

Wizarding with EBS Security Wizards and Proxy Users

User Management Training Part II

January, 2020

Susan Behn



InfosemanticsSM
People first. Driving solutions together.



Gold
Partner



Certified
Partner

About the Speaker – Susan Behn

- Oracle ACE Director 
- Over 20 years E-Business Suite development and support
- Member-Oracle Proactive Support Customer Advisory Board
- Member – EBS ATG Customer Advisory Board
- Chair-Oracle E-Business Suite User Management SIG
- Co-Chair-Texas-Louisiana Oracle User Group TLOAUG
- Board Member – Customizations and Extensions SIG
- Over 100 presentations on E-Business Suite
- Co-author for multiple books on E-Business Suite
 - The ABCs of Workflow for E-Business Suite Release 11i
 - Release 12 and The Release 12 Primer – Shining a Light on the Release 12 World

About Infosemantics



- Established in 2001
- People First
- Global Reach – Offices in US (DFW, LA, Chicago), Singapore, Philippines, and India
- Broad base of Commercial, Federal and Public Sector clients
- www.infosemantics.com



Agenda

- What is a Security Wizard
- Cash Management
- Concurrent Processing
- Flexfield Value Sets
- User Management
- Grant Security Context
- Proxy Users
- References

What is a Security Wizard

Security Wizards

- Security wizards create Grants through guided navigation path
 - Avoids need to know information not displayed on the screens such as application_id, value_set_id which requires sql access or Help→Examine
- Grant specific **action**(s) on a specific **instance**(s) of a given **object** to a specified **role**
 - Examples
 - ▶ Allow responsibility Payables Manager (**role**) to create (**action**) banks (**object**) for the Vision Operations legal entity (**instance**)
 - ▶ Allow responsibility General Ledger Super User to update all value sets for GL key flexfields
- “Role” is either a responsibility or UMX role
 - Example of UMX roles – Application End User Role, Application Super User Role, Security Administrator, Apps Schema Connect Role, Workflow Admin Role
 - ▶ To see UMX roles
Select * from wf_local_roles
where partition_id = 13;

Available Security Wizards

■ 12.1.3

■ CE UMX Security Wizard (Cash management)

- ▶ Enables access to banks by role and legal entity

■ User Management

- ▶ Enables selected abilities to manage users associated with Employee, Customer and/or Supplier

■ 12.2 – same as 12.1.3 plus

■ (added 12.2.4) Concurrent Processing

■ (added 12.2.6) Flexfield Value Sets

- ▶ Enables access to Value Sets by application, flexfield, structure, individual segment, report, or value set

■ (added 12.2.9) Flexfield Segment Security

- ▶ Allows user to specify if a specific segment is insertable or updatable

How to Access Wizards

- All wizards require the User Management Responsibility
 - User Management responsibility is inherited from assigning the role “Security Administrator” to users who need access to the wizards
 - Initially only SYSADMIN has this role
 - This is a powerful responsibility
 - Recommend limiting access to the same people who can create users
- Roles and Role Inheritance tab – query role then click the Update pencil

The screenshot shows the Oracle Roles and Role Inheritance interface. The 'Name' field in the search section is highlighted with a red box. Below the search section, there is a table with columns: Role, Code, Application, Status, View In Hierarchy, and Update. The 'Update' column contains a pencil icon, which is also highlighted with a red box.

Role	Code	Application	Status	View In Hierarchy	Update
Payables, Vision Operations (USA)	FND_RESP SQLAP PAYABLES_OPERATIONS STANDARD	Payables	✓		

How to Access Wizards

- If any grants exist for the role, they will display under Permissions
- To run a wizard, click **Save**, then click **Security Wizards**
- When you click **Save**, you will get a warning that updates require Background Engine to run

1. Click Save

2. Click Security Wizards

- If you don't click **Save** first, you will see the message below and need to click **Save and Proceed**

Warning

You must save your changes before proceeding

Cancel Save and Proceed

How to Access the Wizards

- Click the icon in the **Run Wizard** column

Roles & Role Inheritance > Update Role : Cash Management, Vision Banking >

Security Wizards

Personalize Default Double Column: (contextLayout)

Role Name Cash Management, Vision Banking **Role Code** FND_RESP|CE|CM-INSURANCE|STANDARD

Personalize "Wizard List"

Name	Description	Run Wizard
CE UMX Security wizard		
User Management : Security Administration Setup	Function for UMX security administration setup wizard	
Concurrent Processing: Security Administration Setup	Function for Concurrent Processing Security Administration Setup Wizard	
Flexfield Segments: Security Administration Setup	Function for Flexfield Segment Security Administration Setup Wizard	
Flexfield Value Sets: Security Administration Setup	Function for Flexfield Value Set Security Administration Setup Wizard	

Cash Management Security Wizard

Cash Management Security Wizard

- Cash Management Wizard enables access to banks by role and legal entity
- Roles and Role Inheritance tab – For this example, query the “Cash Management, Vision Banking” responsibility, then click the Update pencil

The screenshot shows the 'Roles and Role Inheritance' section of a web application. It includes a search area with fields for Type, Name (filled with 'Cash Management, Vision Banking'), Code, and Application, along with a 'Go' button. Below the search area is a table with columns: Role, Code, Application, Status, View In Hierarchy, and Update. The 'Update' column for the first row contains a pencil icon, which is highlighted with a red box.

Role	Code	Application	Status	View In Hierarchy	Update
Cash Management, Vision Banking	FND_RESP CE CM-INSURANCE STANDARD	Cash Management	✓		

Cash Management Security Wizard

- This role has an existing grants in my instance, so they display below
 - (See box in yellow)
- Click **Save**, then click **Security Wizards**

Roles & Role Inheritance >

Update Role : Cash Management, Vision Banking

Cancel **Security Wizards** **Save** Apply

* Indicates required field

* Category
Role Code FND_RESP|CE|CM-INSURANCE|STANDARD
Display Name Cash Management, Vision Banking
Description Cash Management

Permissions

Create Grant

Name <input type="button" value="up"/>	Set <input type="button" value="up"/>	Object <input type="button" value="up"/>	Data Context Type <input type="button" value="up"/>	Access Policy	Last Update <input type="button" value="up"/>	Duplicate	Update	Delete
FND_RESP CE CM-INSURANCE STANDARD CEBAC 498	Bank Account Maintenance	Bank Account Maintenance	Instance	498	11-Aug-2006	<input type="button" value="document"/>	<input type="button" value="pencil"/>	<input type="button" value="trash"/>

Cash Management Security Wizard

- Click **Add Legal Entities** to select a Legal Entity applicable for the responsibility selected
- Once the legal entity displays, click the checkbox for the actions allowed
 - In this example, **Maintenance** is selected
 - The Bank Account Transfers checkbox is only available if Treasury is installed
- Click **Apply** to return to the previous screen

Roles & Role Inheritance > Update Role : Cash Management, Vision Banking > Security Wizards >

Bank Account Security Management

Role: Cash Management, Vision Banking

[Cancel](#) [Apply](#)

[Show](#)

[Add Legal Entities](#)    

Legal Entity	Bank Account Grants	
	Use	Bank Account Transfers
Vision ADB	<input type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	

Quick Tip

Adding a legal entity in this page will give the selected role access to all the bank accounts within this legal entity. After adding a legal entity, choose grants that you want to assign to this role on the bank accounts of this legal entity.

Cash Management Security Wizard

■ New grant now appears

Users **Roles & Role Inheritance** Role Categories Registration Processes Security Report Proxy Configuration Responsibility

Update Role : Cash Management, Vision Banking

[Cancel!](#) [Security Wizards](#) [Save](#) [Apply](#)

* Indicates required field

Personalize Table Layout: (ContentLayout)

* **Category** Miscellaneous

Role Code FND_RESP|CE|CM-INSURANCE|STANDARD

Display Name Cash Management, Vision Banking

Description Cash Management, Vision Banking

Application Cash Management

Active From 31-Jul-2002

Active To

Personalize Stack Layout: (GrantsSubTabRN)
Personalize "Permissions"

Permissions

[Create Grant](#) | ...

Name ▲	Set ▲	Object ▲	Data Context Type ▲	Access Policy	Last Update ▲	Duplicate	Update	Delete
FND_RESP CE CM-INSURANCE STANDARDCEBAA498	Bank Account Access	Bank Account Access	Instance	498	11-Jan-2021			
FND_RESP CE CM-INSURANCE STANDARD CEBAC 498	Bank Account Maintenance	Bank Account Maintenance	Instance	498	11-Aug-2006			

CE UMX Security Wizard

- This is an example of the grant displayed when you click a link for the name
- Click **Update** here if needed rather than going back to the list to click the update pencil
- Note: update does not allow changes to the Object or the Data Context

The screenshot shows the Oracle Security Wizard interface. The top navigation bar includes 'Users', 'Roles & Role Inheritance', 'Role Categories', 'Registration Processes', 'Security Report', 'Proxy Configuration', and 'Responsibility'. The 'Roles & Role Inheritance' tab is active, and the breadcrumb path is 'Roles & Role Inheritance >'. The main content area displays the 'View Grant' details for 'FND_RESP|CE|CM-INSURANCE|STANDARD|CEBAC|498'. The 'Update' button is highlighted with a red box. The details are organized into sections: 'Name', 'Description', 'Effective From', 'Effective To', 'Security Context', 'Data Security', 'Data Context', and 'Set'.

View Grant: FND_RESP CE CM-INSURANCE STANDARD CEBAC 498	
Name	FND_RESP CE CM-INSURANCE STANDARD CEBAC 498
Description	
Effective From	11-Aug-2006
Effective To	
Security Context	
Grantee Type	Group Of Users
Grantee	Cash Management, Vision Banking
Operating Unit	
Responsibility	
Data Security	
Object	Bank Account Maintenance
Data Context	
Type	Instance
Name	
Description	
Instance Details	
LEGAL_ENTITY_ID	498
Set	
Name	Bank Account Maintenance
Code	CE_BA_MAINTENANCE
Description	

Flexfield Value Set Security Required in 12.2

Flexfields | Validation | Values

- In 12.2, seeded Security is set to “No Access” to any values in this form

Find Value Set

Find Values By

- Value Set
- Key Flexfield
- Descriptive Flexfield
- Concurrent Program

Name

Forms

FRM-41830: List of Values contains no entries.

OK

Description

Clear Find

Find Key Flexfield Segment

Find Values By

- Value Set
- Key Flexfield
- Descriptive Flexfield
- Concurrent Program

Application

Title

Forms

FRM-41830: List of Values contains no entries.

OK

Description

Clear Find

Find Descriptive Flexfield Segment

Find Values By

- Value Set
- Key Flexfield
- Descriptive Flexfield
- Concurrent Program

Application

Title

Context

Forms

FRM-41830: List of Values contains no entries.

OK

Clear Find

Find Concurrent Program Parameter

Find Values By

- Value Set
- Key Flexfield
- Descriptive Flexfield
- Concurrent Program

Application

Name

Parameter

Forms

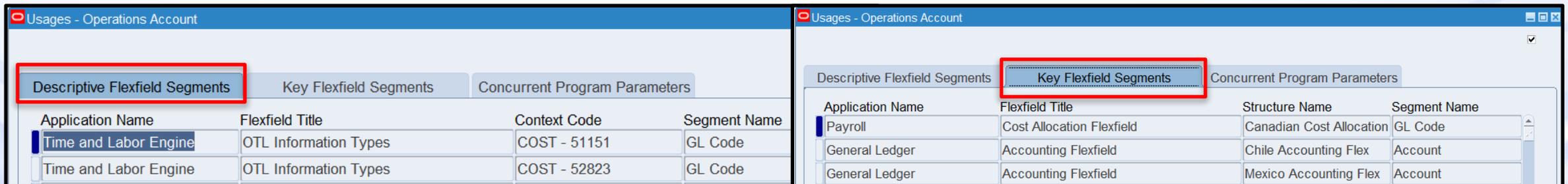
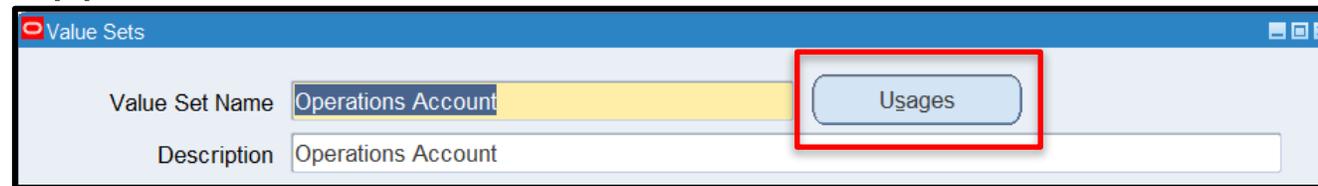
FRM-41830: List of Values contains no entries.

OK

Find

Flexfield Value Sets

- Value Sets are used in Key Flexfields, DFFs, Concurrent Program Parameter LOVs, etc.
 - Discussion limited to Value Set Types: Independent, Dependent, Translatable Independent, Translatable Dependent
- Value Sets do not belong to an Application
 - Where they are used belongs to the application
 - Example - the account segment in the Accounting Key Flexfield is used by OTL, Payroll and General Ledger
- Value Sets can be used by multiple structures
 - Click **Usages** in Application → Validation → Set; there is no “Where Used” Report



Flexfield Value Sets – Useful Queries

■ DFF Value Sets

```
SELECT ffdsvv.application_name,
       ffdsvv.title,
       ffdsvv.context_name,
       ffdsvv.parent_segment_name,
       ffvs.flex_value_set_name
FROM   fnd_flex_descr_seg_vset_v ffdsvv, fnd_flex_value_sets ffvs
WHERE  ffdsvv.flex_value_set_id = ffvs.flex_value_set_id
AND    ffdsvv.validation_type IN ('I','D','Y','X')
ORDER BY ffdsvv.application_name,
         ffdsvv.title,
         context_code,
         ffdsvv.parent_segment_name;
```

■ KFF Value Sets

```
SELECT ffksvv.application_name,
       ffksvv.id_flex_name,
       ffksvv.id_flex_structure_name,
       ffksvv.segment_name,
       DECODE (ffksvv.validation_type,
              'I', 'Independent',
              'D', 'Dependent',
              'Y', 'Translatable Independent',
              'X', 'Translatable Dependent',
              ffksvv.validation_type)
       validation_type,
       ffvs.flex_value_set_name
FROM   fnd_flex_kff_seg_vset_v ffksvv, fnd_flex_value_sets ffvs
WHERE  ffvs.flex_value_set_id = ffksvv.flex_value_set_id
AND    ffksvv.validation_type IN ('I','D','Y','X')
ORDER BY ffksvv.application_name,
         ffksvv.id_flex_name,
         ffksvv.id_flex_structure_name,
         ffksvv.segment_name;
```

Flexfield Value Sets: Setup 12.0 – 12.5

Prior to Security Wizard released in 12.2.6

Grant access to the data

- Functional Administrator → Grants
- This example – General Ledger, Vision Operations (USA) responsibility needs to see GL value sets for Vision Operations Accounting Flexfield

Create Grant: Review and Finish	
Name	GL Grant for Value Sets for General Ledger, Vision Operations (USA)
Description	GL Grant for Value Sets
Effective From	11-Jul-2014
Effective To	
Security Context	
Grantee Type	Group Of Users
Grantee	General Ledger, Vision Operations (USA)
Operating Unit	
Responsibility	General Ledger, Vision Operations (USA)

Data Security - Instance Set

■ Object = Flexfield Value Set Security Object

- Must know name of object

■ Choose the context (how to authorize access)

- Must be familiar with available instance sets

■ Instance Set Details

- Requires SQL to find values for parameters to provide access to a specific Key Flexfield Structure by app id, key flexfield id and structure id

- ▶ In this case, a specific accounting key flexfield

Data Security

Object Flexfield Value Set Security Object

Data Context

Type	Instance Set
Name	Key flexfield structure
Description	Give access to value sets by application id, key flexfield code and structure number

Predicate

```
flex_value_set_id in (select
flex_value_set_id from
fnd_id_flex_segments where
application_id=&
GRANT_ALIAS.PARAMETER1 and
id_flex_code=&
GRANT_ALIAS.PARAMETER2 and
id_flex_num=&
GRANT_ALIAS.PARAMETER3)
```

Instance Set Details

Parameter 1	101
Parameter 2	GL#
Parameter 3	101

Permission set for allowable actions

- Scroll down on the grants form to assign the permission set
- For this example, allow insert or update for the accounting key Flexfield
 - Must be familiar with permission set names

Set	
Name	Flexfield Value Set Security Insert/Update Set
Code	FND_FLEX_VSET_INSERT_UPDATE_PS
Description	Allow insert and update of values in a value set

- Other seeded permission sets for flexfield security

Select	Quick Select	Name ▲▼	Code ▲▼	Type ▲▼	Description ▲▼
<input type="radio"/>		Flexfield Value Set Security Insert Set	FND_FLEX_VSET_INSERT_PS	Permission Set	Allow insert of values into a value set
<input type="radio"/>		Flexfield Value Set Security Insert/Update Set	FND_FLEX_VSET_INSERT_UPDATE_PS	Permission Set	Allow insert and update of values in a value set
<input type="radio"/>		Flexfield Value Set Security Update Set	FND_FLEX_VSET_UPDATE_PS	Permission Set	Allow update of values in a value set
<input type="radio"/>		Flexfield Value Set Security View Only Set	FND_FLEX_VSET_VIEW_ONLY_PS	Permission Set	Allow viewing (only) of values in a value set

Flexfield Value Sets: Using Security Wizard 12.2.6+

Flexfield Value Sets: Security Administration Setup

■ Example

- Query General Ledger Super User
- Click **Save**, then **Security Wizards**

Clicking **Create Grant** before accessing the security wizard will take you to the old setup which is the same form as in the Functional Administrator Responsibility

Roles & Role Inheritance >

Update Role : General Ledger Super User

Cancel **Security Wizards** Save Apply

* Indicates required field

* Category Miscellaneous Application General Ledger
Role Code FND_RESP|SQLGL|...|GENERAL_LEDGER_SUPER_USER|STANDARD Active From 01-Jan-1951
Display Name General Ledger Super User Active To
Description Super User responsibility for Oracle General Ledger

Permissions

Create Grant | ...

Name	Set	Object	Data Context Type	Access Policy	Last Update	Duplicate	Update	Delete
------	-----	--------	-------------------	---------------	-------------	-----------	--------	--------

Flexfield Value Sets: Security Administration Setup

■ Example

- Click the icon for **Flexfield Value Sets: Security Administration Setup**

Roles & Role Inheritance > Update Role : General Ledger Super User >

Security Wizards

Personalize Default Double Column: (contextLayout)

Role Name General Ledger Super User **Role Code** FND_RESP|SQLGL|GENERAL_LEDGER_SUPER_USER|STANDARD

Personalize "Wizard List"

Name	Description	Run Wizard
CE UMX Security wizard		
User Management : Security Administration Setup	Function for UMX security administration setup wizard	
Concurrent Processing: Security Administration Setup	Function for Concurrent Processing Security Administration Setup Wizard	
Flexfield Value Sets: Security Administration Setup	Function for Flexfield Value Set Security Administration Setup Wizard	
Flexfield Segments: Security Administration Setup	Function for Flexfield Segment Security Administration Setup Wizard	

Flexfield Value Sets: Security Administration Setup

■ Now click **Create Grant**

The screenshot shows the Oracle Flexfield Value Set Security Wizard interface. The breadcrumb navigation is: Roles & Role Inheritance > Update Role : General Ledger Super User > Security Wizards >. The title is "Flexfield Value Set Security Wizard" with "Cancel" and "Apply" buttons. Under "Role Details", the Role Name is "General Ledger Super User" and the Role Code is "FND_RESP|SQLGL|GENERAL_LEDGER_SUPER_USER|STANDARD". Under "Grants", there is a toolbar with a "Create Grant" button (highlighted with a red box) and several icons. Below the toolbar is a table with the following structure:

Name	Authorize Value Sets by	Value Set Privileges	Effective From	Update	Remove
No results found.					

Flexfield Value Sets: Security Administration Setup

- Screen displayed is pared down version of full Create Grant screen

- Name Required

- Choose Value Set Privileges (permission set)



- (selected) authorize (instance set)

- Select Parameters (instance set details)

- Parameters display based on authorization selection

- Click **Apply**

Users | Roles & Role Inheritance | Role Categories | Registration Processes | Security Report | Proxy Configuration | Responsibility

Roles & Role Inheritance > Update Role : General Ledger Super User > Security Wizards > Flexfield Value Set Security Wizard >

Value Set Security Wizard

Cancel **Apply**

Define Grant

Grant Details	Security Context
<p>* Grant Name: IS Operations GL Flexfield Access for GL Super User</p> <p>Description: [Text Area]</p> <p>* Effective From: 11-Jan-2021</p> <p>Effective To: [Date Picker]</p>	<p>Operating Unit: [Dropdown]</p> <p>Responsibility: [Dropdown]</p>

Grant Information

Value Set Grant Type	Select Parameters
<p>* Value Set Privileges: Insert/Update</p> <p>* Authorize Value Sets by: Key Flexfield Structure</p> <ul style="list-style-type: none">Value Set NameKey Flexfield ApplicationKey Flexfield NameKey Flexfield StructureKey Flexfield SegmentDescriptive Flexfield ApplicationDescriptive Flexfield NameDescriptive Flexfield ContextDescriptive Flexfield SegmentConcurrent Program ApplicationConcurrent Program NameConcurrent Program ParameterAll Value Sets	<p>Table Diagnostics</p> <p>* Application Name: General Ledger</p> <p>* Key Flexfield Name: Accounting Flexfield</p> <p>* Structure Name: Operations Accounting Flex</p> <p>Diagnostic Console</p>

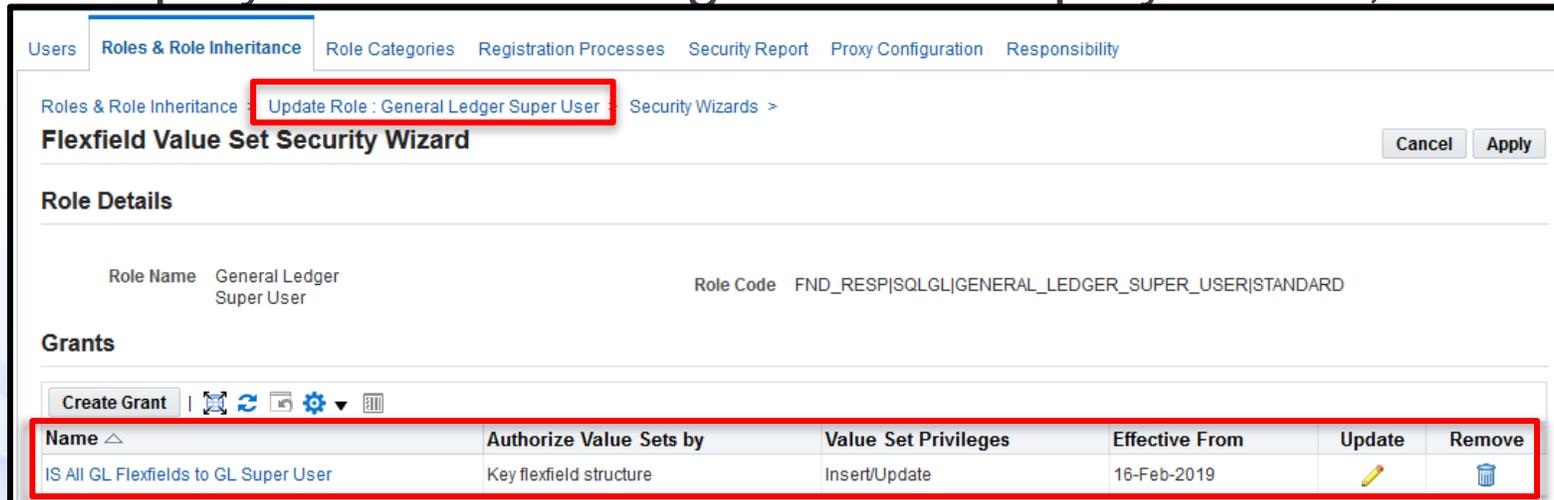
Flexfield Value Sets: Security Administration Setup

■ Click **OK** on the Confirmation Screen



■ New grant is displayed

- Since you are still in the Security Wizard, only grants for Value Sets are displayed – to see all grants for displayed role, click Update Role: <role name>



Flexfield Value Sets: Security Administration Setup

- Clicking Grant name shows definition of grant

Users Roles & Role Inheritance Role Categories Registration Processes Security Report Proxy Configuration Responsibility

Roles & Role Inheritance > Update Role : General Ledger Super User >

View Grant: IS All GL Flexfields to GL Super User Delete Update

Name IS All GL Flexfields to GL Super User

Description

Effective From 16-Feb-2019

Effective To

Security Context

Grantee Type Group Of Users

Grantee General Ledger Super User

Operating Unit

Responsibility

Data Security

Object Flexfield Value Set Security Object(1)

Data Context

Type Instance Set

Name Key flexfield structure

Description Give access to value sets by application id, key flexfield code and structure number

Predicate

```
flex_value_set_id in (select
flex_value_set_id from
fnd_id_flex_segments where
application_id=&
GRANT_ALIAS.PARAMETER1
and id_flex_code=&
GRANT_ALIAS.PARAMETER2
and id_flex_num=&
GRANT_ALIAS.PARAMETER3)
```

Instance Set Details

Parameter 1 101

Parameter 2 GL#

Parameter 3 101

Parameter 4

Parameter 5

Parameter 6

Parameter 7

Parameter 8

Parameter 9

Parameter 10

Set

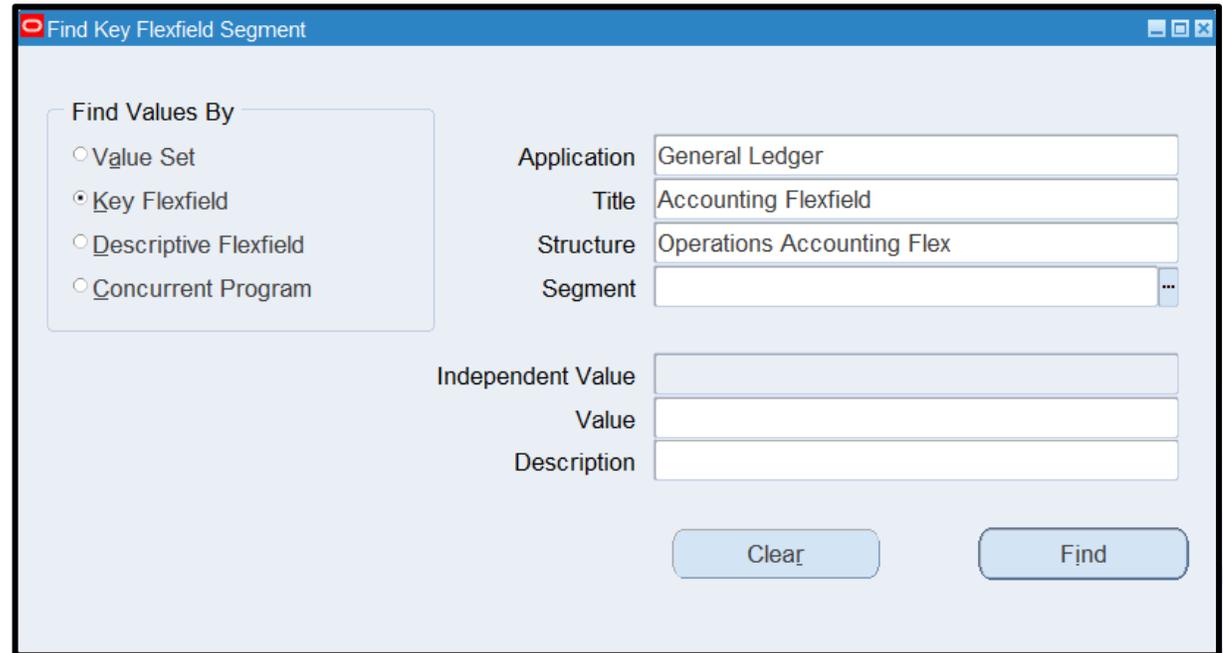
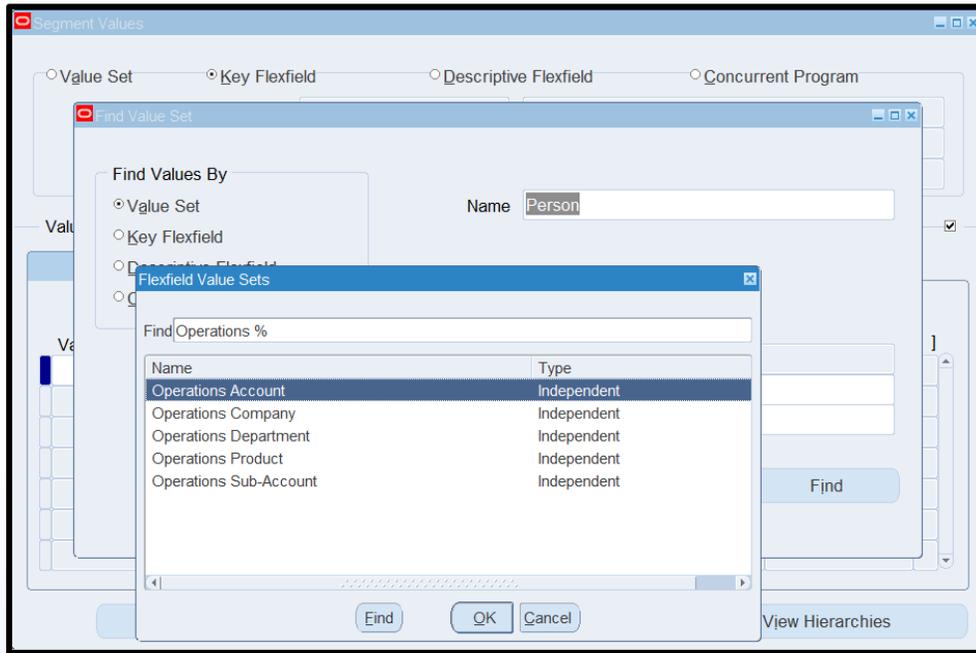
Name Flexfield Value Set Security Insert/Update Set

Code FND_FLEX_VSET_INSERT_UPDATE_PS

Description Allow insert and update of values in a value set

Flexfield Value Sets: Security Administration Setup – Results

- LOV by Value Set limited to KFF Value Sets, to just the Operations Accounting Flexfield



Flexfield Value Sets: Security Administration Setup

- Purchasing example 1
- Grant access to all value sets for Purchasing **key** flexfields to Purchasing **Application**

Users **Roles & Role Inheritance** Role Categories Registration Processes Security Report Proxy Configuration Responsibility

Roles & Role Inheritance > Security Wizards > Flexfield Value Set Security Wizard >

Value Set Security Wizard

Cancel Apply

Define Grant

Grant Details	Security Context
<p>* Grant Name Purchasing super user access to all key value sets</p> <p>Description Purchasing super user access to all key value sets</p> <p>* Effective From 26-Jul-2019</p> <p>Effective To</p>	<p>Operating Unit</p> <p>Responsibility</p>

Grant Information

Value Set Grant Type	Select Parameters
<p>* Value Set Privileges Insert/Update</p> <p>* Authorize Value Sets by Key Flexfield Application</p>	<p>Inspect MDS Contents</p> <p>* Application Name Purchasing</p>

Flexfield Value Sets: Security Administration Setup

- Purchasing example 2
- Grant access to all value sets for Purchasing **descriptive** flexfields to Purchasing **Application**
- Responsibility/Role not applicable

Users Roles & Role Inheritance Role Categories Registration Processes Security Report Proxy Configuration Responsibility

Roles & Role Inheritance > Security Wizards > Flexfield Value Set Security Wizard >

Value Set Security Wizard

Cancel Apply

Define Grant

Grant Details	Security Context
<p>* Grant Name Purchasing super user access to all DFF value sets</p> <p>Description Purchasing super user access to all DFF value sets</p> <p>* Effective From 26-Jul-2019</p> <p>Effective To</p>	<p>Operating Unit</p> <p>Responsibility</p>

Grant Information

Value Set Grant Type	Select Parameters
<p>* Value Set Privileges Insert/Update</p> <p>* Authorize Value Sets by Descriptive Flexfield Application</p>	<p>Inspect MDS Contents</p> <p>* Application Name Purchasing</p>

Flexfield Value Sets: Security Administration Setup

■ Recommendations

- Grant KFF and DFF access at application level to Super User responsibility
 - ▶ Shared applications go to most appropriate super user (HR, Inv)
 - ▶ If further delineation is needed, assign by KFF structure or specific value set
- Grant Value Set access for Concurrent Programs to the role that registers new Concurrent Programs (typically Application Developer or System Administrator)
- Grant Value Sets access other purposes should be assigned to the Super User role associated with the use of the value set or just to the System Administrator
- System Administrator responsibility should be assigned the role “Flexfield Value Set Security: All Privileges” as backup to all Super Users
 - ▶ This role is seeded – use Role Hierarchy to assign role

Security Report Showing Existing Grants

Users Roles & Role Inheritance Role Categories Registration Processes Responsibility Proxy Configuration **Security Report**

Search Report | Report Status

Security Reports

Report Type List of Roles/Responsibilities

For a Given Data Security Object Flexfield Value Set Security

View As HTML On Screen

Notify Report Status

Schedule Recurring Reports

► Show Advanced Search

Go Clear

Security Reports

Use Schedule Recurring Report to schedule periodic offline generation of reports

Use Advanced Search to refine your search further.

Generate Reports in MS Excel or Adobe PDF format

List of Roles/Responsibilities for Object Flexfield Value Set Security Object(1)

Details	Role Name ▲	Accessible ▲	Grant Name ▲	Grant Created By ▲	Grant Creation Date ▲	Grant Updated By ▲	Grant Updated Date ▲
►	FND_RESP FND APPLICATION_DEVELOPER STANDARD	✓	All to Application Developer	SYSADMIN	26-Mar-2019	SYSADMIN	26-Mar-2019
►	UMX FND_FLEX_VSET_ALL_PRIVS_ROLE	✓	Flexfield Value Set Security: All privileges grant	ORACLE12.2.0	09-May-2013	ORACLE12.2.0	09-May-2013
►	UMX KB_ALL_VALUE_SET_ACCESS	✓	KB Operations Accounting Flexfield	OPERATIONS	28-Jul-2015	OPERATIONS	28-Jul-2015
►	FND_RESP SQLGL GENERAL_LEDGER_SUPER_USER STANDARD	✓	IS All GL Flexfields to GL Super User	SYSADMIN	16-Feb-2019	SYSADMIN	16-Feb-2019

Concurrent Processing: Security Administration Setup

Concurrent Processing: Security Administration Setup

- Wizard controls Programs that can be submitted or Viewed
 - This adds access outside of what is assigned by request group
 - Be sure to perform this setup for both Programs and Request Sets if selecting Application or Request Group

Roles & Role Inheritance > Update Role : General Ledger Super User > Security Wizards >

Concurrent Processing Security Wizard

Save Apply Cancel

Role Details

Role Name: General Ledger Super User
Role Code: FND_RESP|SQLGL|GENERAL_LEDGER_SUPER_USER|STANDARD

Submit Request View Request

Select the set of request types that users (assigned the role above) should be able to submit.

All Programs in Request Group * Add

- All Programs in Application
- All Programs in Request Group**
- All Request Sets in Application
- All Request Sets in Request Group**
- Specific Program
- Specific Request Set

Quick Tip:

 **TIP** Add: Gives permission to submit concurrent requests for the request type specified to the above role.

	Value	Application	Remove

Concurrent Processing: Security Administration Setup

■ Example

- Query General Ledger Super User
- Click **Save**, then **Security Wizards**
- Click the icon for **Concurrent Processing: Security Administration Setup**

Roles & Role Inheritance > Update Role : General Ledger Super User >

Security Wizards

Personalize Default Double Column: (contextLayout)

Role Name General Ledger Super User Role Code FND_RESP|SQLGL|GENERAL_LEDGER_SUPER_USER|STANDARD

Personalize "Wizard List"

Name	Description	Run Wizard
CE UMX Security wizard		
User Management : Security Administration Setup	Function for UMX security administration setup wizard	
Concurrent Processing: Security Administration Setup	Function for Concurrent Processing Security Administration Setup Wizard	
Flexfield Value Sets: Security Administration Setup	Function for Flexfield Value Set Security Administration Setup Wizard	
Flexfield Segments: Security Administration Setup	Function for Flexfield Segment Security Administration Setup Wizard	

Concurrent Processing: Security Administration Setup

- Submit Request Tab
- Select “All Request Sets in Application” for “General Ledger” Application
- Click **Add**
- Click **Save** (stays on page) or **Apply** (saves and returns to previous page)
- Allows General Ledger Super User to run all requests in the General Ledger application even if they are not in the request group

Concurrent Processing Security Wizard [Save] [Apply] [Cancel]

Role Details

Role Name: General Ledger Super User Role Code: FND_RESP|SQLGL|GENERAL_LEDGER_SUPER_USER|STANDARD

[Submit Request] [View Request]

Select the set of request types that users (assigned the role above) should be able to submit.

[All Request Sets in Application] [General Ledger] [Add]

Quick Tip:
Add: Gives permission to submit concurrent requests for the request type specified to the above role.

Type	Value	Application	Remove
All Request Sets in Application	SQLGL	SQLGL	[Remove]

Concurrent Processing: Security Administration Setup

- View Request Tab – this is a replacement for the Profile Option Option “Concurrent Report Access Level” which became obsolete in 12.1
- Select the level – Application, Current Responsibility, Responsibility or User
- Click **Add**
- Click **Save** (stays on page) or **Apply** (saves and returns to previous page)
- The example below allows users assigned the General Ledger Super User responsibility to see all GL report output regardless of which responsibility or user ran the report

Users Roles & Role Inheritance Role Categories Registration Processes Security Report Proxy Configuration Responsibility

Concurrent Processing Security Wizard

Save Apply Cancel

Role Details

Role Name: General Ledger Super User Role Code: FND_RESP|SQLGL|GENERAL_LEDGER_SUPER_USER|STANDARD

Submit Request View Request

Select the set of request types that users (assigned the role above) should be able to view.

Application General Ledger Add

Value	Remove
General Ledger	Remove

Quick Tip:
Add: Gives permission to view concurrent requests for the request type specified to the above role.

Concurrent Processing: Security Administration Setup

- Unlike the CE Wizard, resulting grants are not named
 - To see the grant, click **Update**

Users | **Roles & Role Inheritance** | Role Categories | Registration Processes | Security Report | Proxy Configuration | Responsibility

Roles & Role Inheritance >
Update Role : General Ledger Super User Cancel Security Wizards Save Apply

* Indicates required field

* Category Application General Ledger
Role Code FND_RESP|SQLGL|GENERAL_LEDGER_SUPER_USER|STANDARD Active From 01-Jan-1951
Display Name General Ledger Super User Active To
Description Super User responsibility for Oracle General Ledger

Permissions

Create Grant |

Name ^	Set ^	Object ^	Data Context Type ^	Access Policy	Last Update ^	Duplicate	Update	Delete
	Request Operations	Concurrent Requests	Instance Set	Requests that can be viewed by user based on the application	13-Feb-2019			

Concurrent Processing: Security Administration Setup

- If any updates are made on this page, adding a name will be required
 - Recommend just deleting and recreating the grant unless restricting by Operating Unit

Users Roles & Role Inheritance Role Categories Registration Processes Security Report Proxy Configuration Responsibility

Roles & Role Inheritance > Update Role : General Ledger Super User >

Update Grant

Cancel Apply

* Indicates required field

* Name

Description

* Effective From 13-Feb-2019 Effective To

Security Context

Define the context when the grant is applied by selecting a grantee, a responsibility and/or operating unit.

Grantee Type Group Of Users
Grantee General Ledger Super User

Operating Unit

Responsibility

Data Security

Object Concurrent Requests

Data Context

Type Instance Set
Name Requests that can be viewed by user based on the application
Description Requests that can be viewed by user based on the application

Predicate

```
( &TABLE_ALIAS.request_id IN  
( SELECT cr.request_id FROM  
  fnd_concurrent_requests cr  
  ,fnd_application app WHERE  
  cr.program_application_id =  
  app.application_id AND  
  app.application_short_name =  
  &GRANT_ALIAS.PARAMETER1  
  ) )
```

Instance Set Details

Parameter 1 SQLGL
Parameter 2
Parameter 3
Parameter 4
Parameter 5
Parameter 6
Parameter 7
Parameter 8
Parameter 9
Parameter 10

Set

Select the permission set or menu navigation set that defines the grantee's access.

* Set Request Operations

Concurrent Processing: Security Administration Setup

- View Results – requests can be viewed only by searching for Specific Requests
- Can see both Report and Log
- Use Cases
 - Support team - especially when in different locations
 - Potential performance improvement - minimize multiple people running the same report
- Caution – overrides other security limitations especially when granting access at the application level

The screenshot displays the 'Requests' application interface. At the top, there are buttons for 'Refresh Data', 'Find Requests', 'Submit a New Request', 'Submit New Request Set', 'Copy Single Request', and 'Copy Request Set'. Below these buttons is a checkbox for 'Auto Refresh (X)'. The main area features a table with columns: Request ID, Name, Parent, Phase, Status, and Parameters. A single row is visible with the following data: Request ID: 8609775, Name: Trial Balance, Parent: (empty), Phase: Completed, Status: Normal, Parameters: 1017, Vision Operations, 1, 10. A 'Find Requests' dialog box is open in the foreground, showing search criteria: Request ID, Name, Date Submitted, Date Completed, Status, Phase, and Requestor (OPERATIONS). The dialog also includes radio buttons for 'My Completed Requests', 'My Requests In Progress', 'All My Requests', and 'Specific Requests' (which is selected).

Concurrent Processing: Security Administration Setup

■ Additional Tips

- If the grant is by Application, be sure that all needed applications are included
 - ▶ Example: General Ledger also requires Application Report Generator for FSGs and if running Public Sector, requires Public Sector Financials
 - ▶ View The Report Groups attached to the responsibilities and ensure all applications are included
- If the grant is by Responsibility, be sure that all application responsibilities are included
 - ▶ For example, if you are granting access for a manager to see all output for subordinates, multiple responsibilities may be required but to maintain organization security, you may not want to grant access at the application level

User Management: Security Administration Setup

User Management : Security Administration Setup

- Enables Delegated Administration privileges for one or more actions:
 - User Administration – View/Update User, Reset Password
 - Role Administration – Create Role, Manage Role, Manage Role Hierarchy, Run Security Wizard, Assign/Revoke Role
 - Organization Administration – Enable User in External Organization (Customer Only) to manage users for that External Organization

User Management : Security Administration Setup

■ Prior to Running Wizard

■ Determine whether passwords are generated automatically or manually

- ▶ If manual, set profile option “Manual Password Reset Enabled” to Yes

■ Introduced in 12.2.6

■ MOS Doc ID 2260179.1

■ Sends an email to user with password requested by Admin or through self-service

■ Note the Login Assistance link sends an email to user with reset password link rather than password which is the preferred method

■ Application → Menu

- ▶ Unclick Grant for line 35 on “User Management – User Administration and Setups” menu

■ Clear Cache using Functional Administrator Responsibility

Seq	Prompt	Submenu	Function	Description	Grant
1	Users		Search Person / User UI		<input type="checkbox"/>
2		User Maintenance UI's			<input type="checkbox"/>
3	Roles & Role Inhe		Search Roles UI		<input type="checkbox"/>
4		Role & Registration Setup			<input type="checkbox"/>
5	Role Categories		Role Categories UI		<input type="checkbox"/>
6	Registration Proc		Search Registration Proc		<input type="checkbox"/>
35	Responsibility		Search Responsibility		<input checked="" type="checkbox"/>
40	Proxy Configurati	Proxy User Administration			<input type="checkbox"/>
76	Security Report	W3H Homepage			<input type="checkbox"/>

User Management : Security Administration Setup

■ Prior to Running Wizard

■ Create a new “IS Test Role” as shown here

- ▶ The goal is to create limited user management privileges for this role
- ▶ Example is to create a role to update passwords

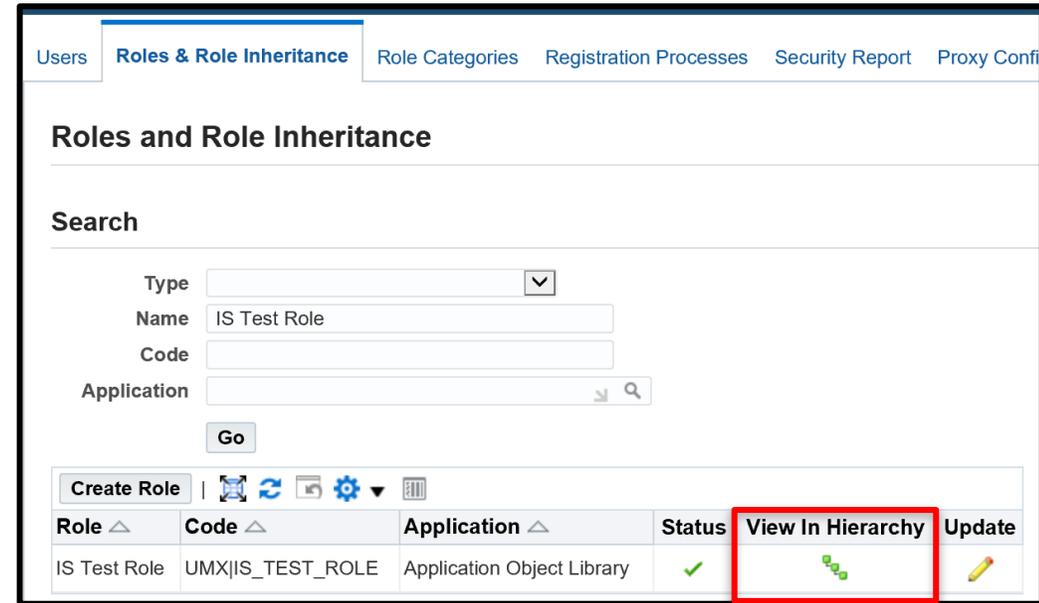
The screenshot displays the Oracle Security Administration console interface. The main navigation tabs include 'Users', 'Roles & Role Inheritance', 'Role Categories', 'Registration Processes', 'Security Report', 'Proxy Configuration', and 'Responsibility'. The 'Roles & Role Inheritance' tab is active, and the page title is 'Update Role : IS Test Role'. The page contains several input fields for role configuration:

- Category:** Security Administration (dropdown menu)
- Application:** Application Object Library (dropdown menu with search icon)
- Role Code:** UMX|IS_TEST_ROLE
- Active From:** 26-Apr-2016 (calendar icon)
- Active To:** (empty field with calendar icon)
- Display Name:** IS Test Role
- Description:** Test Role for User Management Security Wizards (text area with scrollbars)

At the bottom of the page, there is a 'Permissions' section with a 'Create Grant' button and several utility icons (refresh, undo, redo, settings, etc.).

User Management : Security Administration Setup

- Prior to Running Wizard
 - Re-query the role you just created and click on the View in Hierarchy icon



- Click the Add Node icon to add the **User Management** responsibility to the Role Hierarchy for new role, resulting in hierarchy shown below

Focus	Name	Code	Application	Active	Update	Add Node	Remove Node
	▲ All Roles, Responsibilities, and Groups						
📍	IS Test Role	UMX IS_TEST_ROLE	Application Object Library	✓	✎	+	
	User Management	FND_RESP FND UMX STANDARD	Application Object Library	✓	✎	+	✎

User Management : Security Administration Setup

- Prior to Running Wizard
 - Create grant as shown to right
 - ▶ Grantee is your “IS Test User” role
 - Assign this new role to user(s) who don't have Security Administrator role, but need to perform password administration
- Now you have a responsibility with menus but not access to data yet or limits on permissions

The screenshot shows a web interface for updating a role grant. The breadcrumb path is 'Roles & Role Inheritance > Update Role : IS Test Role >'. The main heading is 'Update Grant: UMX Menus' with 'Cancel!' and 'Apply' buttons. A legend indicates that an asterisk (*) denotes a required field. The form contains the following fields:

- Name:** UMX Menus
- Description:** (empty text area)
- Effective From:** 25-Feb-2019
- Effective To:** (empty date field)

Security Context

Define the context when the grant is applied by selecting a grantee, a responsibility and/or operating unit.

- Grantee Type:** Group Of Users
- Grantee:** IS Test Role
- Operating Unit:** (dropdown menu)
- Responsibility:** (dropdown menu)

Set

Select the permission set or menu navigation set that defines the grantee's access.

- Set:** User Maintenance UI's

User Management : Security Administration Setup

■ To Run Wizard

- Query the role created – IS Test Role
- Click the update pencil
- Click **Save**, then **Security Wizards**, then the run Wizard icon for **User Management : Security Administration Setup**

Roles & Role Inheritance > Update Role : IS Test Role >

Security Wizards

Role Name IS Test Role Role Code UMX|IS_TEST_ROLE

Name	Description	Run Wizard
CE UMX Security wizard		
User Management : Security Administration Setup	Function for UMX security administration setup wizard	
Concurrent Processing: Security Administration Setup	Function for Concurrent Processing Security Administration Setup Wizard	
Flexfield Value Sets: Security Administration Setup	Function for Flexfield Value Set Security Administration Setup Wizard	

User Management : Security Administration Setup

- Select whether access is for User, Role, or Organization
 - Our Example - allow role to reset Passwords for users with no other updates
 - On the **User Administration** tab, click **Add More Rows**

Roles & Role Inheritance > Update Role : IS Test Role > Security Wizards >

[Save](#) [Apply](#) [Cancel](#)

Delegated User Administration

Define the administration privileges for administrators that assign/revoke user accounts and roles.

Role Name IS Test Role **Role Code** UMX|IS_TEST_ROLE

User Administration Organization Administration Role Administration

User Administration privileges are defined for administrators that assign/revoke user accounts and roles. Select the set of users that administrators (assigned the role above) should be able to manage.

Details	* Users	* Permissions	Remove
	No User Administration privileges defined for this role		

[Add More Rows](#) [Create Instance Set for Users](#)

User Management : Security Administration Setup

User Administration

- Select which users can be updated (**Data security**), then which Permission can be updated (**Function Security**)
 - Only allowed to select one Permission per type of User
- Click **Apply** or **Save**

The screenshot shows the Oracle Security Administration interface for 'Delegated User Administration'. The breadcrumb trail is 'Roles & Role Inheritance > Update Role : IS Test Role > Security Wizards'. The role name is 'IS Test Role' and the role code is 'UMXJIS_TEST_ROLE'. The 'User Administration' tab is selected, showing a list of users and permissions. A dropdown menu is open for the 'Users' column, with 'All People' selected. Another dropdown menu is open for the 'Permissions' column, with 'Reset Password' selected. The 'Save' and 'Apply' buttons are highlighted with a red box in the top right corner.

Roles & Role Inheritance > Update Role : IS Test Role > Security Wizards >

Delegated User Administration

Define the administration privileges for administrators that assign/revoke user accounts and roles.

Role Name IS Test Role Role Code UMXJIS_TEST_ROLE

User Administration Organization Administration Role Administration

User Administration privileges are defined for administrators that assign/revoke user accounts and roles. Select the set of users that administrators (assigned the role above) should be able to manage.

Users	Permissions	
All People		Remove
People in Partner Organizations		
All People	Reset Password and Manage User Account Reset Password Edit Person Details Edit Person Details and Manage User Account All User Administration Privileges Basic User Administration Privileges Query Person Details Edit Person Details and Reset Password Manage User Account	
People in the Administrator's own Organization		

User Management : Security Administration Setup – Results

User Administration

Navigator - User Management

Functions Documents

Users

Users

Users

User Maintenance

Search for people and user accounts. All fields except "First Name" are case insensitive. For wildcard searches, please use "%"

Search

User Name Role

Email

Last Name

First Name

User Management

Maintain User Accounts

- Register new people, create/disable user accounts, and reset passwords.

Control Access

- Grant access to different parts of the system by assigning/revoking roles.

Register

Last Name	First Name	Email	User Name	Status	Create User	Reset Password	Update
No search conducted.							

User Management : Security Administration Setup – Results

User Administration

- Query user linked to Employee / Customer / Supplier
 - Note: Cannot enter Role name and see all users with that role
 - Click the Reset Password Link

The screenshot displays the 'Users' management interface. At the top, there is a 'User Maintenance' section with a search bar and a 'User Management' button. Below this is a 'Search' section with input fields for 'User Name' (containing 'kbrownfield'), 'Email', 'Last Name', and 'First Name', along with a 'Role' dropdown and a 'Go' button. A table at the bottom shows search results for 'Brownfield, Karen' with columns for 'Last Name', 'First Name', 'Email', 'User Name', 'Status', 'Create User', 'Reset Password', and 'Update'. The 'Reset Password' link is highlighted with a red box. A popup window titled 'Users' is open, showing details for the user 'KBROWNFIELD', including 'Person' (Brownfield, Karen), 'Customer', 'Supplier', 'E-Mail' (karen.brownfield@infosemantics.com), and 'Status' (Active).

User Management : Security Administration Setup – Results

User Administration

- Cannot query user not linked to Customer or Supplier or Employee
 - So, you can't change the SYSADMIN password 😊
- Cannot query your own user record

The screenshot displays the 'User Maintenance' interface. The search results table shows 'No results found.' for the query 'SYSADMIN'. An overlay window titled 'Users' provides details for the user 'SYSADMIN':

Field	Value
User Name	SYSADMIN
Password	
Description	System Administrator
Status	Active
Person	
Customer	
Supplier	
E-Mail	karen.brownfield@infosemantics.com
Fax	

Below the search results, there is a 'Control Access' section with a description: 'Grant access to different parts of the system by assigning/revoking roles.'

User Management : Security Administration Setup – Results

User Administration

- Does enable resetting password
 - Choose Generate Automatically or Enter Manually

The screenshot shows a web interface for user management. At the top left, there is a 'Users' tab. Below it, the breadcrumb 'Users >' is visible. The main heading is 'Reset Password'. On the right side of this heading, there are 'Cancel' and 'Submit' buttons. A legend indicates that an asterisk (*) denotes a required field. The 'User Name' field is populated with 'kbrownfield'. The 'Password' section has two radio button options: 'Generate Automatically' (which is unselected) and 'Enter Manually' (which is selected). Below these options are two input fields: '* Password' and '* Confirm Password'. The '* Password' field has a note '(5 characters or more)' below it. On the right side of the form, there is a 'Quick Tips' box with a clock icon. The text in the box states: 'Account information (User Name, Password) will be sent by email.' and 'Passwords expire automatically and must be changed upon first login.'

User Management : Security Administration Setup – Results

User Administration

- Does allow creation of new user (it shouldn't)
- In the process of researching this issue

The screenshot displays the Oracle User Administration interface. The main window is titled 'Users' and contains a 'User Maintenance' section with a search bar and a 'Search' form. The search form includes fields for User Name, Email, Last Name, and First Name, along with a 'Go' button. Below the search form is a table with columns for Last Name, First Name, Email, and User Name. The table is currently empty, with the text 'No search conducted.' displayed. A 'Register' dropdown menu is set to 'User Account'. A 'Go' button is also present next to the dropdown.

Overlaid on the main window is a smaller window titled 'Create User Account'. This window contains a 'Quick Tips' box with the text: 'Account information (User Name, Password) will be sent by email. Passwords expire automatically and must be changed upon first login.' The 'Create User Account' form includes a legend: '* Indicates required field'. The form fields are: User Name, Active From (26-Feb-2019), Active To, Password, Email, Description, Fax, and Confirm Password. There are also radio buttons for Password Expiration: Days, Access, and None (selected). At the bottom, there is a 'Link to a Party' section with dropdown menus for Person, Supplier, and Customer, each with a search icon.

User Management : Security Administration Setup – Results

User Administration

- Does not allow creation of External Organization Contact

The screenshot displays the 'Users' section of a user management interface. It includes a search form with fields for User Name, Email, Last Name, and First Name, along with a Role dropdown menu. Below the search form is a table with columns for Last Name, First Name, Email, User Name, Status, Create User, Reset Password, and Update. The table currently shows 'No search conducted.' A callout box on the right side of the interface displays an error message: 'Error: You do not have privileges to manage any organization'.

User Management

- Maintain User Accounts**
 - Register new people, create/disable user accounts, and reset passwords.
- Control Access**
 - Grant access to different parts of the system by assigning/revoking roles.

Register **External Organization Contact** Go | [Icons]

Last Name	First Name	Email	User Name	Status	Create User	Reset Password	Update
No search conducted.							

Error
You do not have privileges to manage any organization

User Management : Security Administration Setup – Results

User Administration

- Although Update link is there, clicking it does not expose fields to update
 - No Roles for the User listed and cannot assign any
 - ▶ So even though the earlier issue allows you to create a user, you cannot give them any access

Users

Users >

Update User: kbrownfield

Cancel Reset Password Save Apply

* Indicates required field

Prefix	User Name	kbrownfield
First Name	Email	karen.brownfield@infosemantics.com
Middle Name	Status	Active
Last Name	Active From	29-Dec-2014
Suffix	Active To	

Quick Tips
Personal information originates from the HR system and cannot be updated here.

Roles Contact Information Securing Attributes

Changes can only be made for roles for which you have been granted administrative privileges.

Assign Roles

Search All Roles GO

Details	Role
	No Roles Assigned to this user

http://r122visint5.infosemantics.net:8225/?_t=fredRC&enc=UTF-8&_minWidth=750...

Search and Select: Assign Roles

Cancel Select

Search

To find your item, select a filter item in the pulldown list and enter a value in the text field, then select the "Go" button.

Search By Roles and Responsibilities % Go

Results

No items were found matching your request.

Name	Description	Type	Code
No Items found			

User Management : Security Administration Setup

Role Administration

- We will continue to use the IS Test Role in our example
- Click the **Role Administration** tab
- First decision – can this role create additional roles (typically no – not checked)
- Then click **Create New Criteria**

Roles & Role Inheritance > Update Role : IS Test Role > Security Wizards >

Save Apply Cancel

Delegated User Administration

Define the administration privileges for administrators that assign/revoke user accounts and roles.

Role Name IS Test Role Role Code UMX\IS_TEST_ROLE

User Administration Organization Administration **Role Administration**

Role Administration privileges are defined for administrators that can assign/revoke user accounts and roles, update roles, alter role hierarchies and run security wizards. Select what roles can be administered by the Role Administrator (administrator who has the above role assigned).

Allow Creation of New Roles

*Allow the users having this Admin Role to create new roles.

Role Administration Criteria

Create New Criteria

View / Modify Criteria

*Add or Remove roles to/from an already defined criteria and modify the associated privileges.
*The privileges apply only to the selected roles.

Criteria Name

View / Modify * Privileges Only

Go Clear Delete Criteria

User Management : Security Administration Setup

Role Administration

- Second decision – Which Roles and What Actions can be administered by this role
- Either click “Define Privileges for all the roles in the System” or enter criteria
- For specific role, must know the Role Code or search by application or role category
 - ▶ There is no LOV for Role Code

The screenshot shows the Oracle Security Administration console. The breadcrumb trail is 'Roles & Role Inheritance > Update Role : IS Test Role > Security Wizards >'. The page title is 'Delegated User Administration' with a description: 'Define the administration privileges for administrators that assign/revoke user accounts and roles.' The 'Role Name' is 'IS Test Role' and the 'Role Code' is 'UMXJIS_TEST_ROLE'. There are 'Save', 'Apply', and 'Cancel' buttons at the top right. The 'Role Administration' tab is selected, showing instructions: 'Role Administration privileges are defined for administrators that can assign/revoke user accounts and roles, update roles, alter role hierarchies and run security wizards. Select what roles can be administered by the Role Administrator (administrator who has the above role assigned).' There is a checkbox for 'Allow Creation of New Roles' with a note: '*Allow the users having this Admin Role to create new roles.' Below is the 'Role Administration Criteria' section with a sub-section 'Define New Criteria' and instructions: '*Define a New Criteria and associate privileges to the roles present in the criteria. *The privileges apply only to the selected roles.' A checkbox 'Define Privileges for all the roles in the System' is checked and highlighted with a red box. Below it is a form with fields for 'Criteria Name', 'Role Code', 'Application' (with a search icon), and 'Role Category' (a dropdown menu). A checkbox 'Define privileges for all roles satisfying the above criteria' is also present. At the bottom are 'Search', 'Reset', and 'Cancel' buttons.

User Management : Security Administration Setup

Role Administration

- In this example, search for roles for the Payables Application

User Administration Organization Administration **Role Administration**

Role Administration privileges are defined for administrators that can **assign/revoke use**

Allow Creation of New Roles
*Allow the users having this Admin Role to create new roles.

Role Administration Criteria

Define New Criteria

*Define a New Criteria and associate privileges to the roles present in the criteria.
*The privileges apply only to the selected roles.

Define Privileges for all the roles in the System

Criteria Name

Role Code

Application

Role Category

Define privileges for all roles satisfying the above criteria

User Management : Security Administration Setup

Role Administration

- Select a role to administer by checking the check boxes
 - For this example, **Oracle Payables Superuser for Vision Operations**
- Click the **Assign Roles** and **Revoke Roles** check boxes
- Click **Save**
- This will allow users with the IS Test User role to assign other roles or revoke this role for users that meet all the various criteria assigned to the IS Test User role

The screenshot displays the Oracle Security Administration interface. At the top, there is a search bar with 'Role Code' selected and a 'Go' button. Below the search bar are 'Select All' and 'Select None' options. A table lists several roles, with the second row, 'FND_RESP|SQLAP|PAYABLES_OPERATIONS|STANDARD', highlighted with a red box. Below the table, the 'Specify Privileges for Selected Roles' section has 'Assign Roles' and 'Revoke Roles' checked, also highlighted with a red box. At the bottom right, 'Save', 'Apply', and 'Cancel' buttons are visible, with 'Save' highlighted by a red box.

Select	Role Code	Role Name	Description
<input type="checkbox"/>	FND_RESP SQLAP PAYABLES_MANAGER STANDARD	Payables Manager-Pay	
<input checked="" type="checkbox"/>	FND_RESP SQLAP PAYABLES_OPERATIONS STANDARD	Payables, Vision Operations (USA)	Oracle Payables Superuser for Vision Operations
<input type="checkbox"/>	FND_RESP SQLAP PAYABLES_SSC_FR STANDARD	Payables, SSC France	Oracle Payables Superuser for SSC France
<input type="checkbox"/>	FND_RESP SQLAP PAYABLES_SSC_IT STANDARD	Payables, SSC Italy	Oracle Payables Superuser for SSC Italy
<input type="checkbox"/>	FND_RESP SQLAP PAYABLES_SSC_US01A STANDARD	Payables, SSC US OU 01	Oracle Payables Superuser for SSC US OU 01
<input type="checkbox"/>	FND_RESP SQLAP PAYABLES_SSC_US02 STANDARD	Payables, SSC US OU 02	Oracle Payables Superuser for SSC US OU 02
<input type="checkbox"/>	FND_RESP SQLAP PAYABLES_VISION_UKR STANDARD	Payables, Vision Ukraine	Payables, Vision Ukraine
<input type="checkbox"/>	UMX AP_ENDECA_ACCESS_ROLE	Payables Endeca Access Role	Payables Endeca Access Role

Specify Privileges for Selected Roles

Update Roles Manage Grants Alter Role Hierarchy
 Assign Roles Revoke Roles Run Security Wizard

Save Apply Cancel

User Management : Security Administration Setup - Results

Role Administration

- User with IS Test User role can now see users with roles they are authorized to administer
 - I can see Karen because she is a Payables Superuser
 - But what about new users who don't have any roles yet?

Users

Users > **Update User: kbrownfield** Cancel | Reset Password | Save | Apply

* Indicates required field

Prefix		User Name	kbrownfield
First Name	Karen	Email	karen.brownfield@infosemantics.com
Middle Name		Status	Active
Last Name	Brownfield	Active From	29-Dec-2014
Suffix		Active To	

Quick Tips
Personal information originates from the HR system and cannot be updated here.

Roles | Contact Information | Securing Attributes

Changes can only be made for roles for which you have been granted administrative privileges.

Assign Roles

Search All Roles |

Details	Role	Description	Status	Remove
	Workflow User Web Applications	Responsibility to access general workflow functions	Assigned	

User Management : Security Administration Setup - Results

Role Administration

- Potential Recommendation – If you want your payables manager to be able to assign payables roles to any employee, especially new employees, create an “Employee” role and give the payables manager access to assign/revoke payables roles and the employee role
 - They will be able to select all employees because everyone is initialized with one role
 - **However...** they could accidentally revoke the employee role too
 - ▶ Train administrators not to do this
- Preferred method would be to set up self service access requests with approval by the manager

Security Reports

- Even though only partial access is granted, user appears on security report with implication that full access is granted
- Clicking the arrow to show details will show it was inherited from IS Test User so consider creating a more descriptive name indicating partial privileges

Users Roles & Role Inheritance Role Categories Registration Processes Responsibility Proxy Configuration **Security Report**

[Search Report](#) | [Report Status](#)

Security Reports

Report Type: List of Users

For a Given: Role/Responsibility | User Management

View As: HTML | On Screen

Notify Report Status

Schedule Recurring Reports

[Show Advanced Search](#)

[Go](#) [Clear](#)

Security Reports

Use Schedule Recurring Report to schedule periodic offline generation of reports

Use Advanced Search to refine your search further.

Generate Reports in MS Excel or Adobe PDF format

List of Users Having Role User Management

Rows 1 to 15

Details	User Name	Assignment Type	Assignment Status	User Status
▶	OPERATIONS	Inherited	Inactive	Active
▶	KBROWN	Inherited	Active	Active
▶	JOGUNTUASE	Inherited	Active	Active
▶	BJOSEPH	Direct	Active	Active
▶	JKBOWERS	Direct	Active	Active
▶	CMOORE	Direct	Active	Active
▶	KBWIZARD	Inherited	Active	Active
▶	EBUSINESS	Direct	Active	Active

Grant Security Context

Grant Security Context

- If choosing a specific user, must repeat for all applicable users
- If choosing a role, role can be assigned to multiple users using User Management
 - For example, can create role Employee, assign grant to this role, then assign role to all employees
 - Roles can inherit responsibilities, but since role is assigned to user, not dependent on being in specific responsibility
- If choosing operating unit, grant only applicable when operating unit context is set (i.e. won't work in GL)
- If choosing responsibility, and responsibility assigned to user (or inherited via role), grant applicable regardless of current responsibility
 - Responsibilities can inherit roles or roles can inherit responsibilities
- **Grants are additive**

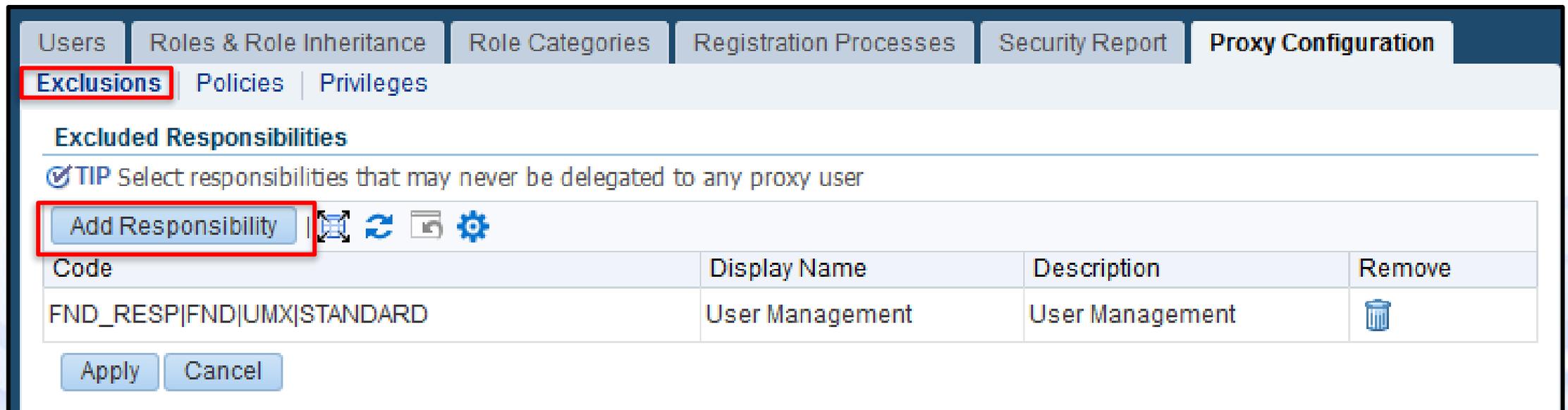
Proxy Users

Proxies

- Proxy authority can be granted to another user for a specific time period
 - Cover vacation/leave of absence/emergencies
- Audit control - Actions are tracked to show delegate is acting on behalf of delegator
- 12.2.4+ new features (Now backported to 12.1)
 - Limit responsibilities and workflow notifications granted to proxy user
 - Responsibility exclusions
 - Delegation policies
 - Grant proxy capabilities to all to selected users
 - Patch for 12.1 is 19804456

Proxy Configuration – 12.2.4+

- User Management → Proxy Configuration → Exclusions (What cannot be delegated)
- Identify responsibilities which can never be delegated
 - ▶ Click **Add Responsibility** to add any responsibility such as User Management, that should never be delegated
- By default, nothing is excluded



Users | Roles & Role Inheritance | Role Categories | Registration Processes | Security Report | Proxy Configuration

Exclusions | Policies | Privileges

Excluded Responsibilities

TIP Select responsibilities that may never be delegated to any proxy user

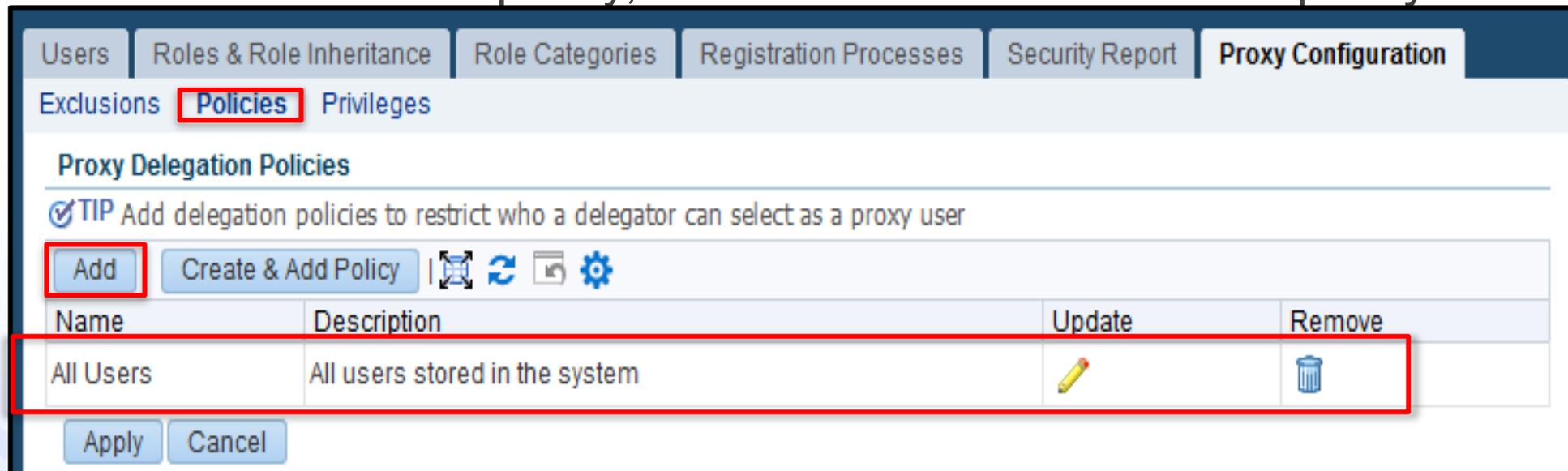
Add Responsibility |    

Code	Display Name	Description	Remove
FND_RESP FND UMX STANDARD	User Management	User Management	

Apply Cancel

Proxy Configuration – 12.2.4+

- User Management → Proxy Configuration → Policies (Who can you delegate to?)
 - By default, you can delegate proxy access to any user
 - In 12.2.4+, you can add a pre-defined policy using the Add button or create your own using the Create and Add Policy button
 - Click **Add** to add a new policy, then remove the “All Users” policy



The screenshot shows the 'Proxy Configuration' interface with the 'Policies' tab selected. The 'Add' button is highlighted in red. Below the buttons, a table lists the existing policies. The 'All Users' policy row is highlighted in red.

Name	Description	Update	Remove
All Users	All users stored in the system		

Proxy Configuration – 12.2.4+

- Enter % and click Go to see all seeded policies
- In this example, we will only allow a user to delegate only to their direct supervisor and peers of that supervisor
- Check the checkbox for the policy and click **Select**

Search and Select: Add ✕

Search

To find your item, select a filter item in the pulldown list and enter a value in the text field, then select the "Go" button.

Search By Name ▾ Go

Results

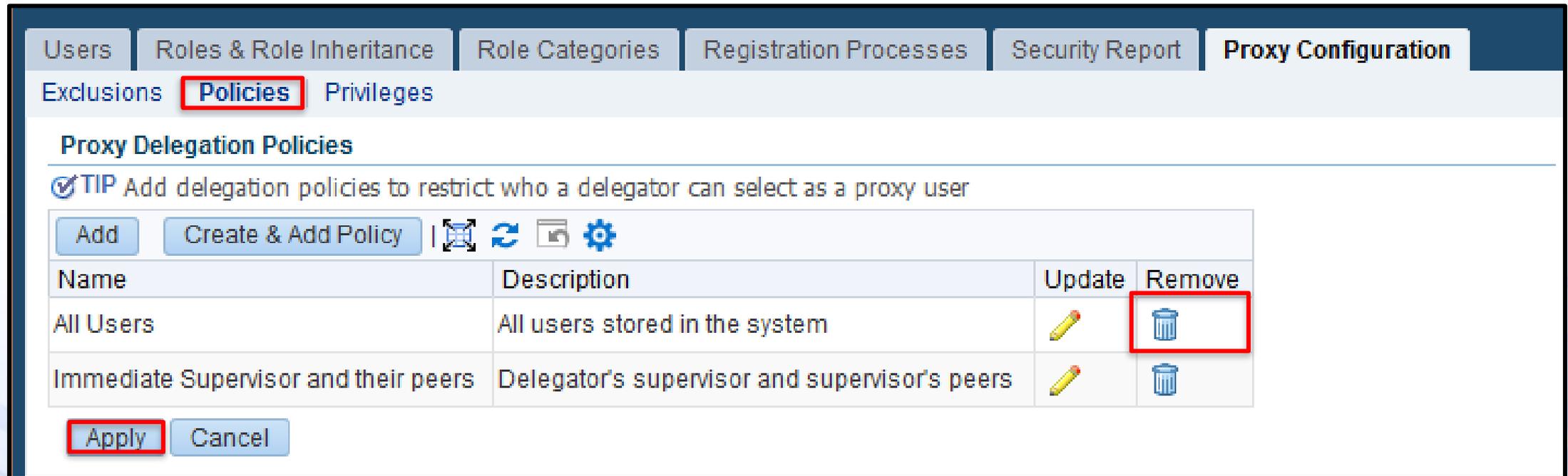
<input type="checkbox"/>	Name	Description	Code
<input checked="" type="checkbox"/>	Immediate Supervisor and their peers	Delegator's supervisor and supervisor's peers	UMX_IMMEDIATE_SUPERVISOR
<input type="checkbox"/>	Supervisor's Supervisor and his peers	Delegator's supervisor's supervisor and peers of that supervisor	UMX_SUPERVISORS_SUPERVISOR
<input type="checkbox"/>	Direct Line of Command	Delegator's direct reports	UMX_REPORTTEE_DIRECT_LINE
<input type="checkbox"/>	Second line of Command	Delegator's direct reports and their subsequent direct reports.	UMX_REPORTTEE_TILL_SECOND_LINE
<input type="checkbox"/>	Third line of Command	Delegator's direct reports, plus their direct reports and their subsequent reports	UMX_REPORTTEE_TILL_THIRD_LINE
<input type="checkbox"/>	All Employees	All employees with user accounts stored in the system	UMX_ALL_EMPLOYEES

[About this Page](#)

Cancel Select

Proxy Configuration – 12.2.4+

- Click on the trash can to remove the policy for All Users
 - Click **Apply**
- Remember, you can also create a policy if the seeded policies do not meet your needs using **Create and Add Policy**



The screenshot shows the Oracle Proxy Configuration interface. The 'Policies' tab is selected and highlighted with a red box. Below the navigation tabs, there are buttons for 'Add', 'Create & Add Policy', and several icons. A table titled 'Proxy Delegation Policies' is displayed, with columns for Name, Description, Update, and Remove. The 'Remove' column for the 'All Users' policy is highlighted with a red box. At the bottom, there are 'Apply' and 'Cancel' buttons, with 'Apply' also highlighted with a red box.

Users Roles & Role Inheritance Role Categories Registration Processes Security Report **Proxy Configuration**

Exclusions **Policies** Privileges

Proxy Delegation Policies

✓ TIP Add delegation policies to restrict who a delegator can select as a proxy user

Add Create & Add Policy [Icons]

Name	Description	Update	Remove
All Users	All users stored in the system	[Pencil]	[Trash Can]
Immediate Supervisor and their peers	Delegator's supervisor and supervisor's peers	[Pencil]	[Trash Can]

Apply Cancel

Proxy Configuration – 12.2.4+

- User Management → Proxy Configuration → Privileges (Who can delegate)
- Grant proxy privileges to all users
 - ▶ “All Users” is the default setting – this is a potential security risk
 - ▶ Consider limiting to selected users (i.e. Managers)

Users | Roles & Role Inheritance | Role Categories | Registration Processes | Security Report | **Proxy Configuration**

Exclusions | Policies | **Privileges**

Proxy Delegation Privilege

TIP Select which user roles or responsibilities include the privilege to delegate to a proxy user

Enable Proxy Delegation Privileges for

All Users

Users with the Selected Roles or Responsibilities

Apply Cancel

Proxy Configuration – 12.2.4+

- User Management → Proxy Configuration → Privileges
 - Grant proxy privileges to selected users
 - ▶ Choose the “Users with Selected Roles or Responsibilities” radio button, then click **Add**

Users | Roles & Role Inheritance | Role Categories | Registration Processes | Security Report | **Proxy Configuration**

Exclusions | Policies | **Privileges**

Proxy Delegation Privilege

TIP Select which user roles or responsibilities include the privilege to delegate to a proxy user

Enable Proxy Delegation Privileges for All Users **Users with the Selected Roles or Responsibilities**

Add    

Code	Name	Description	Remove
No results found.			

Apply **Cancel**

Proxy Configuration – 12.2.4+

- User Management → Proxy Configuration → Privileges
 - Search and click the checkbox for the responsibility or role
 - Click **Select**

Search and Select: Add ×

Search

To find your item, select a filter item in the pulldown list and enter a value in the text field, then select the "Go" button.

Search By

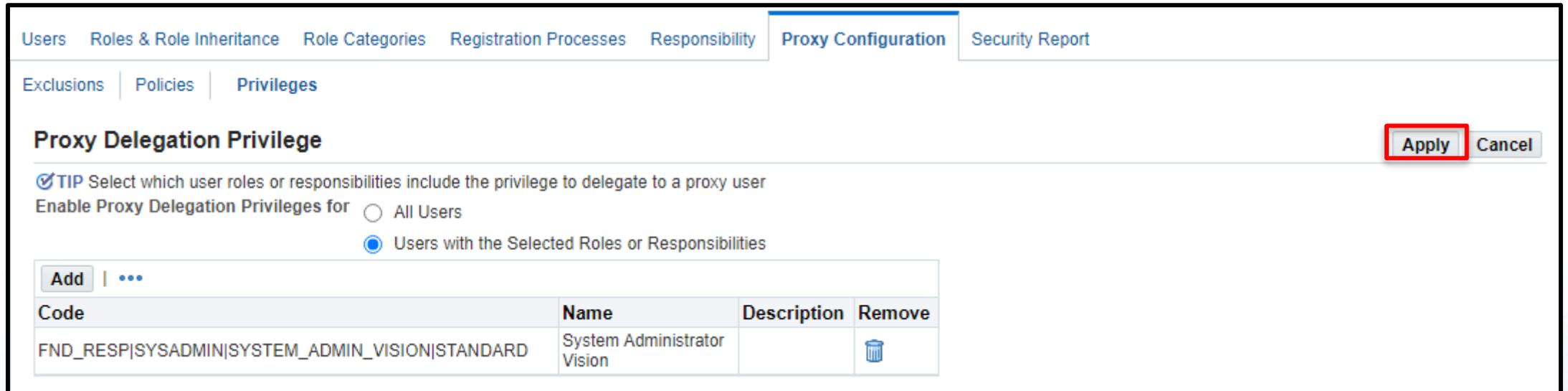
Results

<input checked="" type="checkbox"/>	Code	Name	Description
<input checked="" type="checkbox"/>	FND_RESP SYSADMIN SYSTEM_ADMIN_VISION STANDARD	System Administrator Vision	

[About this Page](#)

Proxy Configuration – 12.2.4+

- User Management → Proxy Configuration → Privileges
 - Click **Apply**

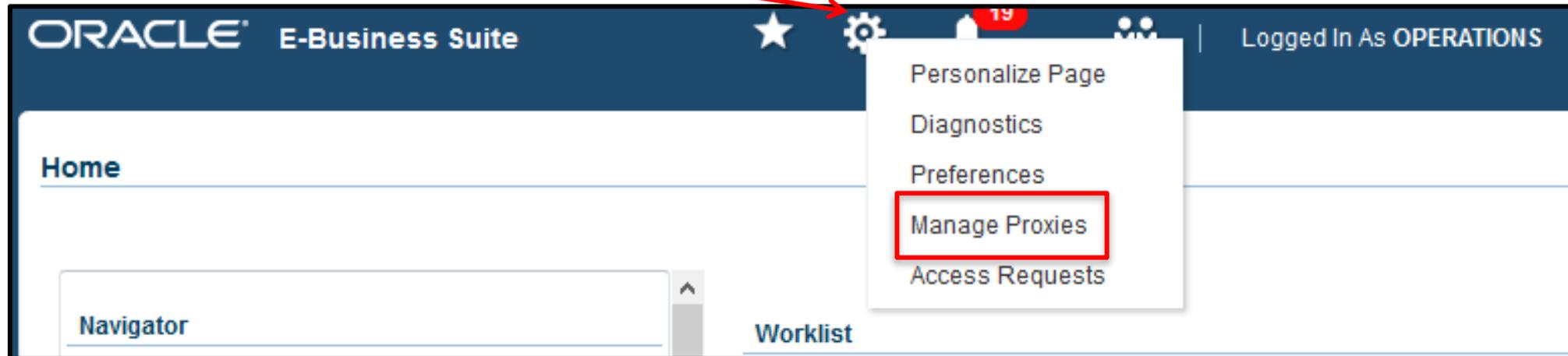


The screenshot shows the Oracle Identity Management console interface. At the top, there are navigation tabs: Users, Roles & Role Inheritance, Role Categories, Registration Processes, Responsibility, Proxy Configuration (selected), and Security Report. Below these, there are sub-tabs: Exclusions, Policies, and Privileges. The main heading is "Proxy Delegation Privilege". To the right of this heading are "Apply" and "Cancel" buttons, with "Apply" highlighted by a red box. Below the heading, there is a tip: "TIP Select which user roles or responsibilities include the privilege to delegate to a proxy user". Underneath, there are two radio buttons: "All Users" (unselected) and "Users with the Selected Roles or Responsibilities" (selected). Below the radio buttons is a table with an "Add" button and a menu icon. The table has four columns: Code, Name, Description, and Remove. The table contains one row with the following data:

Code	Name	Description	Remove
FND_RESP SYSADMIN SYSTEM_ADMIN_VISION STANDARD	System Administrator Vision		

Proxies – 12.2.4+

- Click the settings gear, then Manage Proxies



Proxies – 12.2.4+

- Click **Add Proxy**

- In early releases, this button is “Add People”

Proxy Configuration

Manage the people that can access your account and act on your behalf.

Add Proxy | **Run Proxy Report** |    

Details	Last Name	First Name	User Name	Start Date	End Date	Update
No results found.						

Proxies – 12.2.4+

- Logged in as Operations user (Pat Stock) and will give access to SBEHN to be the proxy for Pat Stock
- Choose the user name, then choose the appropriate options for responsibility and workflow access

Add People Submit Cancel

Add Proxy

* User Name

* Active From

Active To

Notes to Proxy

Grant Responsibility Access

Responsibilities None Selected All

Grant Worklist Access

Workflow Item Types None Selected All

Proxies – 12.2.4+

- To grant selected responsibility access, click the “Selected radio” button and all current responsibilities will appear
 - Move the desired responsibilities from the available column to the selected column

Grant Responsibility Access

Responsibilities None Selected All

Available Responsibilities

- Advanced Planning Administrator
- Alert Manager, Vision Enterprises
- Application Developer
- Application Diagnostics
- Approvals Management Administrator
- Approvals Management Business Analyst
- Business Intelligence System, Vision Operations (USA)
- CADView-3D Administration
- CADView-3D User
- CRL 11i Projects

Selected Responsibilities

- Asset Inquiry, Vision Operations (USA)
- Asset Tracking Super User, Vision Operations
- Assets, Vision Operations (USA)
- Bill Presentment Super User, Vision Operations (USA)

Move
Move All
Remove
Remove All

Proxies – 12.2.4+

- To grant selected worklist access, click the Selected radio button and all current workflow item types will appear
 - Move the desired item types from the available column to the selected column
- Scroll up and click **Submit**

Grant Worklist Access

Workflow Item Types None Selected All

Available Item Types

- Expenses Export
- PO Create Documents
- UMX Proxy Notification

Selected Item Types

- PO Approval
- Expenses

Move, Move All, Remove, Remove All

Proxies – 12.2.4+

- A workflow notification is sent to the user who is granted proxy access

Notification Details

To SBEHN
Sent 11-Sep-2014 12:19:06
ID 7953900

You have been granted the ability to act as a proxy for Pat Stock. In order to act as a proxy, click on the 'Switch User' global icon or link from the Navigator screen

Start Date	11-SEP-2014 00:00:00
End Date	
Notes From Delegator	

[Go to Details Page](#)

Proxies – 12.2.4+

- As the SBEHN user, click the switch user icon



- Then click the switch icon

Switch User
Select a user and act as their proxy

Switch	Last Name \triangle	First Name \triangle	User Name \triangle	Job Title	Phone	Email \triangle
	Stock	Pat	OPERATIONS	MGR500.Manager	 212-484-4505	nobody@localhost

Proxies – 12.2.4+

- Now logged in as SBEHN as Proxy for Operations

The screenshot shows the Oracle E-Business Suite interface. At the top, the user is logged in as SBEHN, and the proxy is set to OPERATIONS. The Navigator pane on the left lists responsibilities granted, and the Worklist table on the right shows item types granted.

Navigator (Only includes responsibilities granted):

- Asset Inquiry, Vision Operations (USA)
- Asset Tracking Super User, Vision Operations
- Assets, Vision Operations (USA)
- Bill Presentment Super User, Vision Operations (USA)

Worklist (Only includes item types granted):

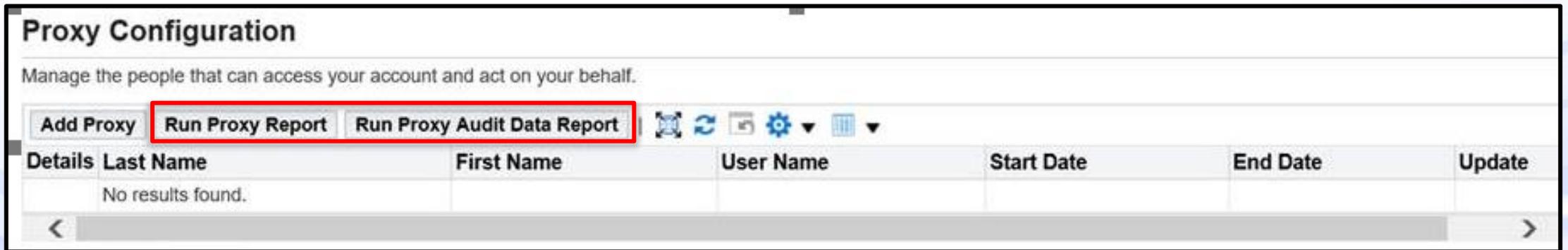
From	Type	Subject	Sent	Due
SYSADMIN SYSADMIN	Expenses	Expense W42112 (100.00 USD)	04-Sep-2014	11-Sep-2014
Brown	PO	Standard Purchase Order		

Tracking approvals by proxy user

- Audit control - Actions are tracked to show delegate is acting on behalf of delegator
 - 12.2 Patch 21463185; MOS note [2045841.1](#)
 - ▶ Records the proxy user who did an approval – but the values are stored in wf_comments
 - Oracle Support Document [738230.1](#) (How to Verify who Owns and Approves a Notification when Using the Worklist Access Functionality?)
 - `select notification_id, from_user, to_user, proxy_role
from wf_comments`
 - This table is purged when the workflow purge occurs so you may want to run a daily report before any workflow purges to find any approvals where these fields are populated or not the same
- Proxy Auditing
 - Provides a consolidated report for auditors to evaluate the transactions of proxy users or any other user on a specific data object
 - ▶ Administrators and delegators can run this report to see the transactions that were executed by the proxy user on their behalf.

Proxy Reports

- Run the **Page Access Tracking Data Migration** concurrent program to populate the Proxy Report
 - There are no parameters
- Go to Manage Proxies and click **Run Proxy Report**
 - Only shows pages accessed
- Click **Run Proxy Audit Data Report**
 - Transactions that were executed by the proxy user for tables that are set up for auditing



Proxy Configuration
Manage the people that can access your account and act on your behalf.

Add Proxy **Run Proxy Report** **Run Proxy Audit Data Report** |       

Details	Last Name	First Name	User Name	Start Date	End Date	Update
No results found.						

< >

Proxy Report Example

- The report shows all navigation completed by the proxy user

User Name	Responsibility	Action	Date
OPERATIONS	Payables Manager	LOGIN	24-Jun-2011 18:09:45
OPERATIONS	Payables Manager	LOGOUT	24-Jun-2011 18:17:44
OPERATIONS	System Administrator, Vision Insurance (USA)	RESP_CHANGE	24-Jun-2011 18:15:11
OPERATIONS	Payables Manager	RESP_CHANGE	24-Jun-2011 18:12:48
OPERATIONS	Payables Manager	Invoice Workbench	24-Jun-2011 18:12:49
OPERATIONS	Payables Manager	General Preferences	24-Jun-2011 18:16:18
OPERATIONS	Payables Manager	Manage Proxies	24-Jun-2011 18:16:21
OPERATIONS	Payables Manager	Manage Proxies	24-Jun-2011 18:16:33
OPERATIONS	Payables Manager	Proxy Report	24-Jun-2011 18:16:33
OPERATIONS	Payables Manager	Proxy Report	24-Jun-2011 18:16:50

⏪ Previous 1-10 ⏩ Next 10 ⏪

References

References – My Oracle Support

- 401463.1 – User Management Security Wizard Feature
- 394083.1 – Understanding and Using HRMS Security in Oracle HRMS
- 1457691.1 – R12/CE: Cash Management Security, UMX Security
- 435654.1 – R:12: CE:How To Run the CE UMX Security Wizard for Cash Management Responsibility?
- 403975.1 – R12 CE:How To Setup Bank Account Maintenance Security and Account Access Security
- 755809.1 – Unable to Restrict Access To Use of Bank Account By Legal Entity
- 727822.1 – How to Hide Any Tab from User Management Menu
- 1222703.1 – Tables/Views and SQL statement behind the UMX Security Infrastructure Reports

References My Oracle Support

- 1222663.1 – User Management (UMX) Security Infrastructure Reporting
- 2291928.1 – How To Create A Role To Manage Users/Roles With Selected Privileges Using User Management Responsibility (With Screenshots)
- 2399548.1 – R12 E-Business Suite User Management Administration Steps To Create A User Management Responsibility / Role With Read Only Access (View / Query Only)
- 743683.1 – How To Create a Role That Can Query Users and Reset Passwords
- 743549.1 – What is the Setup in UMX to Allow User Administrator to Administer Only Employees in An Organization

References Oracle Documentation

- Oracle E-Business Suite Flexfields Guide, Release 12.2 Part Number E22963-10
 - Chapter 6 Flexfield Value Set Security
- Oracle E-Business Suite System Administrator's Guide – Security, Release 12.1 Part Number E12843-05
 - Chapter 3 Oracle User Management Setup and Administration
- Oracle E-Business Suite Security Guide, Release 12.2 Part Number E22952-22
 - Chapter 3 Oracle User Management Setup and Administration

References – Proxy Users

- Oracle Applications System Administrator's Guide - Security
- E-Business Suite User Management SIG
 - <http://ebsumx.oaug.org/>
- Transfer of Information training

http://ilearning.oracle.com/ilearn/en/learner/jsp/offering_details_find.jsp?classid=1524577857

References – Other

- OATUG User Management / RBAC SIG - <https://www.oatug.org/ebsumx/home>
 - Resources → Documents
 - ▶ Must be a member to see presentations

Questions? Comments

