

How To Access Fusion Setup Pages In Read Only Mode

Setup to be done

1. Navigate to Setup and Maintenance > Task > Search> "Manage Administrator Profile Values" task

The screenshot shows the Oracle Fusion Setup interface. At the top is the Oracle logo and a search bar. Below the header, the page title is "Manage Profile Options". There is a "Search" section with input fields for "Profile Option Code" (containing "FND_READ"), "Profile Display Name", "Application", and "Module". Below the search fields, the "Search Results" section is titled "Search Results : Profile Options". It includes a toolbar with "Actions", "View", and a "Detach" icon. A table displays the search results with columns: Profile Option Code, Profile Display Name, Application, Module, Start Date, End Date, and Description. One result is shown for "FND_READ_ONLY_MODE".

Profile Option Code	Profile Display Name	Application	Module	Start Date	End Date	Description
FND_READ_ONLY_MODE	Read Only Mode	Oracle Middleware Exten...	Oracle Middleware Exten...	19.09.2013		Enable all applications to be read-only for a specified user.

2. Enable profile option 'FND_READ_ONLY_MODE' at user level

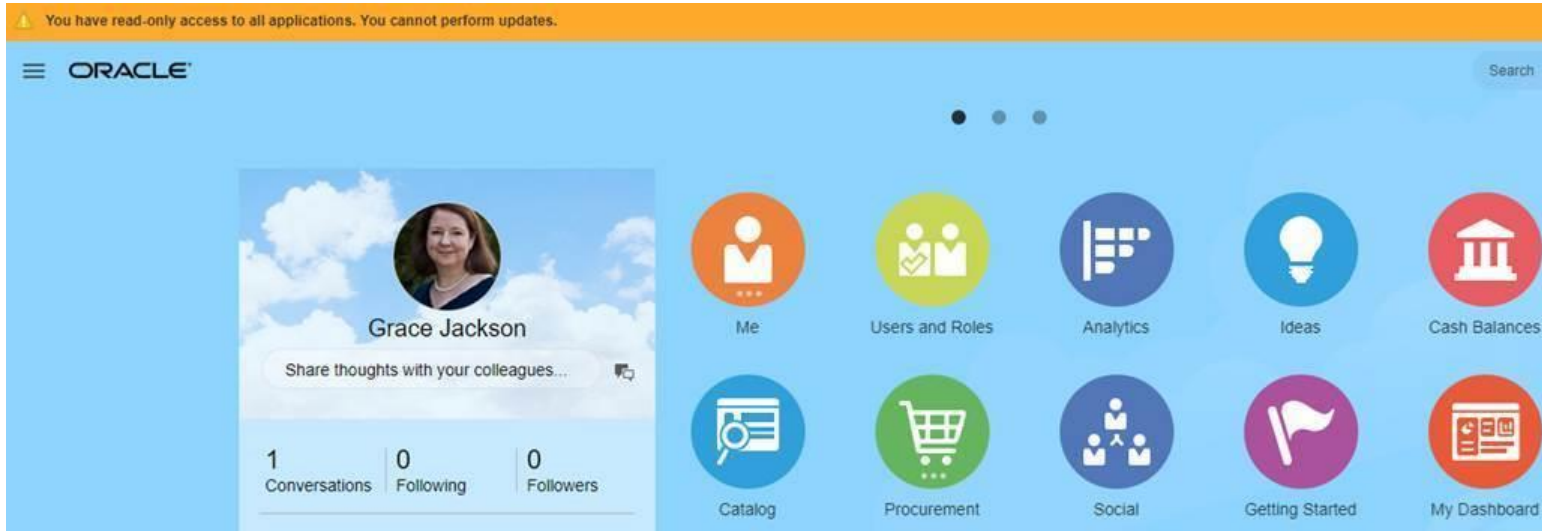
▲ FND_READ_ONLY_MODE: Profile Values

Actions ▼ View ▼ + ×   Detach

* Profile Level	Product Name	User Name	▲ ▼ Profile Value
User		EXTN_OKC_CONMGR_VIEW	Enabled
User		FINUSER1	Enabled
User		FIN_APP_ADMIN_OPERATIONS	Enabled

How it Works

1. When the user with read only access logs into the environment there shall be a red band displayed above the global menu in all the pages user navigates. The band displays a message that the user has read only access to the application and cannot make any updates.



2. When user navigates to the setup pages and as soon as the pages loads there is a message stating that user has ready only access ("You have read-only access to all applications. You cannot perform updates. (FND-3319)") and cannot make any updates.

If user edits the data and saves the data same error message is displayed again.

Oracle Manage Common Options for Payables and Procurement

Business Unit: Vision Operations

Default Distributions

* Liability	01-000-2210-0000-000
* Prepayment	01-000-1340-0000-000
Bill Payable	01-000-2580-0000-000
* Conversion Rate Variance Gain	01-740-7842-0000-000
* Conversion Rate Variance Loss	01-740-7844-0000-000
* Discount Taken	01-740-7825-0000-000
Miscellaneous	01-110-7210-0000-000
Freight	01-580-7740-0000-000
Prepayment Tax Difference	01-580-7740-0000-000
* Realized Gain Distribution	01-740-7842-0000-000
* Realized Loss Distribution	01-740-7844-0000-000

Automatic Offsets

Offset Segments: ☒ None
☐ Primary balancing segment
☐ All segments, except natural account

Currency Conversion

☒ Require conversion rate entry
 Conversion Rate Type: Corporate

Expense Accruals

Accrue Expense Items: At receipt

Self-Billed Invoices

☐ Gapless invoice numbering

Legal Entity Information

VAT Registration Member State: United States
 Bill-to Location: V1- New York City

Error
 You have read-only access to all applications. You cannot perform updates. (FND-3319)
 OK

For customers looking for read only access to the Payables application, so far we had supported read only access to only the transaction pages (invoice/payment pages) using read only duty roles. There was no such provision to access the setup pages in read only mode. Now users can access the setups pages in read only mode by enabling the profile option.

When this profile option is enabled at a user level it will grant read only access to the setup pages in the application.

How to create a Read Only Project Accountant role to just view the Project Costs in Fusion PPM ?

Solution

To view project costs in a read-only mode, here's what needs to be done:

1. Create a custom role and grant the following functional privileges:

- Manage Project Cost Activities
- Manage Project Expenditure Item
- View Project Expenditure Item Borrowed and Lent Distribution Lines
- View Project Expenditure Item Cost Distribution Lines
- View Project Labor Cost

2. Grant the following data security policy to this custom role:

- Data Resource: Business Unit
- Data Set: Select by instance set
- Condition Name: Access the business units for which the user is explicitly authorized
- Actions: Manage Project Expenditure Item

3. Assign this role to the user who you want to have read-only access to view project costs.

4. Grant data access to this user to the relevant business units for which you want the data to be viewed using the Manage Data Access for Users setup task.

The above user can now navigate to the Manage Project Costs page and view project costs but can't take any actions/perform adjustments on them.

How to create read only role to view project costs?

Solution

To view project costs in a read-only mode, here's what needs to be done:

1. Create a custom role and grant the following functional privileges:

- Manage Project Cost Activities
- Manage Project Expenditure Item
- View Project Expenditure Item Borrowed and Lent Distribution Lines
- View Project Expenditure Item Cost Distribution Lines
- View Project Labor Cost

2. Grant the following data security policy to this custom role:

- Data Resource: Business Unit
- Data Set: Select by instance set
- Condition Name: Access the business units for which the user is explicitly authorized
- Actions: Manage Project Expenditure Item

3. Assign this role to the user who you want to have read-only access to view project costs.

4. Grant data access to this user to the relevant business units for which you want the data to be viewed using the Manage Data Access for Users setup task.

The above user can now navigate to the Manage Project Costs page and view project costs but can't take any actions/perform adjustments on them.

The customer created View Only Custom Role and after giving to the users the view only privileges, they are still able to update and save customer details.

Solution

In Oracle Fusion Receivables there is no possibility to achieve the same. For this functionality the following Enhancement Requests have been opened:

ENH 22727557 - VIEW ONLY ROLE FOR AR > BILLING > MANAGE CUSTOMERS

How to Create Read-Only / View Only Custom Role for Transactions & Receipts ?

Solution

To create a role to grant only view privileges for Transactions and Receipts:

I.

1. Functional Security Policies:

ORA_AR_RECEIVABLE_INQUIRY_DUTY

XLA_REVIEW_SUBLEDGER_JOURNAL_ENTRY_PRIV

2. Data Security Policies:

> Business Unit:

Data Set: Select by instance set

Condition Name: Access the business units for which the user is explicitly authorized

Actions Enabled:

Manage Receivables Activities

Manage Receivables Activity data

Manage Receivables Receipts

Manage Receivables Transactions

View Receivables Activities

> SetID Set:

Data Set: Select by instance set

Condition Name: Access the application reference data sets for which the user is explicitly authorized

Actions Enabled:

Manage Customer Account Relationship

Manage Customer Account Site

Manage Customer Account Site Use

Manage Trading Community Salesperson Setup

View Customer Account Relationship

View Customer Account Site

View Customer Account Site Use

View Trading Community Salesperson Setup

> Trading Community Customer Account

Data Set: All values

Actions Enabled:

Read

View Customer Account

> Trading Community Customer Account Site

Data Set: All values

Actions Enabled:

Read

View Customer Account Site

> Trading Community Customer Account Site Use

Data Set: All value

Actions Enabled:

Read

View Customer Account Site Use

3. Save and close

II.

Add the new role to the user along with the Employee role (ORA_PER_EMPLOYEE_ABSTRACT)

III.

Go to Task: Setup and Maintenance > Manage Data Access For Users

Grant the Business Unit access to the user for the custom role along with Reference Data Set.

IV.

Go to Scheduled Processes

1. Run Ess Job: Send Pending LDAP Requests
2. Run Ess Job: Import User and Role Application Security Data
3. Run Ess Job: Retrieve Latest LDAP Changes
4. Sign out and Sign in again to the application.

.....

Oracle Inventory Management Inventory Management View Only Role

The first step in the process is to create a custom job role for Inventory Inquiry. In order to create a new job role, you must navigate to Oracle Security Console. To access Oracle Security Console, navigate to the main menu navigator and select 'Security Console' under 'Tools.'

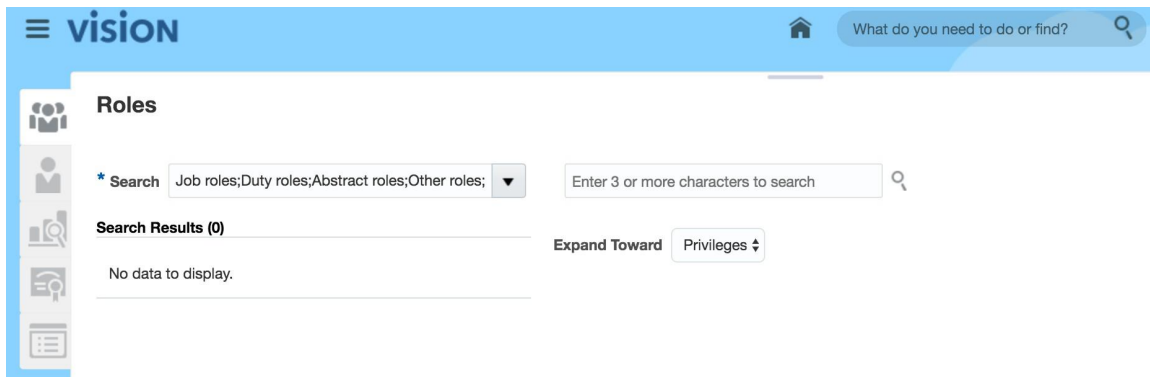


Figure 1 Security Console

Click the 'Create Role' button to create a new job role.

You need to complete the basic information when defining a new job role. Enter the Role Name, Role Code, Role Category, and Description. The Role Category Name is SCM – Job Roles. In the example, the role name 'Inventory View Only Job Role' has been entered as the role name. The role name should be intuitive and reflect the access provided to the user by assigning the job role.

The screenshot shows the 'Edit Role' page in the Oracle Vision Security Console. The page has a blue header with the 'vision' logo and a search bar. Below the header is a navigation bar with four tabs: 'Basic Information', 'Function Security Policies', 'Data Security Policies', and 'Role Hierarchy'. The 'Basic Information' tab is selected. The main content area is titled 'Edit Role Inventory View Only Job Role: Basic Information'. It contains several fields: 'Role Name' (Inventory View Only Job Role), 'Role Code' (INV_VIEW_ONLY_JOB_ROLE), 'Role Category' (SCM - Job Roles), and 'Description' (Inventory view only job role.). There is also a checkbox for 'Predefined role' which is unchecked.

Figure 2 Create Job Role

The next step is to assign the newly create job role to the appropriate users.

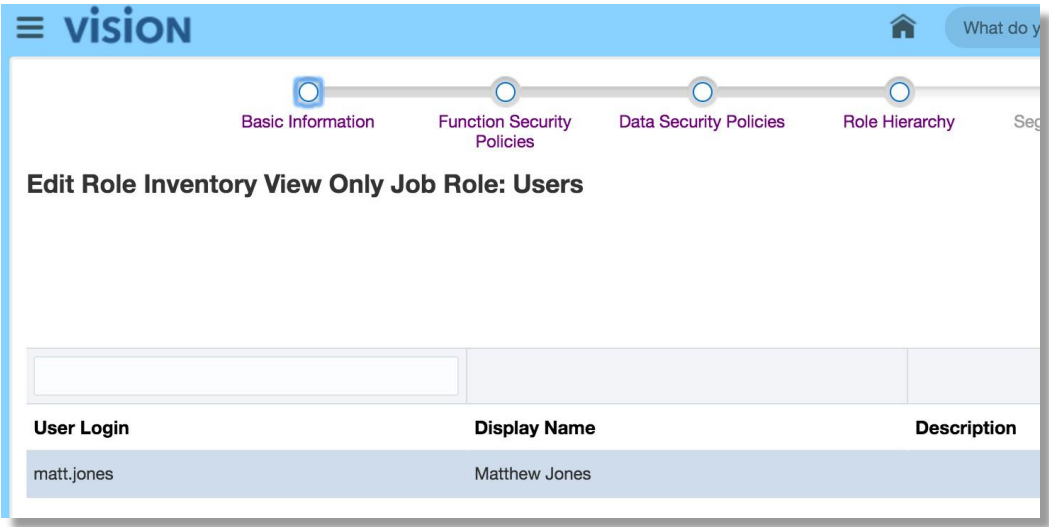


Figure 3 Assign Job Role to User

Create Inventory View Only Duty Role

Once the job role has been created successfully, the next step in the process is to create a new duty role. The duty role is created in Oracle Security Console.

You need to complete the basic information when defining a new duty role. Enter the Role Name, Role Code, Role Category, and Description. The Role Category is SCM – Duty Roles. In the example, the role name 'Inventory View Only Duty Role' has been entered as the role name. The role name should be intuitive and reflect the access provided to the user by assigning the job role.

The screenshot shows a web application interface with a blue header bar containing the 'vision' logo and a home icon. Below the header, there is a horizontal navigation bar with four tabs: 'Basic Information' (selected), 'Function Security Policies', 'Data Security Policies', and 'Role Hierarchy'. The main content area is titled 'Edit Role Inventory View Only Duty Role: Basic Information'. It contains several form fields: a required 'Role Name' field with the value 'Inventory View Only Duty Role', a 'Role Code' field with the value 'INV_VIEW_ONLY_DUTY_ROLE', a 'Role Category' field with the value 'SCM - Duty Roles', a 'Predefined role' checkbox (unchecked), and a 'Description' field with the value 'Inventory view only duty role.'.

Figure 4 Create Duty Role

In this worked example, three privileges will be assigned to the duty role.

1. Manage On-Hand Quantity – This privilege will provide access to the Manage Item Quantities page.
2. Monitor Inventory Work Area – This privilege will provide access to the Inventory Management work area.
3. Review Completed Inventory Transaction – This privilege will provide access to the Review Completed Transactions page.

vision

Basic Information Function Security Policies Data Security Policies Role Hierarchy

Edit Role Inventory View Only Duty Role: Function Security Policies

Privilege Name	Inherited from Role
Manage On-Hand Quantity	
Monitor Inventory Work Area	
Review Completed Inventory Transaction	

Figure 5 Create Function Security Policy

The next step is to create the data security policy. Fill in the following fields below.

- Policy Name – User-defined name
- Database Resource – Inventory Organization
- Data Set – Select by key
- ORGANIZATION_ID – Enter organization id associated with the inventory organization
- Actions – Manage On-Hand Quantity

Validate View Only Access

The last step in the process is to validate the changes in the Inventory work area. Login to Inventory Management with the user assigned the view only job role. Navigate to the Inventory work area. The Manage Item Quantities page is the default page for the Inventory work area. Open the task drawer and you will see two tasks Review Completed Transactions and Review Consumption Advice Exceptions. The Review Consumption Advice Exceptions page shares the same entitlement as the Review Completed Transactions page.

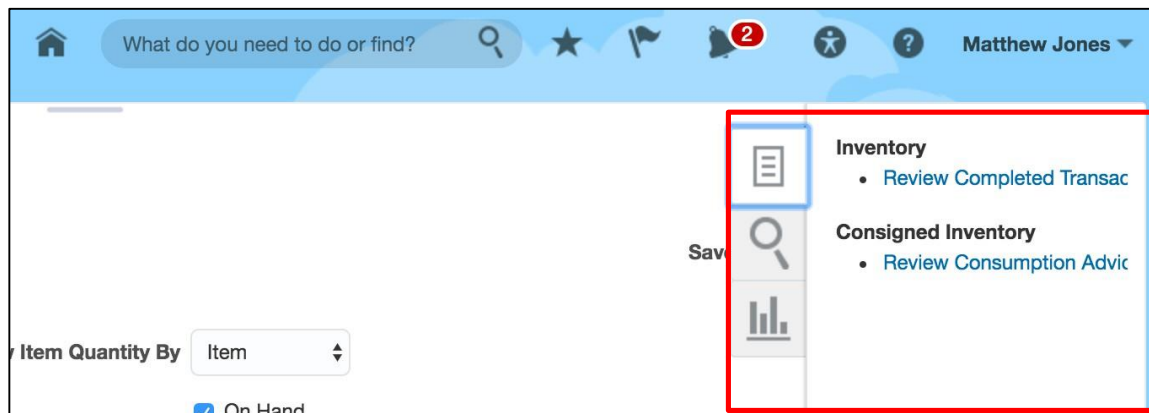


Figure 8 View Changes

PROCESS COMPLETE

EL Expression to make Read Only Field For Employee Role ?

We wanted to read only field for employee role

While employee are resigning we want that the user/ employee should be able read only Date of resignation field while Line manager and human resources specialist should be able to edit the field

We have used this el expression by it is making read only for Line Manager and Human resources specialist too
`#{{securityContext.userInRole['ORA_PER_EMPLOYEE_ABSTRACT']}}`

Solution

1. Customer would like to make resignation date field read only for employee.
2. Add below EL expression for read only attribute.
`"#{{(pageFlowScope.ResignationFlag eq 'Y' and pageFlowScope.SameUserLoggedInFlag eq 'Y')}}"`
3. Save and Apply the changes .
4. In the resignation page for employee the field became read only. Submit the transaction.
5. Logged in as the approver (HR/LM) and the field is editable for the approvers.

Need to create a custom role for an AP clerk that needs to see purchase orders when running a report but not have access to the PO UI?

Solution

The new buyer roles should only have the following function security (privileges and duty roles). Please keep the data security policies you have assigned and remove roles not in this list from the custom buyer role.

Purchase Order Inquiry Duty
Purchase Order Transaction Analysis Duty
Implemented Change Order Transaction Analysis Duty
Pending Change Order Transaction Analysis Duty
Purchase Requisitions Transaction Analysis Duty
Business Intelligence Applications Worker
Transactional Business Intelligence Worker
Item Inquiry Duty
Supplier Profile Inquiry Duty
Payables Invoice Inquiry Duty

Please include the following privileges assigned to the buyer role:

View Purchase Agreement Work Area
View Purchase Order Work Area

PRC:POZ How To Create A Supplier Read Only Role In Release 12 And Later Releases?

Steps in creating a custom role



1. From Security console -> Create role

* Role Name

* Role Code

* Role Category

☐ Predefined role

Description

2. Add the required functional security policies.

1. Supplier Profile Inquiry

2. Access Suppliers Work Area overview

Security Policies

Add Function Security Policy

* Search

All

▼

Supplier Profile Inquiry

🔍

Search Results (1)

Name	Supplier Profile Inquiry
Code	ORA_POZ_SUPPLIER_PROFILE_INQUIRY_DUTY
Description	View supplier profile information.

Security Policies

Add Function Security Policy

* Search

All

▼

Access Suppliers Work Area Overview

🔍

Search Results (1)

Name	Access Suppliers Work Area Overview
Code	POZ_ACCESS_SUPPLIER_WORKAREA_OVERVIEW_PRIV
Description	Allows access to the suppliers work area.

3. Create and add the required data security polices(Not a mandatory step)

Policy Name	Po	Data Resource	Privilege	Condition
SIQ		Supplier Personally Identifiable Information	Read;	

4.Add users

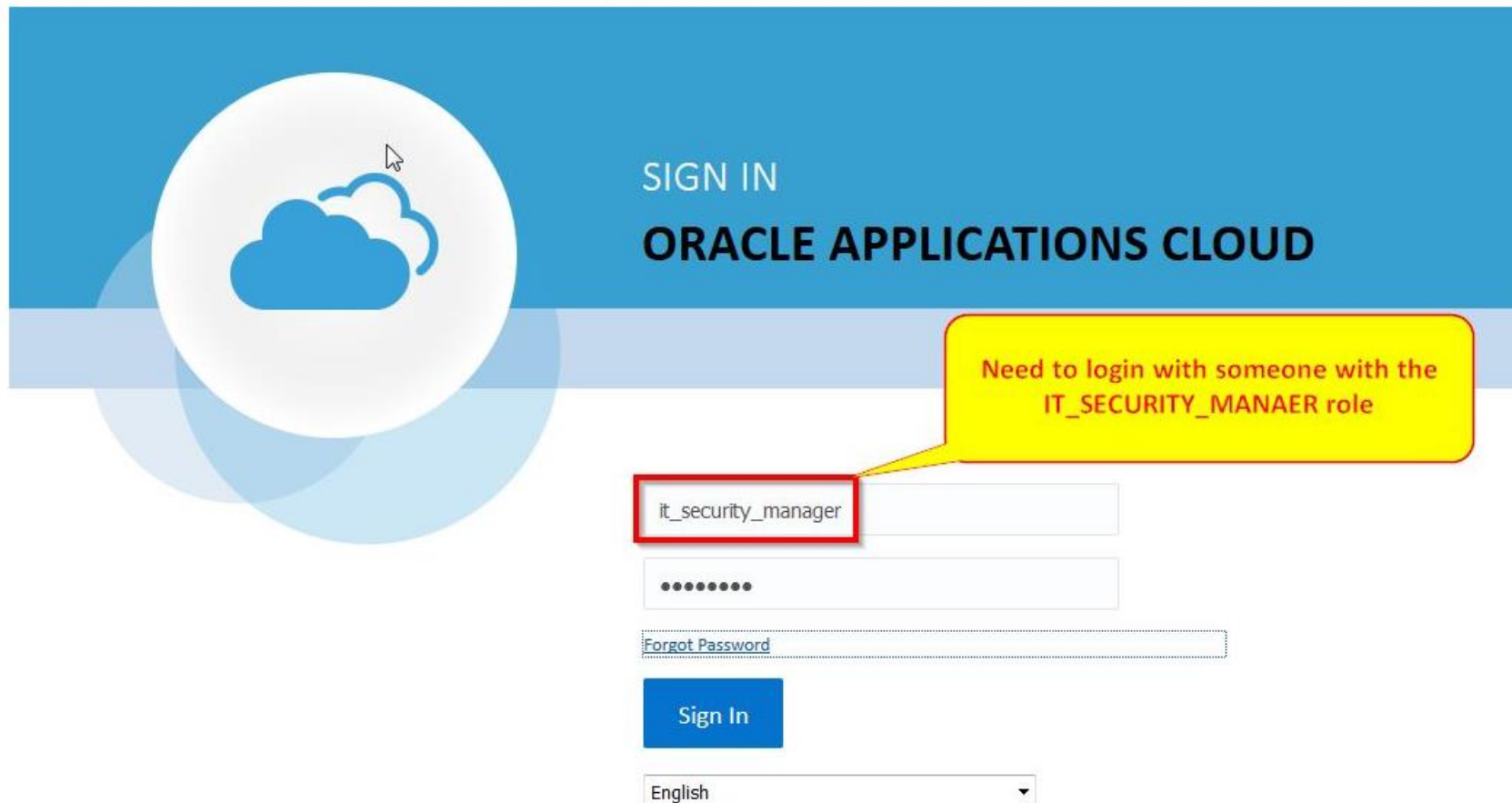
5. Review and submit

Run Retrieve Latest LDAP Changes

Login as the assigned user to see the supplier workarea

How To Create A Custom Fixed Asset Read Only Role in Release 12 and onward?

1. Login to the Application with the **IT_SECURITY_MANAGER** privilege



The image shows the Oracle Applications Cloud sign-in interface. On the left is a large circular logo with a blue cloud icon and a mouse cursor pointing at it. To the right of the logo, the text "SIGN IN" and "ORACLE APPLICATIONS CLOUD" is displayed. Below this, there is a login form. The username field contains "it_security_manager" and is highlighted with a red box. A yellow callout bubble points to this field with the text "Need to login with someone with the IT_SECURITY_MANAGER role". Below the username field is a password field with masked characters. To the right of the password field is a "Forgot Password" link. Below these fields is a blue "Sign In" button. At the bottom, there is a language dropdown menu currently set to "English".

SIGN IN
ORACLE APPLICATIONS CLOUD

Need to login with someone with the
IT_SECURITY_MANAGER role

it_security_manager

.....

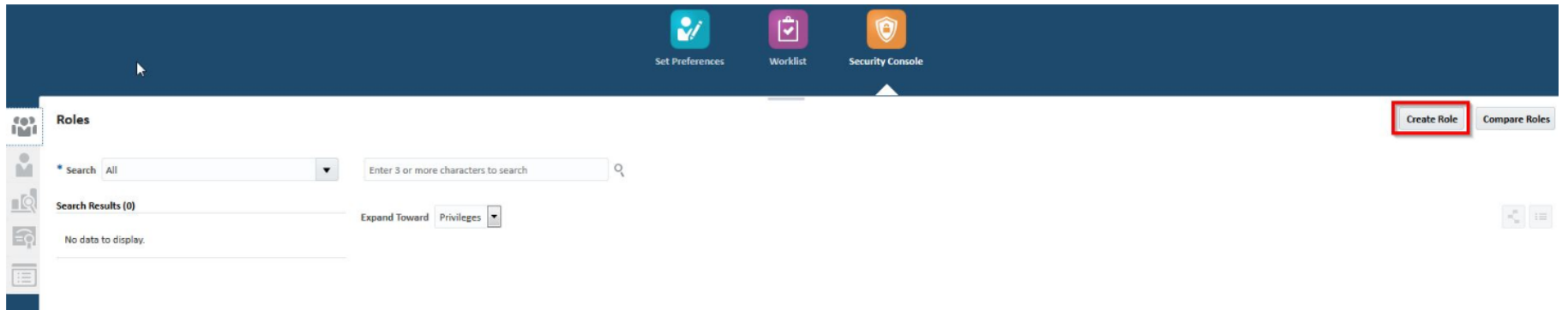
[Forgot Password](#)

Sign In

English ▼

2. Click on the **Tools - Security Console**

3. Click on **Create Role**.



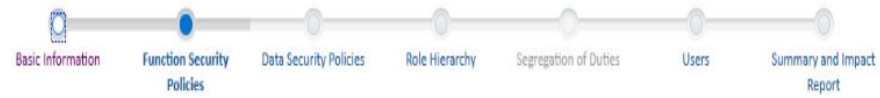
4. Name the **Role**, set the **Role Code** (with underscore values) and select the **Role Category** of Financials - Job Roles and click **NEXT**.

The screenshot shows the 'Create Role Fixed Asset Inquiry: Basic Information' form. At the top, there is a progress bar with seven steps: 'Basic Information', 'Function Security Policies', 'Data Security Policies', 'Role Hierarchy', 'Segregation of Duties', 'Users', and 'Summary and Impact Report'. The 'Basic Information' step is currently active. Below the progress bar, the form fields are as follows:

- Role Name:** Fixed Asset Inquiry
- Role Code:** FA_ASSET_INQ
- Role Category:** Financials - Job Roles
- ☐ Predefined role
- Description:** (empty field)

A yellow callout box points to the 'Role Name' field with the text: 'Name your Role, provide an Role Code (with underscores) and selct Financials - Job Roles'. The 'Next' button is visible at the bottom right.

5. Click on **Add Function Security Policy**



Create Role Fixed Asset Inquiry: Function Security Policies

Back Next Cancel

Add Function Security Policy

--	--	--	--

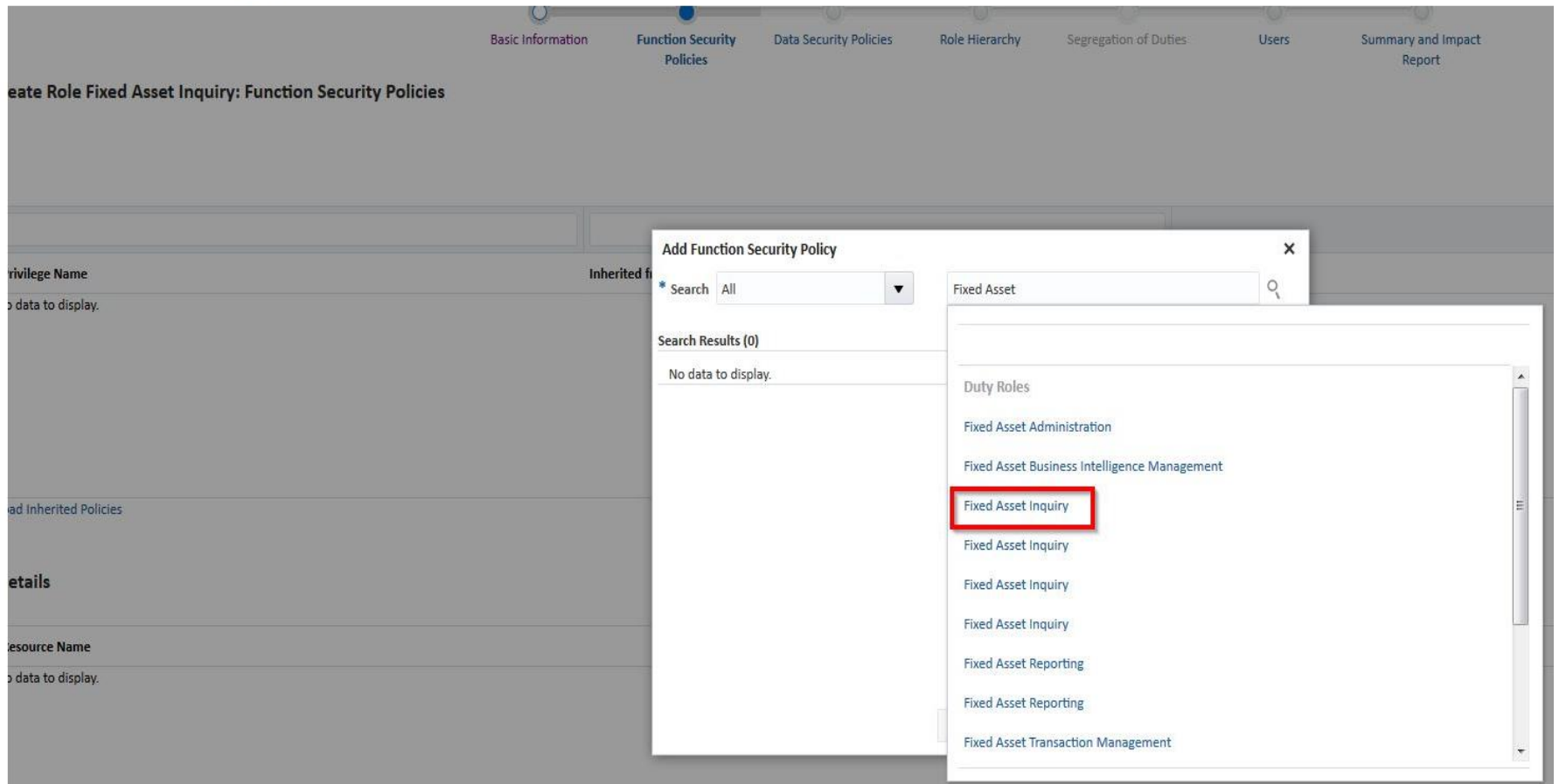
Privilege Name

Inherited from Role

Description

No data to display

6. Look for the **Fixed Asset Inquiry Duty Role**. There may be a number of them, but you need to make sure that you select the one that only shows Fixed Asset Inquiry as shown below:



Add Function Security Policy ✕

* Search 🔍

Search Results (1)

Name	Fixed Asset Inquiry
Code	ORA_FA_FIXED_ASSET_INQUIRY_DUTY
Description	Views asset information, transaction details, and accounting entries.

7. Click on **Add Selected Privileges**

8. Then search for the **Manage Fixed Asset Transactions Activities** and click **Add Privilege to Role** then Cancel.

Add Function Security Policy ✕

* Search 🔍

Search Results (1)

Name	Manage Fixed Asset Transactions Activities
Code	FA_MANAGE_FIXED_ASSET_TRANSACTIONS_ACTIVITIES_PRIV
Description	Allows access to the asset accounting manager dashboard.

9. The next screen shows you what you added.

10. In the **Data Security Policies** form, click on **Create Data Security Policy**.

Create Role Fixed Asset Inquiry: Data Security Policies

Back Next Cancel

Create Data Security Policy

Policy Name	Policy Description	Data Resource	Privilege	Condition
-------------	--------------------	---------------	-----------	-----------

No data to display.

11. Fill in the fields as shown below.

Create Data Security Policy

Policy Name: Asset Book

* Database Resource: Fixed Asset Book

* Start Date: 5/5/17

End Date:

Policy Description:

* Data Set: Select by instance set

Select data by condition

Condition Name: Access the fixed asset book for table FA_BOOK_CONTROLS for the asset books for which they are authorized

* Actions: Submit Fixed Assets Reports;1

- ☐ Add Fixed Asset
- ☐ Change Fixed Asset
- ☐ Manage Fixed Asset Book
- ☐ Retire Fixed Asset
- ☒ Submit Fixed Assets Reports
- ☒ Track Fixed Asset

OK Cancel

12. Then when you get to the form to add user, click on **Add User**.

Create Role Fixed Asset Inquiry: Users

Policies Report

Back Next Cancel

Add User

User Login	Display Name	Description
No data to display.		

13. Search for the User you would like to add this role to.

Add User

* Search All Asset Inquiry

Search Results (1)

Asset Inquiry
User Login AssetInquiry

Add Selected Users Add User to Role Cancel

14. The **Summary and Impact Report** shows you the breakdown of what was added.



Create Role Fixed Asset Inquiry: Summary and Impact Report

▲ Function Security Policies: Added (7), Removed (0)

Privilege Name

Inquire Fixed Asset
Inquire Fixed Asset Transaction
Manage Fixed Asset Tracking
Submit Fixed Asset Trace Report
View Fixed Asset Books
View Project Asset Details

▲ Data Security Policies: Added (1), Removed (0)

Policy Name

Asset Book

► Role Hierarchy: Added (0), Removed (0)

▲ Users: Added (1), Removed (0)

User Login

AssetInquiry

15. Next you need to go to **Setup and Maintenance - Manage Asset Book Data Access for Users** task.

Search

Match With Tasks, Task Lists, Business Objects

Name

Manage Asset Book Data Access for Users

16. Search for the user that you want to add access for and click on **Authorize Data Access**.

Manage Users Data Access for Users

☒ Users without Data Access ☐ Users with Data Access

Security Context

Search

Search Results

Actions ▼	View ▼				Detach	Authorize Data Access
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>		
User Name	Role	Security Context	Security Context Value			
AssetInquiry	Fixed Asset Inquiry	Asset book				
Columns Hidden	8					

17. This opens up the Spreadsheet. Here is where you enter in the Books that you want this role to have access to.

ORACLE

Authorize Data Access for Users

Add rows to authorize additional security context values for a valid combination of security context, role and user name.

Worksheet Status

Changed	Status	*Security Context	*Security Context Value[...]	User Name	Role
▲		Asset book	OPS CORP	AssetInquiry	Fixed Asset Inquiry

Enter a row for the Book
you want this user to see.

18. Then go to the **Authorize Data Access For Users** tab in Excel (Beside the ADD-INS tab) and click Upload.

19. You should see the Row updated successfully.

20. Now you need to run the following requests:

- **Retrieve Latest LDAP Changes**
- **Import User and Role Application Security Data**

Schedule New Process

Type ☒ Job ☐ Job Set

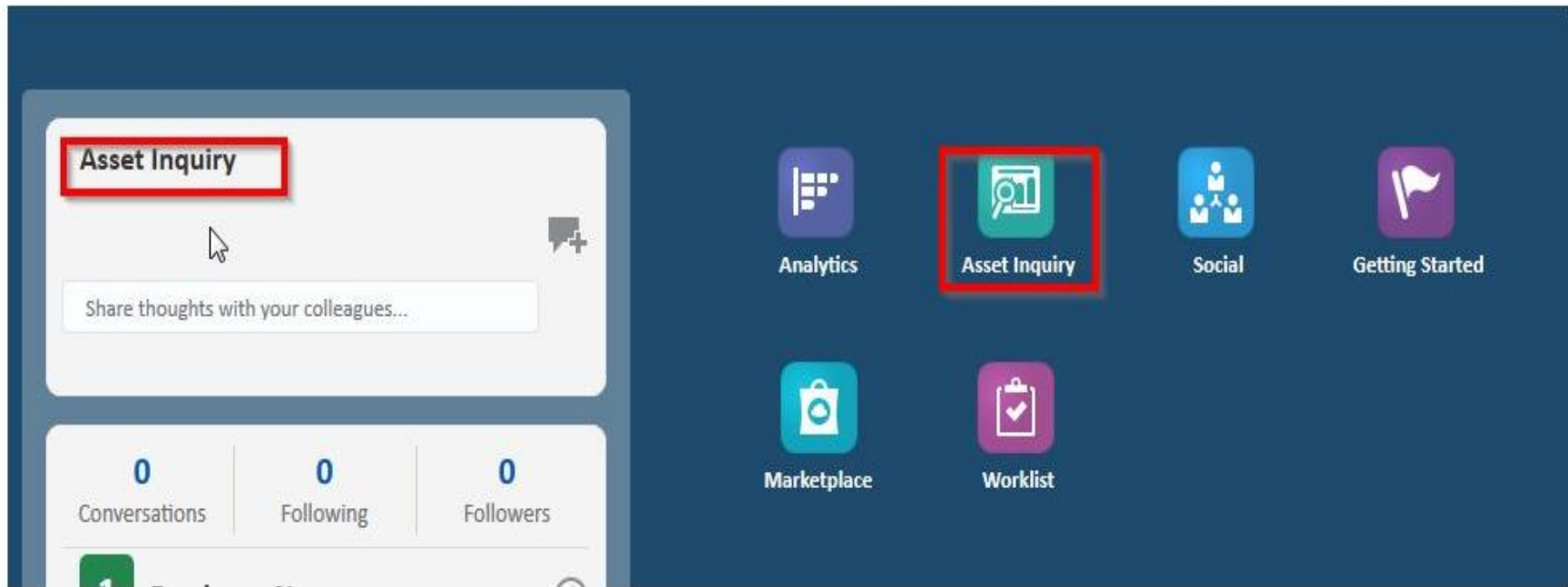
Name Import User and Role Application Security Data ▼

Description Import user and role data from LDAP and store in Applications Security tables.

OK

Cancel

21. Logout and log back in with the user and see if they have the Asset Inquiry functionality.



Revenue Management - RMCS View Only / Read Only Role - Customer Contract UI

Requirement -

Restricted user should have view only/read only option to customer contract screen.

Currently assigning privilege Manage Revenue Processing grants access to edit screen as well.

Solution

As per the current system configuration, view only / read-only role for RMCS Contracts UI is not available.

Fusion Global HR: Employee Role - Read Only Functionality For Identification Info

Remove the Add button for Employee role on Visas and Permits - Identification info but keep it visible for HR roles.

Solution

To implement the solution please follow below steps:

1. Create an sandbox and make it active.
2. Go to Edit Pages
3. Switch to Source view
4. Select the edit button and will see that the edit option is unavailable.
5. Scroll to the first line from source code: 'PanelSectionEdit'
6. Click on edit and go to the attribute: "Edit Rendered".
7. Click on down arrow and go to Expression Builder and delete the EL expression.

Please add EL Expression: `# {!securityContext.userInRole['HRRoleName']}`

Apply and close.

Retest the issue.

PRC:PO:Making Read only Role To View Only PO Without Creating Any PO

How to give role for creating PO without any edit or enable to create order ?

Solution

1. To give the access for view PO only, create a custom role with the privileges of the "View Purchase Order Work Area", "Search Purchase Order" and add it to user and assign data access.
2. Then Run User and Roles Synchronization Process .
3. Add the person in manage agents list so user will have the access to search and open the PO.

How to Create a Custom Role which is a Read Only version of the delivered Human Resource Specialist?

- Customer is trying to create a custom role which is derived from the delivered Human Resource Specialist but does not have access to modify and add updates to person records.

Solution

One needs to remove the duties that secure the actions that allow for performing updates.

It is a matter of identifying the actions that the role should not have and removing the securing duties.

And in some cases, pages are not designed with specific actions secured, so a page composer personalization may be the only other solution.

How to Create Custom Role To Have Read Only Access To One Book and Full Access to Another

Create a new Role and ONLY add the inquiry roles. If you have any transaction data policies, then the one book will be able to perform transactions as well.

In custom role setup, you need to assign Fixed Asset Inquiry seeded duty role and then this data policy.

In Role Hierarchy tab you need to select fixed assets inquiry duty role.

Search Result Count : 1

Name FA_TEST_INQUIRY
Code FA_TEST_INQUIRY
Description

Expand Toward Privileges

FA_TEST_INQUIRY

Show Roles

Role Name	Role Code	Inherited by Role Name	Inherited by Role Code
Fixed Asset Inquiry	ORA_FA_FIXED_ASSET_INQUIRY_DUTY	FA_TEST_INQUIRY	FA_TEST_INQUIRY
Payables Invoice Inquiry	ORA_AP_PAYABLES_INVOICE_INQUIRY_DUTY	Fixed Asset Inquiry	ORA_FA_FIXED_ASSET_INQUIRY_DUTY
Customer Account Inquiry	ORA_FUN_CUSTOMER_ACCOUNT_INQUIRY_DUTY	Fixed Asset Inquiry	ORA_FA_FIXED_ASSET_INQUIRY_DUTY

Data Security Policy on that custom role:

Edit Role FA_TEST_INQUIRY: Data Security Policies

Back Next Cancel

View Create Data Security Policy Detach

Policy Name	Policy Description	Data Resource	Privilege	Condition
		Fixed Asset Book	Submit Fixed Assets Reports;	Access the fixed asset book for table FA_BOOK_CONTROLS for the asset books for which they are authorized

Data Security Policy on that custom role:

Edit Role FA_TEST_INQUIRY: Data Security Policies

[Back](#)[Next](#)[Cancel](#)

View ▾

[+ Create Data Security Policy](#)[Detach](#)

Policy Name	Policy Description	Data Resource	Privilege	Condition
		Fixed Asset Book	Submit Fixed Assets Reports;	Access the fixed asset book for table FA_BOOK_CONTROLS for the asset books for which they are authorized

Edit Security Policy shows:

Edit Data Security Policy



Policy Name

* Database Resource

Fixed Asset Book



* Start Date

5/28/19



End Date

m/d/yy



Policy Description

* Data Set

Select by instance set



Select data by condition

* Condition Name

Access the fixed asset book 1



* Actions

Submit Fixed Assets Reports

[OK](#)[Cancel](#)

Then assign the following to the user.

User has two roles, seeded asset accounting manager and custom inquiry role. Give one book full access for seeded role and the other book access to custom role for inquiry only.

Roles

Role	Role Code	Assignable	Auto-Provisioned
Asset Accounting Manager	ORA_FA_ASSET_ACCOUNTING_MANAGER_JOB	Yes	No
Employee	ORA_PER_EMPLOYEE_ABSTRACT	No	No
FA_TEST_INQUIRY	FA_TEST_INQUIRY	No	No

How to remove Privilege: 'Lock Project Budget Working Version' From A Project Manager Read Only Custom Role?

Solution

Privilege name: 'Lock Project Budget Working Version' is Inherited from Role: 'Project Budget Management Custom'

You need to go directly and alter the 'Project Budget Management Custom' Duty Role. Remove whichever Privileges are not desired (ie 'Lock Project Budget Working Version') and that will be rolled up to the custom Job Role

Then recheck the issue.

Collections Inquiry Role : How to Create a Read Only Custom Role For Collections Dashboard And Collections Work Area?

Is it possible to create a custom read only role for viewing information on the collections work area ?

Solution

At this moment is not possible to create a customer read only role to view the information from Collection.

For this functionality it was opened an Enhancement request : ENH 27893935 - INQUIRY ROLE FOR FUSION ADVANCED COLLECTIONS.

Need A View Only Role For OTBI Payables Transactions Real Time

How can we create a View Only Role for OTBI Payables Transactions real time?

We are unable to view Payables Transactions in OTBI.

Requirement is to be able to provide Readonly to this, without enabling data entry via the UI.

You will need to add Data Security privilege "Report Payables" to the Duty role you are using.

Steps:-

- 1) In the Fusion UI go to Setup and Maintenance.
- 2) Search for "Manage Duties"
- 3) Filter the duty roles and edit the appropriate Duty Role.
- 4) Click on "Create Data Security Policy"
- 5) Policy Name:- "Report Payables"
Database Source :- "Business Unit"
Fill up the remaining fields appropriately.

How to Restrict Employee's Ability To Edit Invoice Distributions

Customer has an invoice approver who just has employee role, but user is able to edit the distributions on the approval notifications. Ideally, the Accounts payable specialist/supervisor should be able to edit them.

Solution

The Employee role is able to edit the distributions because of the Privilege Manage Payables Invoices. Employee Job role is inheriting this privilege through duty role Payables Invoice Inquiry Duty.

So to stop this access, we need to remove this privilege from Employee job role. Please execute the following :

- 1. Create a custom employee job role by doing a deep copy of employee job role**
- 2. Verify the name of the custom role created for Payables Invoice Inquiry Duty under the new custom job role.**
- 3. Now query this custom Payables Invoice Inquiry Duty role**
- 4. Remove the privilege Manage Payables Invoice form the custom Payables Invoice Inquiry Duty role**

5. Now the custom Employee Job Role doesn't inherit the Manage Payables Invoice privilege

6. Assign this custom Employee Job Role to user and test

Payables Invoice Inquiry (Read-Only custom role)

Create a new custom role based on seeded Payables Inquiry duty: ORA_AP_PAYABLES_INVOICE_INQUIRY_DUTY.

1. Create custom role (from Security Console)

Role Name: MF Payables Invoice Inquiry Custom Role1

Role Code: MF_AP_PAYABLES_INVOICE_INQUIRY_DUTY1

Role Category: Financials – Job Roles

The screenshot shows the 'Basic Information' tab of the Security Console. The breadcrumb trail at the top includes: Basic Information, Function Security Policies, Data Security Policies, Role Hierarchy, Segregation of Duties, Users, and Summary and Impact Report. The main heading is 'Custom Role1: Basic Information'. The form contains the following fields:

- * Role Name:** MF Payables Invoice Inquiry Custom Role1
- * Role Code:** MF_AP_PAYABLES_INVOICE_INQUIRY_DUTY1. A tooltip is visible next to this field containing the text 'MF_AP_PAYABLES_INVOICE_INQUIRY_DUTY1'.
- * Role Category:** Financials - Job Roles (selected from a dropdown menu).
- ☐ Predefined role
- Description:** (empty text area)

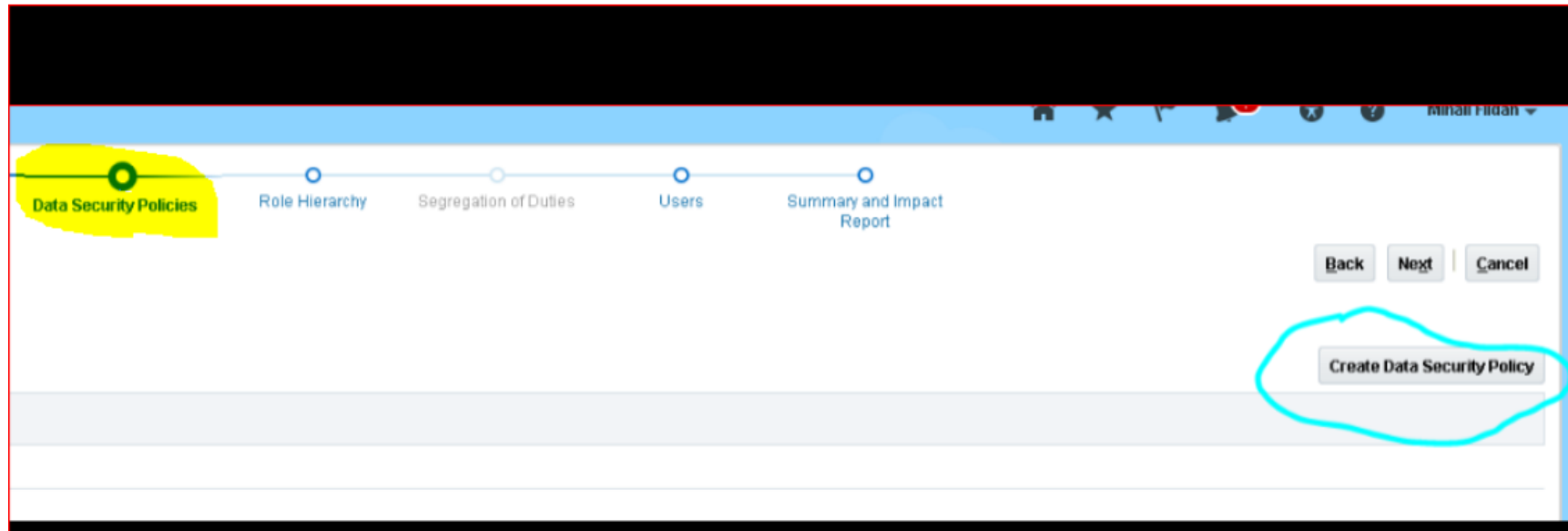
2. Add seeded duty role:

Select role in Role Hierarchy tab and add Payables Transaction Review (Add role)
ORA_AP_PAYABLES_TRANSACTION_REVIEW_DUTY



3. Add data security policy

Security console: Edit custom role



Create **Data Security Policy**

Create Data Security Policy

Policy Name

MF Grant on Business Unit

* Database Resource

Business Unit

* Start Date

1/1/01

End Date

Policy Description

* Data Set

Select by instance set

* Actions

☐ Manage Receivables Transactions

☐ View Receivables Activities

☐ Create Payables Payment Request

☐ Manage Payables Distribution Set

☐ Manage Payables Financials Option

☒ Manage Payables Invoice

☐ Manage Payables System Option

☐ Manage Payables Tax Reporting Entity

☐ Manage Payables Withholding Tax Setup

OK

Cancel

Check:

- Manage Payables Invoice
- Manage Payment by Business Unit

Basic Information
Function Security Policies
Data Security Policies
Role Hierarchy
Segregation of Duties

Edit Role MF Payables Invoice Inquiry Custom Role1: Data Security Policies

Policy Name

Policy Description

Data Resource

Privilege

Condition

MF Grant on Business Unit		Business Unit	Manage Payments By Business Unit; Manage Payables Invoice;	Access the business units for which the user is explicitly authorized
---------------------------	--	---------------	--	---

Do the same for Grant on Subledger Accounting Ledger, Grant on Subledger Accounting Ledger, Grant on Subledger Source Transaction.

Finally you will have 4 policies defined.

#	Policy Name	Database Resource	Start Date	Data Set	Condition Name	Action/Privilege
1	XX Grant on Business Unit	Business Unit	Any Date	Select by instance set	Access the business unit for which the user is explicitly authorized	Manage Payables Invoice Manage Payments by Business Unit
2	XX Grant on Subledger Accounting Ledger	Subledger Accounting ledger	Any Date	Select by instance set	Access Ledgers associated with Business Unit	Manage Ledger for Subledger Data
3	XX Grant on Subledger Application	Subledger Application	Any Date	Select by instance set	Subledger Application Instance Set Parameter1: 200	Manage Subledger Application Data
4	XX Grant on Subledger Source Transaction	Subledger Source Transaction	Any Date	Select by instance set	Access Subledger Source Transactions for a Business Unit Parameter1: 200	Manage Subledger Source Transaction Data

Policy Name	Policy Description	Data Resource	Privilege	Condition	
Business Unit		Business Unit	Business Unit; Manage Payables Invoice;	which the user is explicitly authorized	▼
MF Grant on Subledger Application		Subledger Application	Manage Subledger Application Data;	Subledger Application Instance Set	▼
MF Grant on Subledger Source Transaction		Subledger Source Transaction	Manage Subledger Source Transaction Data;	Access Subledger Source Transactions for a Business Unit	▼
MF Grant on Subledger		Subledger	Manage Ledger	Access Ledgers	▼

4. Assign the custom role to the user

- MF Payables Invoices Inquiry Custom Role1
- Employee

Current Roles		
View ▼ Format ▼ ✕		
Role Name	Start Date	Provisioning Method
Employee	2/13/18	Manual
MF Payables Invoice Inquiry Custom Role1	2/13/18	Manual

5. Add data access set for user

Manage Data Access for Users

☐ Users without Data Access ☒ Users with Data Access

Security Context

▲ Search

** User Name

Search Results

Actions ▼ View ▼ +

Detach

Authorize Additional Data Access

	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
User Name	Role	Security Context	Security Context Value	
mihai.fildan.emp2	MF Payables Invoice Inquiry Custom Role1	Business unit	MF USA BU1	

Columns Hidden 8

6. Test the custom role

ORACLE

Home

Star

Flag

Play

Help

Info

mihal.fildan.emp2

Manage Invoices

Search Results MF INV1

Invoice Details

Actions Done

Invoice Date1/10/17Invoice Amount120.00 USDBusiness UnitMF USA BU1

Invoice TypeStandardApplied Prepayments0.00 USDPayment Business UnitMF USA BU1

Supplier or PartyMF Supplier1Unpaid Amount0.00 USDPayment TermsImmediate

Supplier SiteMF ADDRESS1 USHolds0Payment CurrencyUSD

AddressAddress1,,-NotesAttachmentsNone

Lines

Holds and Approvals

Payments

Installments

Holds

View + X Print Detach

Hold					Release			Details
Name	Reason	Details	Line Held	Held By	Date	Name	Reason	Date
No holds.								

Invoice Summary

Status

Validation	Validated
Approval	Not required
Accounting	Accounted
Paid	Paid
Canceled	No

Holds

Installments	0
Line Variance	0
Distribution Variance	0
Manual Holds	0
System Holds	0
Supplier Site	No

Payments

Payments	120.00 USD
----------	------------

Invoice Totals

Items	100.00
Freight	0.00
Miscellaneous	0.00
Exclusive Tax	20.00
Inclusive Tax	0.00