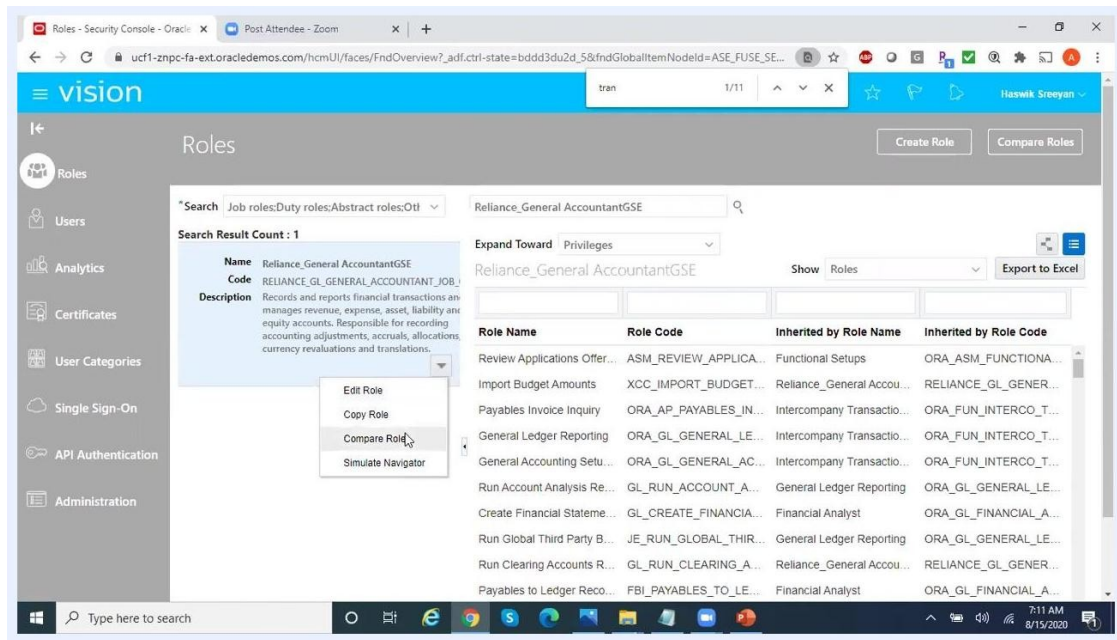


Edit Role wizard at the Role Hierarchy step, showing a list of inherited roles and their codes. Action buttons are visible.

Comparing roles

32. Search for the role to compare

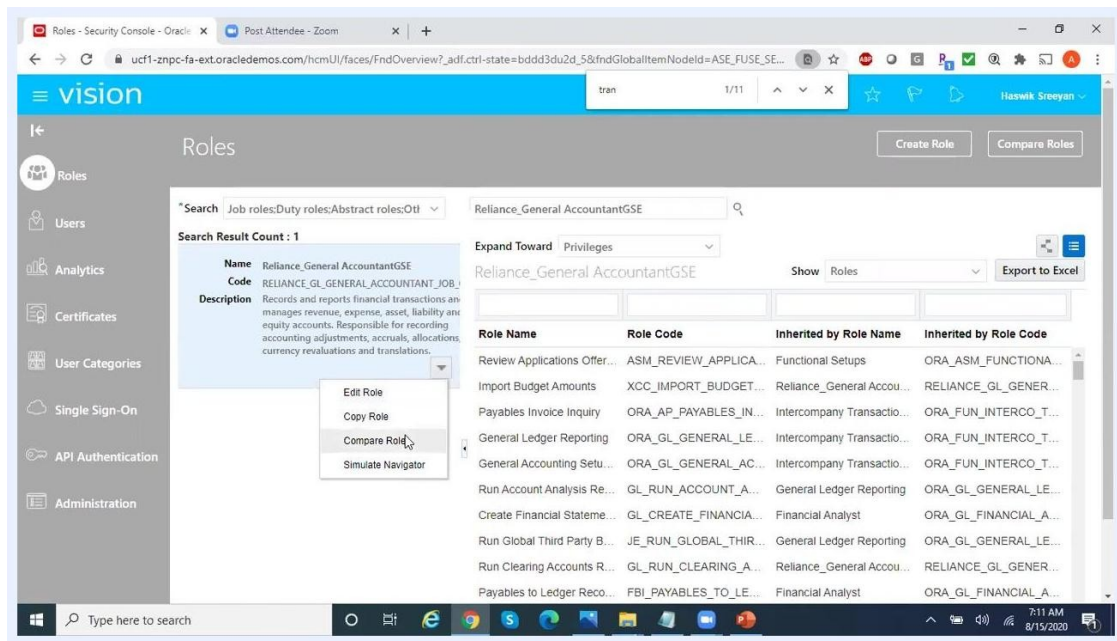
In the "Roles" section, use the search bar to enter the role name, for example [Reliance_General AccountantGSE](#). Review the search results, which display the role's Name, Code, and Description. Click the dropdown arrow next to the role name and select **Compare Role** from the context menu.



The Roles screen with the [Reliance_General AccountantGSE](#) role selected, context menu open, and "Compare Role" highlighted.

33. Select a second role for comparison

On the "Compare Roles" screen, the selected role ([Reliance_General AccountantGSE](#)) is set as the *First Role*. In the *Second Role* field, start typing the name of the role you want to compare — for example, [Financial](#). A dropdown list of matching roles appears; select [Financial Analyst](#) from the list.



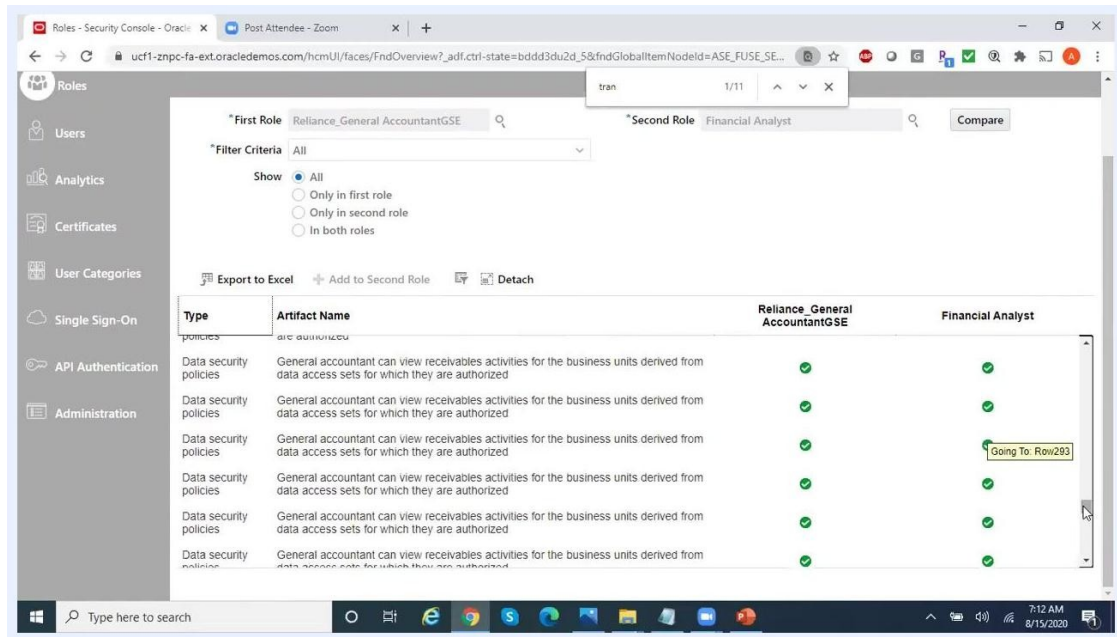
The Compare Roles screen with the "Second Role" search box open and a list of roles matching "financial" displayed.

34. Configure the comparison criteria

Under *Filter Criteria*, ensure "All" is selected to compare all available policies and roles. Under *Show*, you can choose:

- **All** (default): Shows all policies and roles.
- **Only in first role**: Shows items unique to the first role.
- **Only in second role**: Shows items unique to the second role.
- **In both roles**: Shows items common to both roles.

Use the checkboxes to include or exclude function security policies, data security policies, and inherited roles. Make sure all checkboxes are selected for a comprehensive comparison.



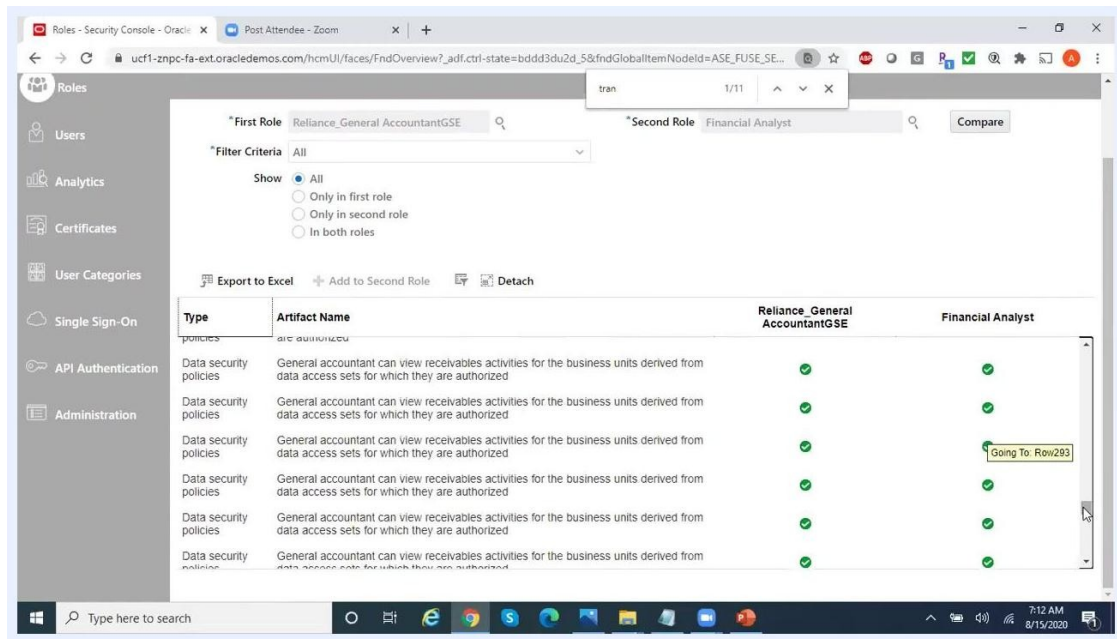
The Compare Roles screen with filter options expanded, showing checkboxes for function security policies, data security policies, and inherited roles.

35. Review the comparison results

The results table displays the comparison between the two roles, with columns for:

- **Type:** The type of policy or role (for example, Function security policies, Data security policies, Inherited roles).
- **Artifact Name:** The specific privilege or policy.
- **Reliance_General AccountantGSE:** Indicates whether the artifact is present in this role (green checkmark for present, red minus for absent).
- **Financial Analyst:** Indicates whether the artifact is present in this role (green checkmark for present, red minus for absent).

Scroll through the list to analyze which policies and roles are available in each role.



The Compare Roles screen showing a table with artifact names and presence indicators (green checkmarks and red minuses) for each role.

36. Analyze detailed privileges

Continue scrolling to view more detailed data security policies and inherited roles. Use the "Export to Excel" button if you need to analyze the results outside the application. The table updates as you scroll, showing additional privileges and their availability in each role.

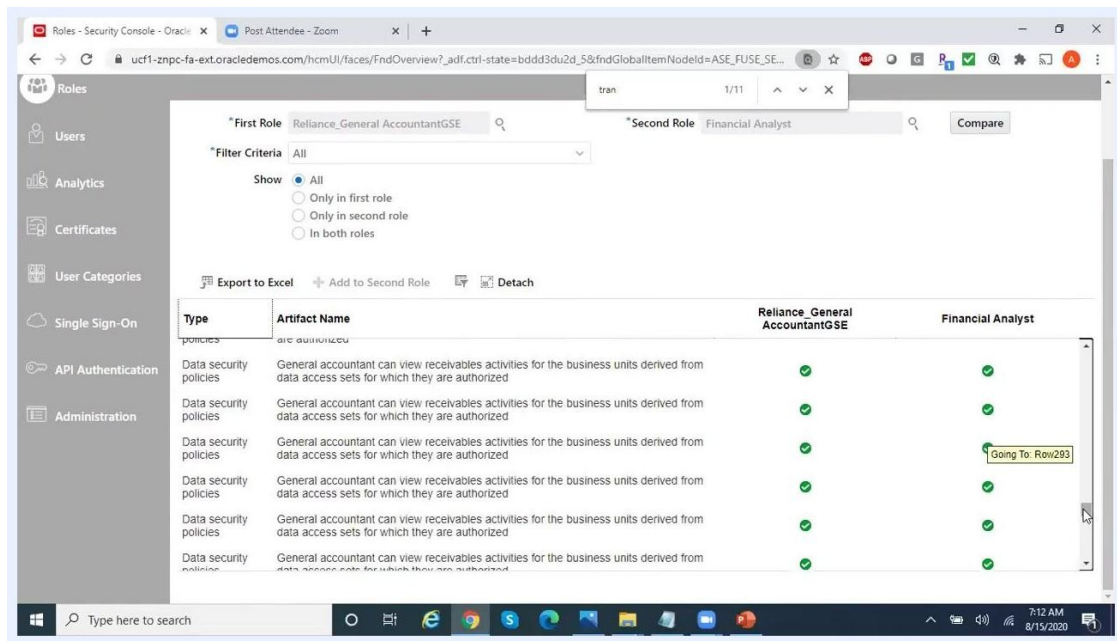
The screenshot shows the Oracle Roles - Security Console interface. The left sidebar contains navigation links: Roles, Users, Analytics, Certificates, User Categories, Single Sign-On, API Authentication, and Administration. The main content area is titled "Compare Roles" and shows a comparison between two roles: "Reliance_General AccountantGSE" (First Role) and "Financial Analyst" (Second Role). The "Filter Criteria" is set to "All". The "Show" options are "All", "Only in first role", "Only in second role", and "In both roles". The "Export to Excel" button is visible. The table below lists data security policies and their presence in each role.

Type	Artifact Name	Reliance_General AccountantGSE	Financial Analyst
Data security policies	General accountant can view receivables activities for the business units derived from data access sets for which they are authorized	✓	✓
Data security policies	General accountant can view receivables activities for the business units derived from data access sets for which they are authorized	✓	✓
Data security policies	General accountant can view receivables activities for the business units derived from data access sets for which they are authorized	✓	✓
Data security policies	General accountant can view receivables activities for the business units derived from data access sets for which they are authorized	✓	✓
Data security policies	General accountant can view receivables activities for the business units derived from data access sets for which they are authorized	✓	✓
Data security policies	General accountant can view receivables activities for the business units derived from data access sets for which they are authorized	✓	✓

The Compare Roles screen with a detailed list of data security policies and inherited roles, showing presence indicators for each role.

37. Complete the comparison

Once you have finished reviewing the comparison, click **Done** to exit the comparison screen. You can use the comparison results to help create a custom role or assign roles to users as appropriate.



The Compare Roles screen with the comparison complete, showing inherited roles and their presence in each role.

What's next

By following these steps, you have learned how to create a custom role in Oracle Fusion by copying a standard role, adjusting its function and data security policies, configuring its role hierarchy, and assigning it to users. You can now use the Administration tab to monitor role copy status, the User Accounts screen to manage user assignments, and the Compare Roles feature to validate your custom role against other roles as your organization's security requirements evolve.