EBS User Management for Dummies

Current requirements and features including Grants, Permissions, RBAC, and Proxy users

Presented by:

Susan Behn

Vice President

Infosemantics, Inc.

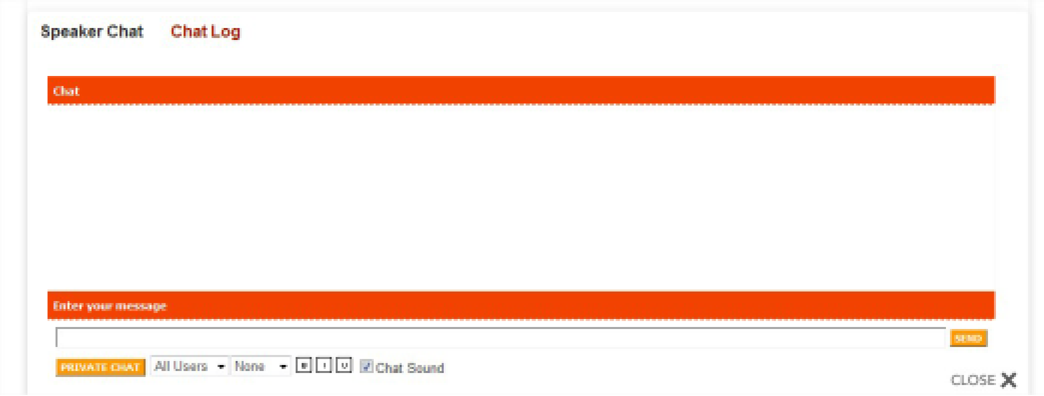
susan.behn@infosemantics.com

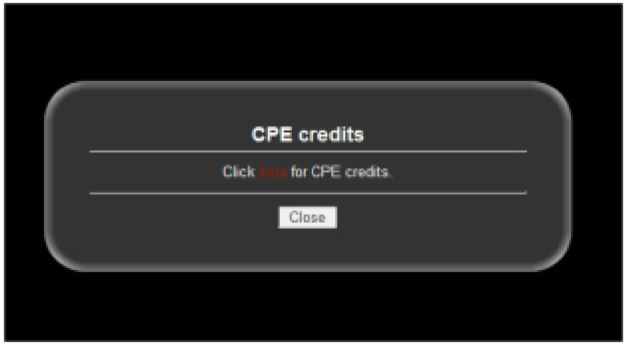
@suzybehn

EBS Answers

Virtual Conference

Webinar Mechanics




CPE credits

Click here for CPE credits.

- Submit text questions in the chat log.
- Q&A addressed at the end of the session. Answers will be posted within two weeks on our new LinkedIn Group, EBS Answers: http://www.linkedin.com/groups/EBS-Answers-4683349/about
- Polling questions will be presented during the session. If you want CPE credit for this webinar, you must answer all of the polling questions.
- A recording of today's event will be available for 90 days for conference registrants.

Learning Objectives

Objective 1: Explain role-based access control (RBAC), where it is required and where it is optional.

Objective 2: Describe how user management (UMX) and RBAC work together to mitigate security risks within Release 12.

Objective 3: Show specific recommended examples on how to set up and use some of the key functionality .

eprentise®: *Transformation Software for E-Business Suite*

Company Overview: Incorporated 2007, Helene Abrams, CEO

eprentise Can…

- Consolidate Multiple EBS Instances
- Change Underlying Structures and Configurations
  - Chart of Accounts, Other Flexfields
  - Merge or Split Ledgers or Sets of Books, Operating Units, Legal Entities, Inventory Organizations
  - Calendars, Currency, Costing Methods
  - Asset Revaluation, Inventory Valuation
- Separate Data

…So Our Customers Can:

- Reduce Operating Costs and Increase Efficiencies
  - Shared Services
  - Data Centers
- Adapt to Change
  - Align with New Business Initiatives
  - Mergers, Acquisitions, Divestitures
- Avoid a Reimplementation
- Reduce Complexity and Control Risk
- Improve Business Continuity, Service Quality and Compliance
- Streamline Operations with Visibility to All Parts of the Business
- Establish Data Quality Standards and a Single Source of Truth

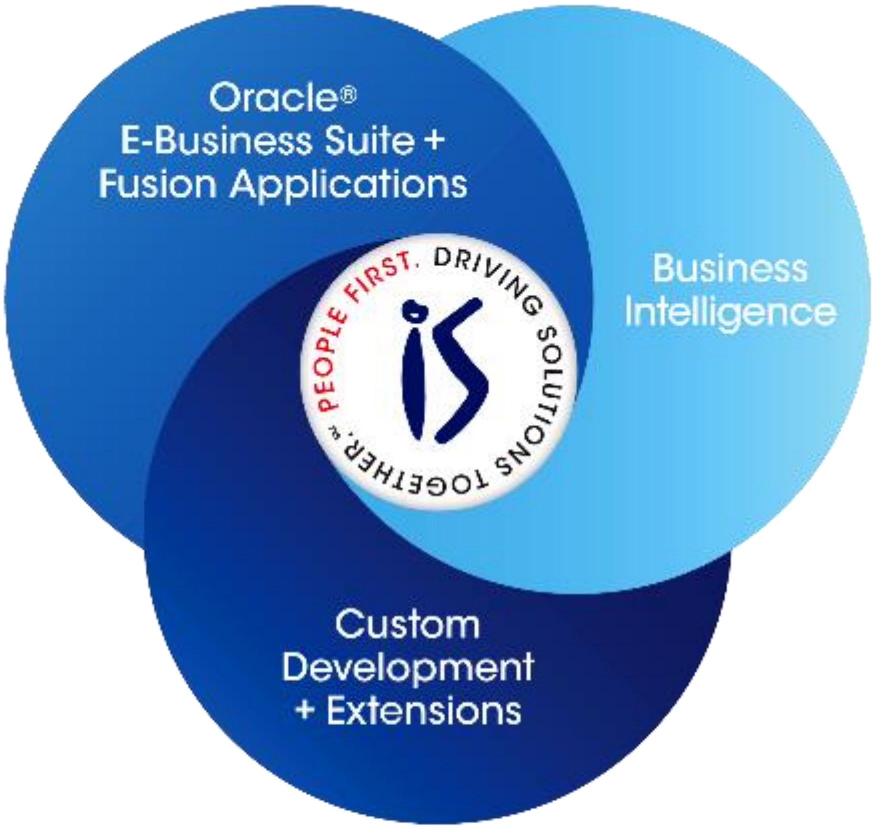
Finished But Not Done®

About the Speaker

- Oracle Ace
- Over 20 years E-Business Suite development and support
- Member-Oracle Proactive Support Customer Advisory Board
- Chair-Oracle E-Business Suite User Management SIG
- Chair-Texas-Louisiana Oracle User Group TLOAUG
- 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.*

Infosemantics℠

People first. Driving solutions together.



ORACLE® Gold Partner

- Established in 2001
- SBA 8(a) Small Business disadvantaged company
- GSA Schedule contract GS-35F-0680V
- Texas State HUB vendor
- For more information, check out our web site at www.Infosemantics.com
  - R12.1.3, R12.2, OBIEE public vision instances
  - Posted presentations on functional and technical topics

Abstract

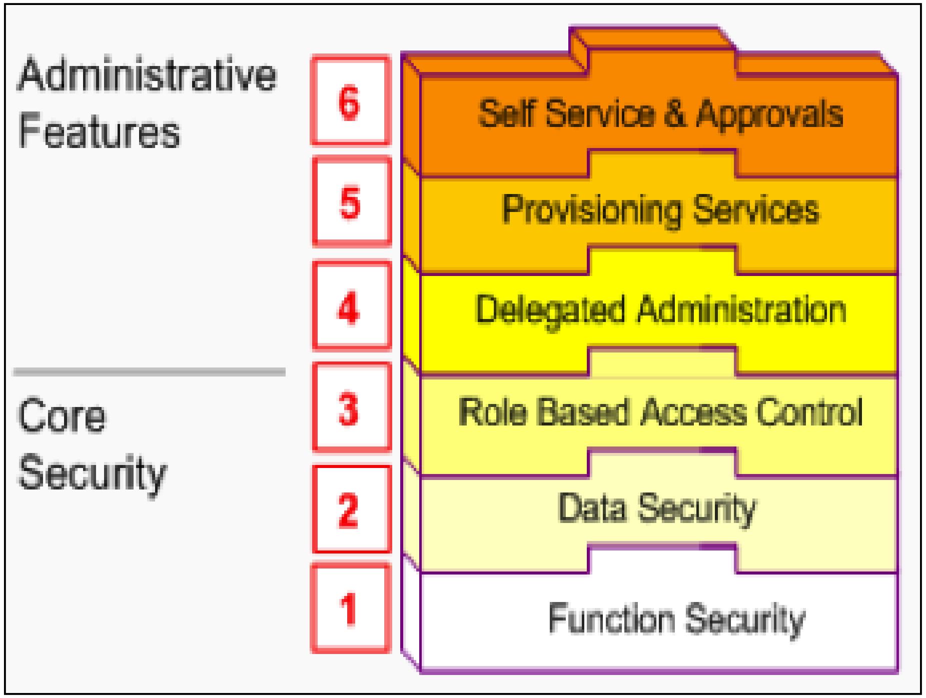
Unravel the mysteries of role based access control, grants and permissions to provide more granular function and data control. The presentation covers basic concepts, how to apply these concepts using real examples and the required setups in 12.1 and 12.2. Also covered are the most recent improvements in proxy user functionality to reduce auditor concerns about this functionality

Agenda

- Understanding User Management Principles
  - Overview
  - Building Blocks for User Management
  - Modeling Security Policy Basic Example
- User Management Surprises
  - Reporting
  - Help → Examine (Update and Read Only)
  - Integration Repository
  - Grant Worklist Access
  - View Concurrent Requests
  - Flexfield Value Set Security
- Security Reports
- Proxy User Access (If time allows)
- References

User Management Layers

- Core security – levels 1 – 2 is accomplished through AOL or with grants and permissions
- Core security – level 3 is required for some apps
- Administrative features – levels 4 – 6 are optional



6 User access requests with AME Approval Processes

5 Registration processes

4 Administer functions/data for specific groups

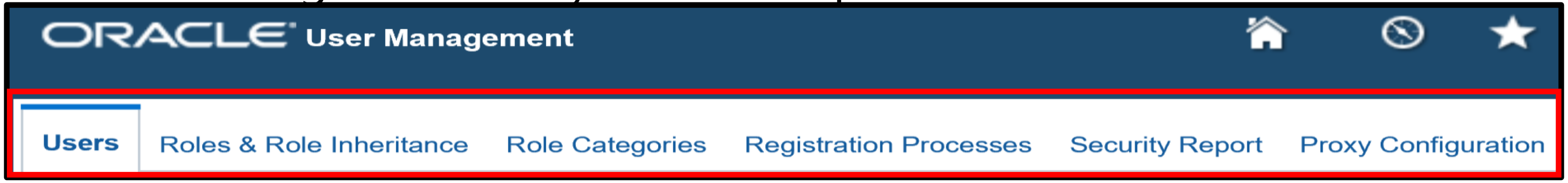
3 Grant access to roles that include function/data security

2 What data can a user see

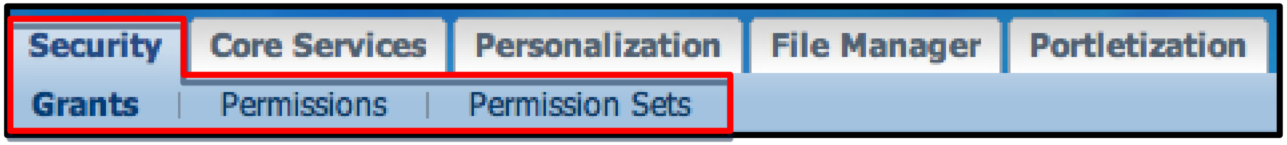
1 What can a user do

Components by Responsibility

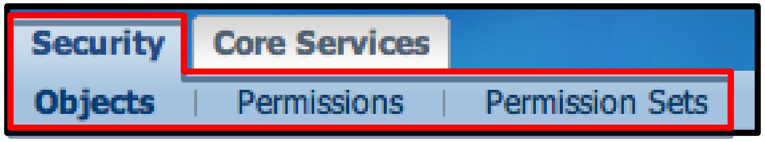
- System Administrator Responsibility
  - Manage responsibilities and menus; Create users
- User Management – Layers 3 and up



- Functional Administrator Responsibility
  - Function Security Layer



- Functional Developer Responsibility
  - Data Security Layer



User Management Building Blocks

- Functional **D**eveloper Responsibility (Secure the data)
- Objects
  - **D**ata to be secured – a table or view
    - FND_OBJECTS
    - FND_OBJECTS_TL
- Object Instance Sets
  - "WHERE" clause for the object
    - FND_OBJECT_INSTANCE_SETS
    - FND_OBJECT_INSTANCE_SETS_TL

User Management Building Blocks

- Permissions – 2 types – function and data
  - Functional **D**eveloper or Functional Administrator Responsibility
  - Function Security Permissions – control access to abstract functions
    - Examples
      - Executable function is access to User Management → Roles & Role Inheritance Form
      - Abstract functions are defined as role permissions
        - Create Role – Assign Role
        - Manage Role – Revoke Role
  - Data Security Permissions – control access to objects
    - Data limited by where clause
  - Tables
    - FND_FORM_FUNCTIONS
    - FND_FORM_FUNCTIONS_TL

User Management Building Blocks

- Permission Sets
  - Grouping of permissions
    - Example: All User Administration Privileges
  - A permission set can contain other permission sets
  - Tables
    - FND_MENUS, FND_MENUS_TL
    - FND_MENU_ENTRIES
    - FND_MENU_ENTRIES_TL

User Management Building Blocks

- Grants
  - Provide permissions for actions on a specified object
    - Attach function permissions and data permissions (data security polices) to grantee
- Grantee
  - Who gets the grant
    - A role or group
    - A specific user
    - All Users
- Table: FND_GRANTS

Stacking Up the Building Blocks

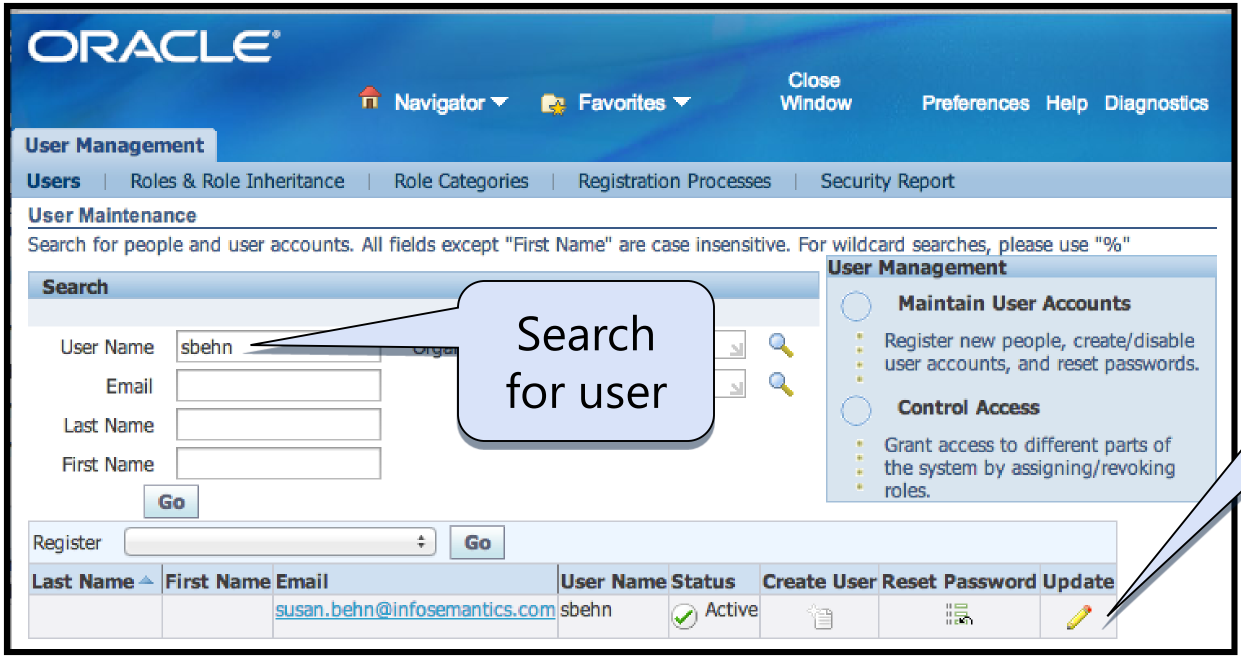
Modeling Security Policies

- Step 1 – Assign access to user management to users
  - Never do tasks signed in as SYSADMIN for audit reasons
- Step 2 – Function security
  - Identify or create permissions/permission sets that group functions
- Step 3 – Data security
  - Identify or create product seeded objects / object instance sets
- Step 4 – Create grants
- Step 5 – Assign role to user or responsibility

Grant Access to User Management to Appropriate User(s)

Managing Users – Step 1

- Out of the box, only Sysadmin has access to User Management
  - Assign a user management role to the appropriate user



User Maintenance

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

Search

User Name	sbehn
Email	
Last Name	
First Name	

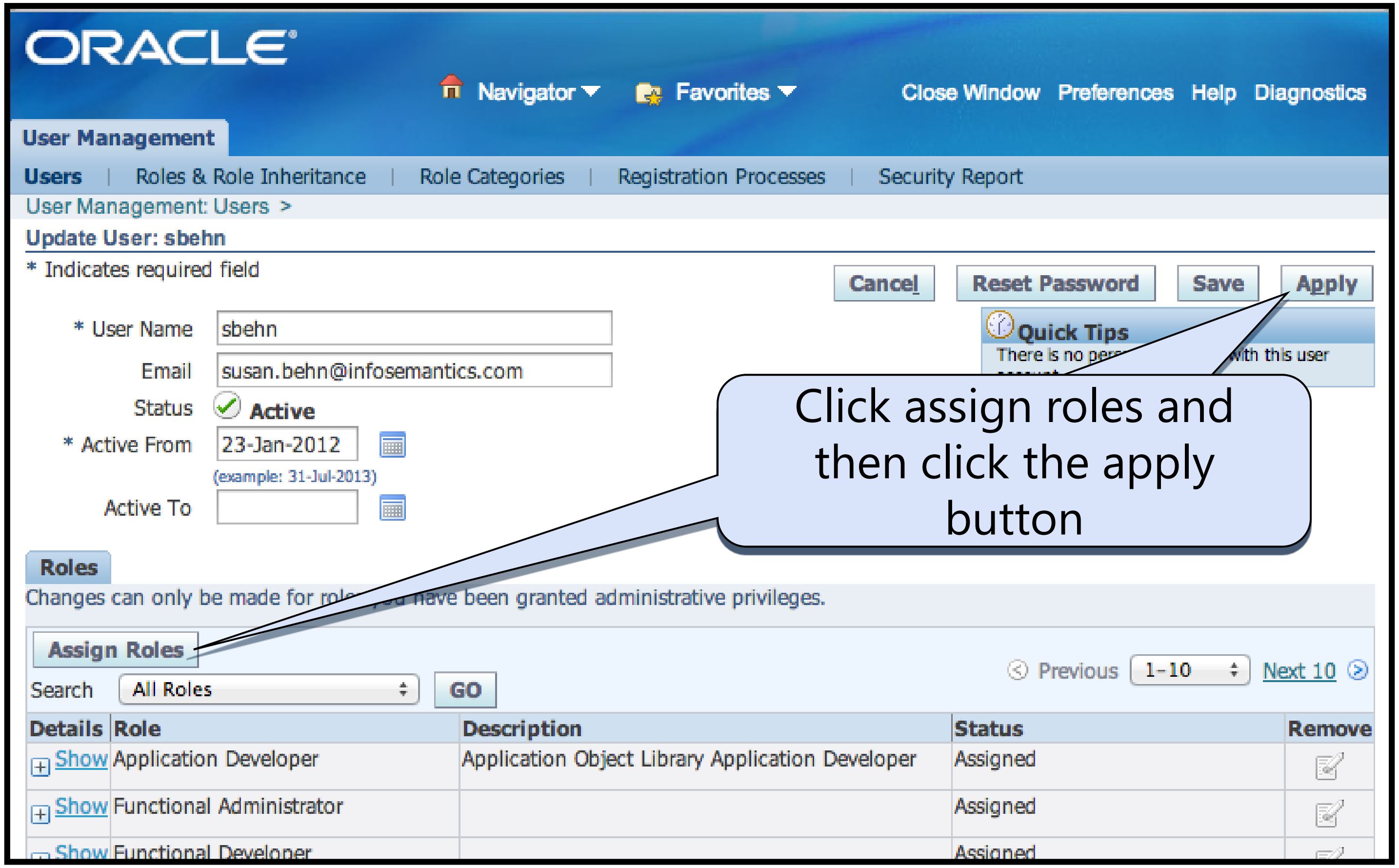
Last Name	First Name	Email	User Name	Status	Create User	Reset Password	Update
		susan.behn@infosemantics.com	sbehn	✓ Active			✎

Search for user

Click pencil to edit

Managing Users – Step 1

- Click the “Assign Roles” button to add a role, then click the apply button (not save)



Update User: sbehn

* Indicates required field

There is no pers... with this user account

* User Name	sbehn
Email	susan.behn@infosemantics.com
Status	✓ Active
* Active From	23-Jan-2012 (example: 31-Jul-2013)
Active To	

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

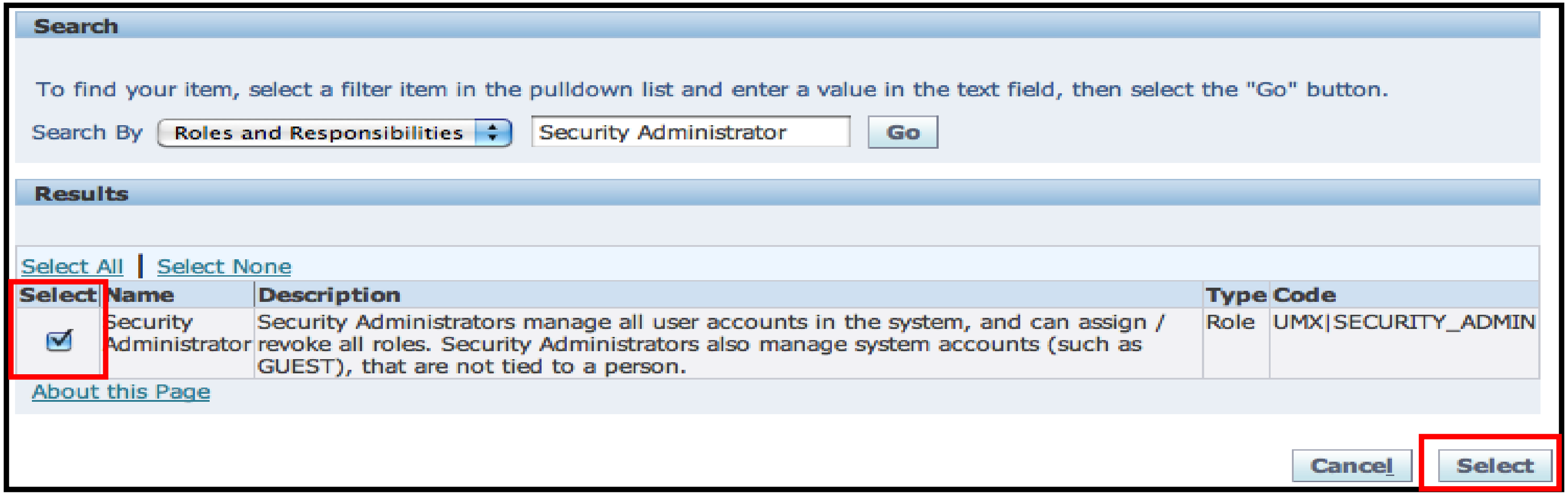
Search: All Roles

Details	Role	Description	Status	Remove
⊞ Show	Application Developer	Application Object Library Application Developer	Assigned	
⊞ Show	Functional Administrator		Assigned	
⊞ Show	Functional Developer		Assigned	

Click assign roles and then click the apply button

Managing Users – Step 1

- Search for the “Security Administrator” Role, check the box and click select
  - Customer Administrator
    - manage users with party type = customer
  - Partner Administrator
    - manage users with party type = partner



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 | Security Administrator | Go

Results

Select All | Select None

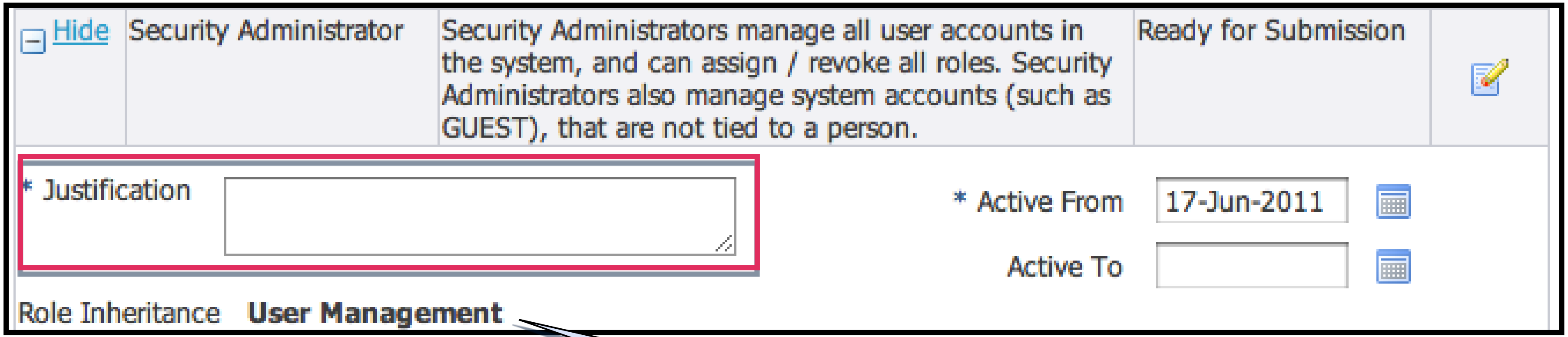
Select	Name	Description	Type	Code
☑	Security Administrator	Security Administrators manage all user accounts in the system, and can assign / revoke all roles. Security Administrators also manage system accounts (such as GUEST), that are not tied to a person.	Role	UMX|SECURITY_ADMIN

About this Page

Cancel Select

Managing Users – Step 1

- Enter a justification and click "Apply"



⊟ Hide	Security Administrator	Security Administrators manage all user accounts in the system, and can assign / revoke all roles. Security Administrators also manage system accounts (such as GUEST), that are not tied to a person.	Ready for Submission	

* Justification

* Active From 17-Jun-2011

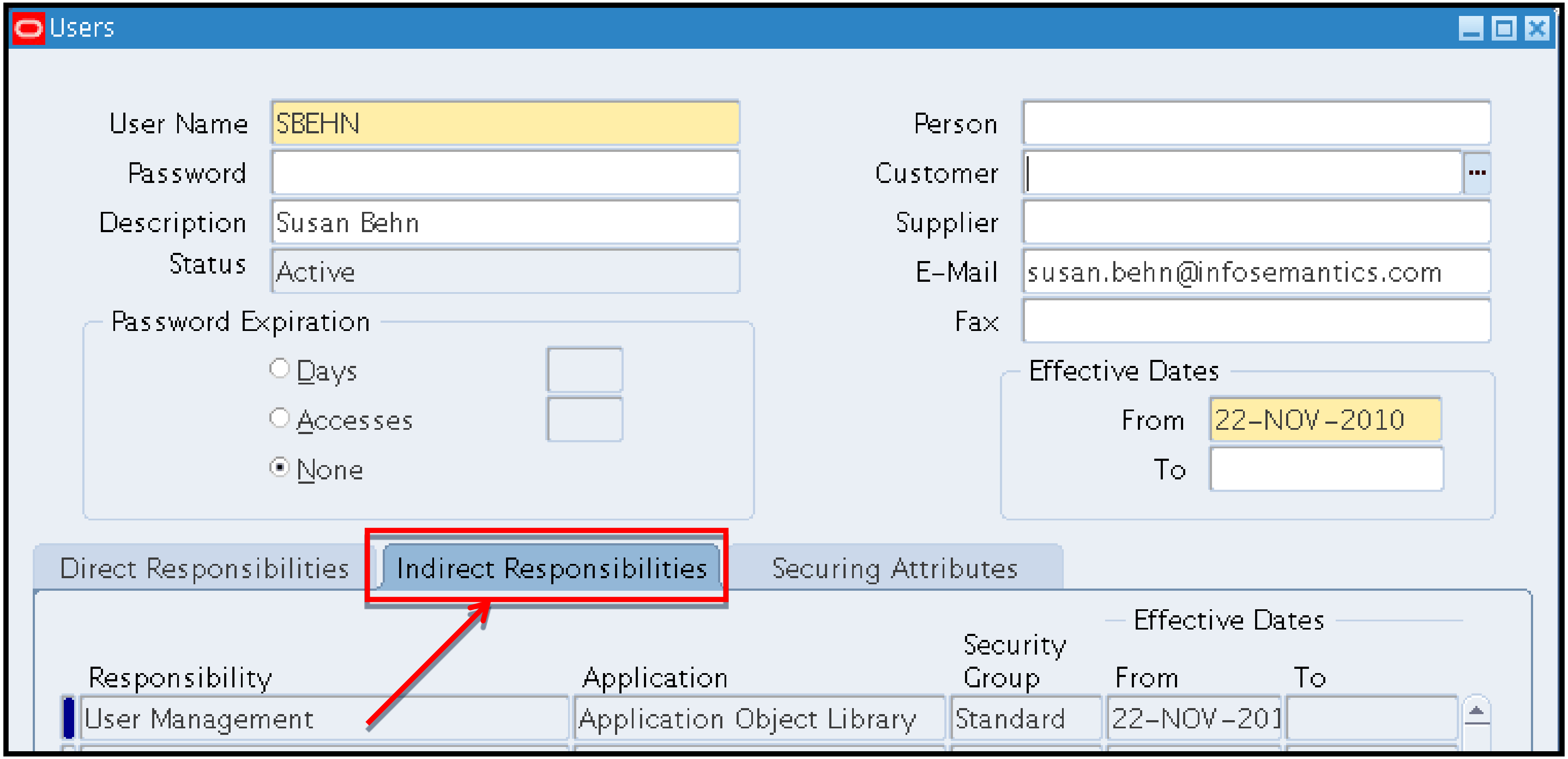
Active To

Role Inheritance **User Management**

User Management responsibility is inherited by assigning this role

Managing Users – Step 1

- System Administrator → User → Define
  - User Management is shown as an indirect responsibility



User Name	SBEHN	Person	
Password		Customer	
Description	Susan Behn	Supplier	
Status	Active	E-Mail	susan.behn@infosemantics.com
		Fax	

Password Expiration

○ Days
○ Accesses
● None

Effective Dates

From 22-NOV-2010
To

Responsibility	Application	Security Group	Effective Dates From	Effective Dates To
User Management	Application Object Library	Standard	22-NOV-201	

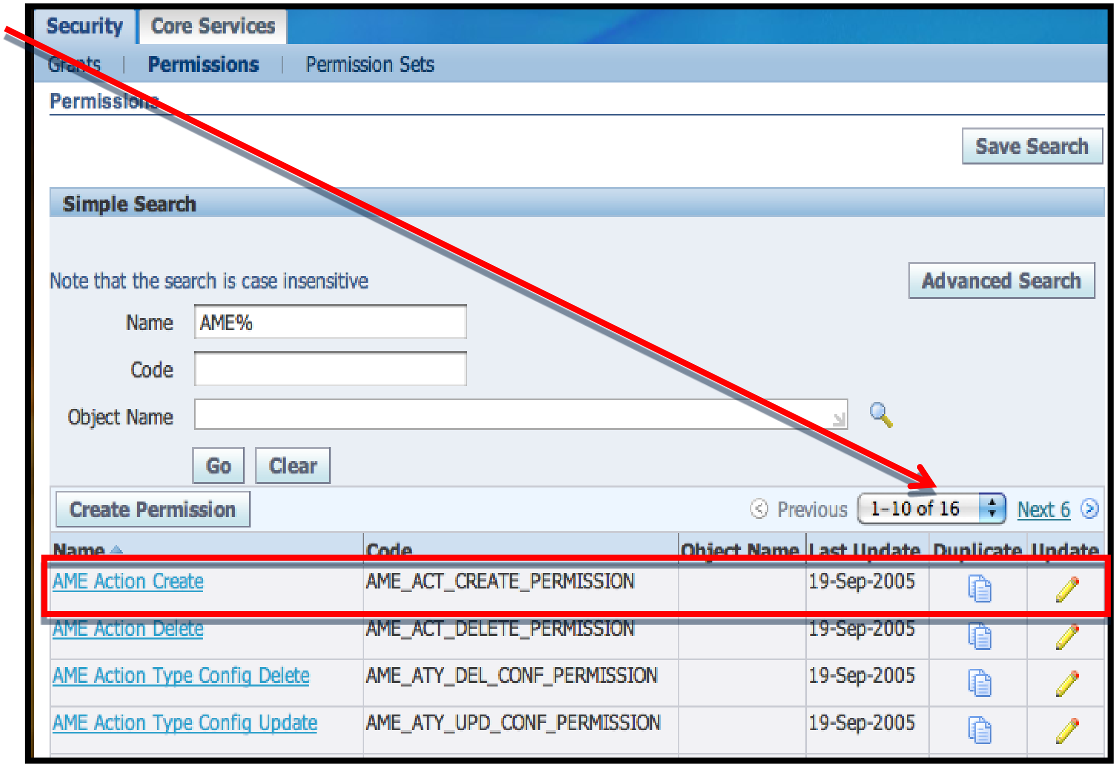
Step 2
Function Security – Identify or Create Permissions/Permission Sets That Group Functions

Permissions

- Function security
  - Approvals Management (AME) will be used as the example
    - AME allows you to approve transactions
    - Transaction types in AME are invoices, requisitions, POs, etc….
- A user will be given access to perform <u>all functions</u> in approvals management
- To gain familiarity with permissions available
  - Go to Functional Administrator → Permissions to search for seeded permissions

Permissions

- There are 16 permissions available for AME



Note that the search is case insensitive

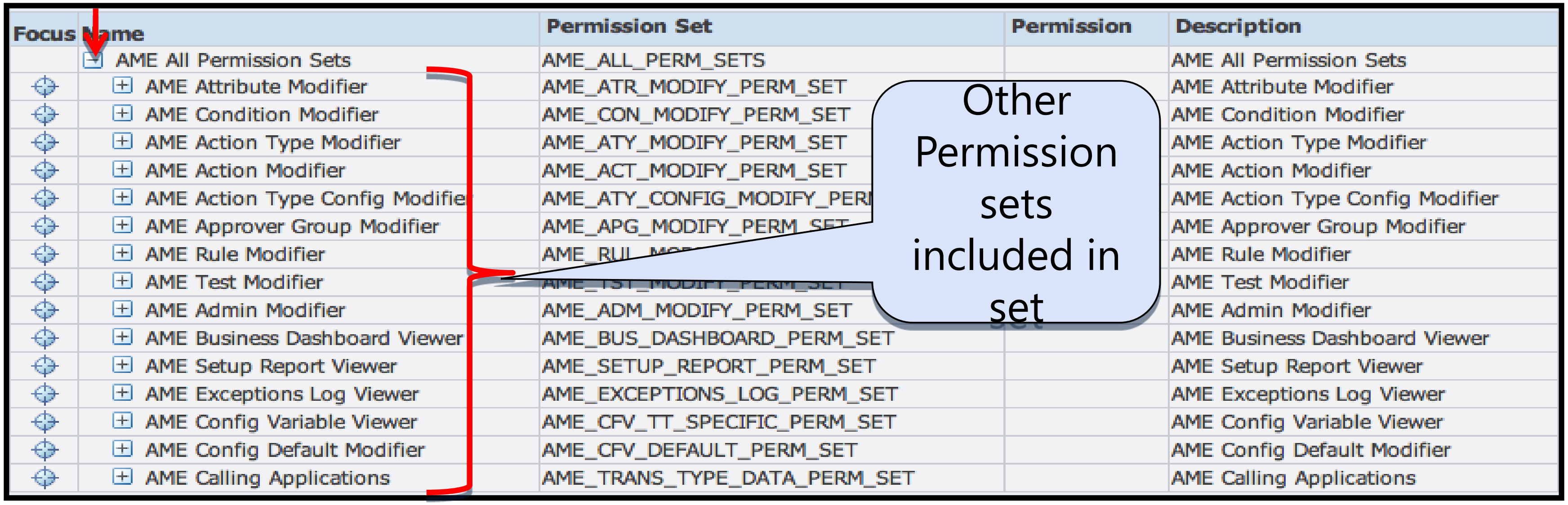
Name	AME%
Code	
Object Name	

1-10 of 16

Name	Code	Object Name	Last Update	Duplicate	Update
AME Action Create	AME_ACT_CREATE_PERMISSION		19-Sep-2005		
AME Action Delete	AME_ACT_DELETE_PERMISSION		19-Sep-2005		
AME Action Type Config Delete	AME_ATY_DEL_CONF_PERMISSION		19-Sep-2005		
AME Action Type Config Update	AME_ATY_UPD_CONF_PERMISSION		19-Sep-2005		

Permission Set

- Our example - given access to perform all functions in AME
- In the permission set tab find the permission sets for AME. You will find “AME All Permission Sets”
  - This permission set includes all the other permission sets which contain all the other permissions



Focus	Name	Permission Set	Permission	Description
	⊟ AME All Permission Sets	AME_ALL_PERM_SETS		AME All Permission Sets
⊕	⊞ AME Attribute Modifier	AME_ATR_MODIFY_PERM_SET		AME Attribute Modifier
⊕	⊞ AME Condition Modifier	AME_CON_MODIFY_PERM_SET		AME Condition Modifier
⊕	⊞ AME Action Type Modifier	AME_ATY_MODIFY_PERM_SET		AME Action Type Modifier
⊕	⊞ AME Action Modifier	AME_ACT_MODIFY_PERM_SET		AME Action Modifier
⊕	⊞ AME Action Type Config Modifie	AME_ATY_CONFIG_MODIFY_PER		AME Action Type Config Modifier
⊕	⊞ AME Approver Group Modifier	AME_APG_MODIFY_PERM_SET		AME Approver Group Modifier
⊕	⊞ AME Rule Modifier	AME_RUL_MO		AME Rule Modifier
⊕	⊞ AME Test Modifier	AME_TST_MODIFY_PERM_SET		AME Test Modifier
⊕	⊞ AME Admin Modifier	AME_ADM_MODIFY_PERM_SET		AME Admin Modifier
⊕	⊞ AME Business Dashboard Viewer	AME_BUS_DASHBOARD_PERM_SET		AME Business Dashboard Viewer
⊕	⊞ AME Setup Report Viewer	AME_SETUP_REPORT_PERM_SET		AME Setup Report Viewer
⊕	⊞ AME Exceptions Log Viewer	AME_EXCEPTIONS_LOG_PERM_SET		AME Exceptions Log Viewer
⊕	⊞ AME Config Variable Viewer	AME_CFV_TT_SPECIFIC_PERM_SET		AME Config Variable Viewer
⊕	⊞ AME Config Default Modifier	AME_CFV_DEFAULT_PERM_SET		AME Config Default Modifier
⊕	⊞ AME Calling Applications	AME_TRANS_TYPE_DATA_PERM_SET		AME Calling Applications

Other Permission sets included in set

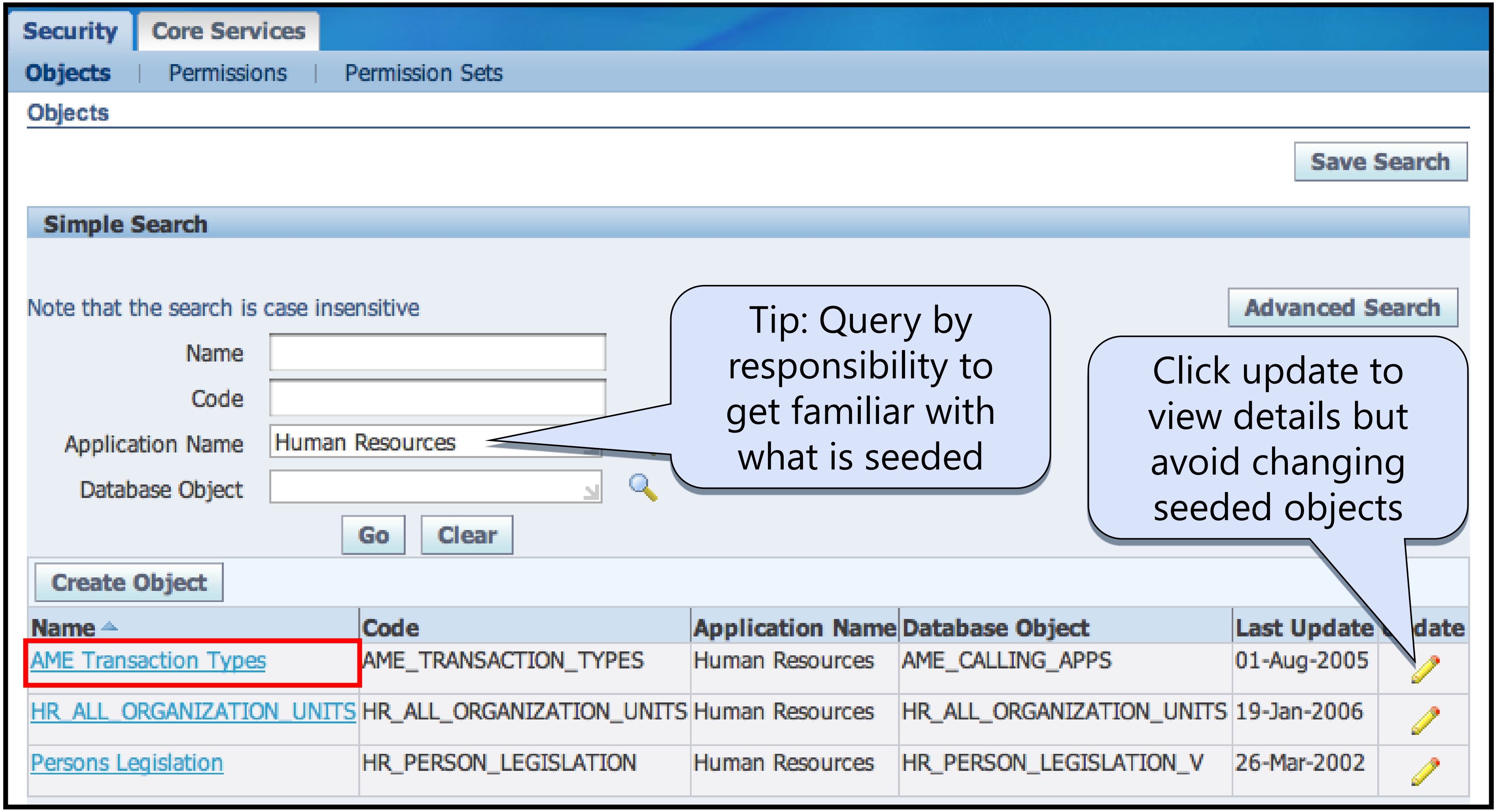
Poll Question

Step 3
Data Security – Identify or Create Product Seeded Objects/Object Instance Sets

Seeded Objects

- To demonstrate data security, Approvals Management will be used again as the example
- A user will be given access to manage the approval process for the payables invoice approval which is a transaction type
- Go to Functional Developer → Objects to search for available seeded objects
- Note that if an object is not available, you can create objects

Seeded Objects



Objects

Simple Search

Note that the search is case insensitive

Name	
Code	
Application Name	Human Resources
Database Object	

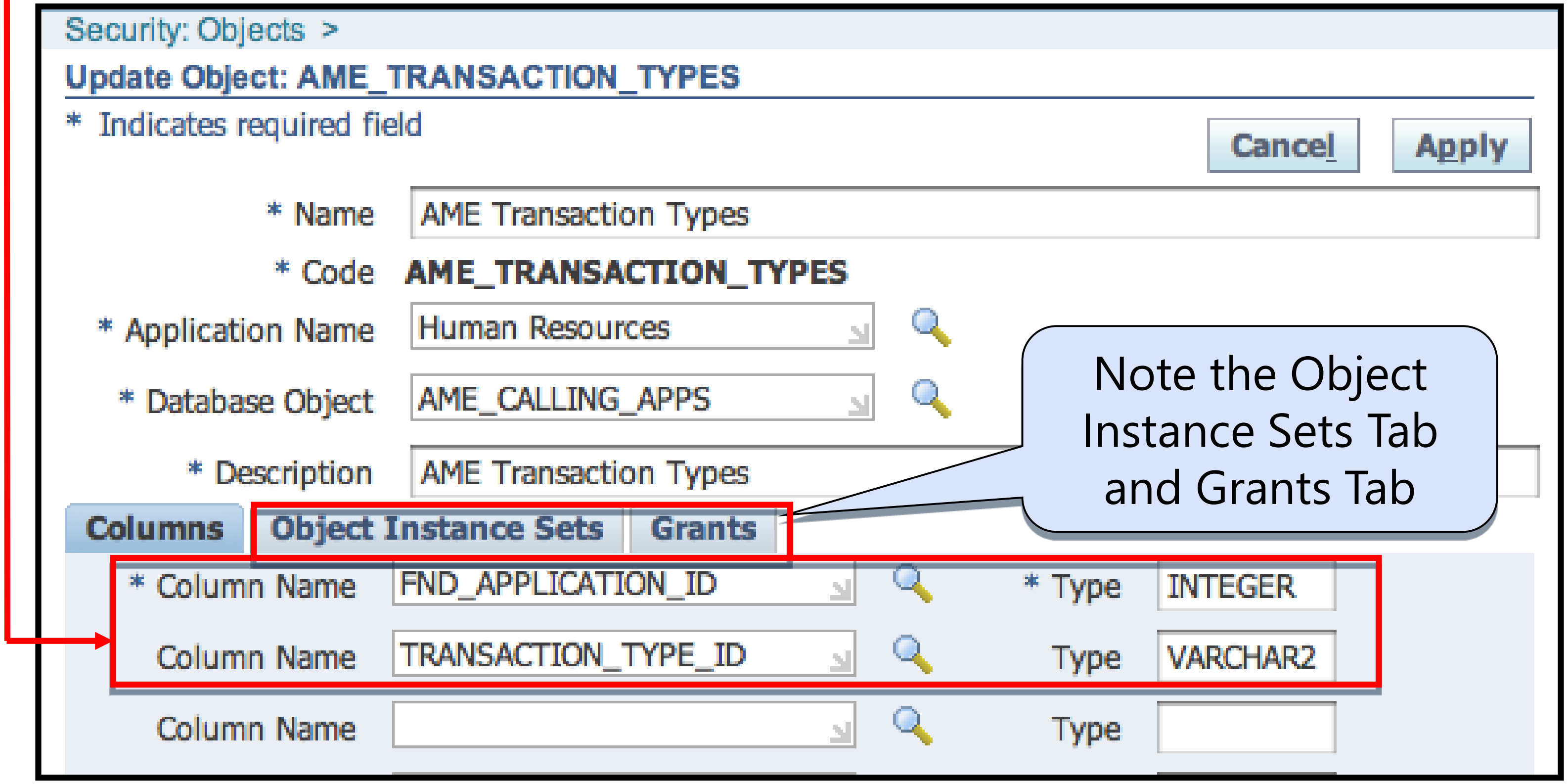
Name	Code	Application Name	Database Object	Last Update	Update
AME Transaction Types	AME_TRANSACTION_TYPES	Human Resources	AME_CALLING_APPS	01-Aug-2005	✎
HR_ALL_ORGANIZATION_UNITS	HR_ALL_ORGANIZATION_UNITS	Human Resources	HR_ALL_ORGANIZATION_UNITS	19-Jan-2006	✎
Persons Legislation	HR_PERSON_LEGISLATION	Human Resources	HR_PERSON_LEGISLATION_V	26-Mar-2002	✎

Tip: Query by responsibility to get familiar with what is seeded

Click update to view details but avoid changing seeded objects

Seeded Objects

- Two columns are included to limit access
  - Application ID
  - Transaction Type ID



Security: Objects >

Update Object: AME_TRANSACTION_TYPES

* Indicates required field

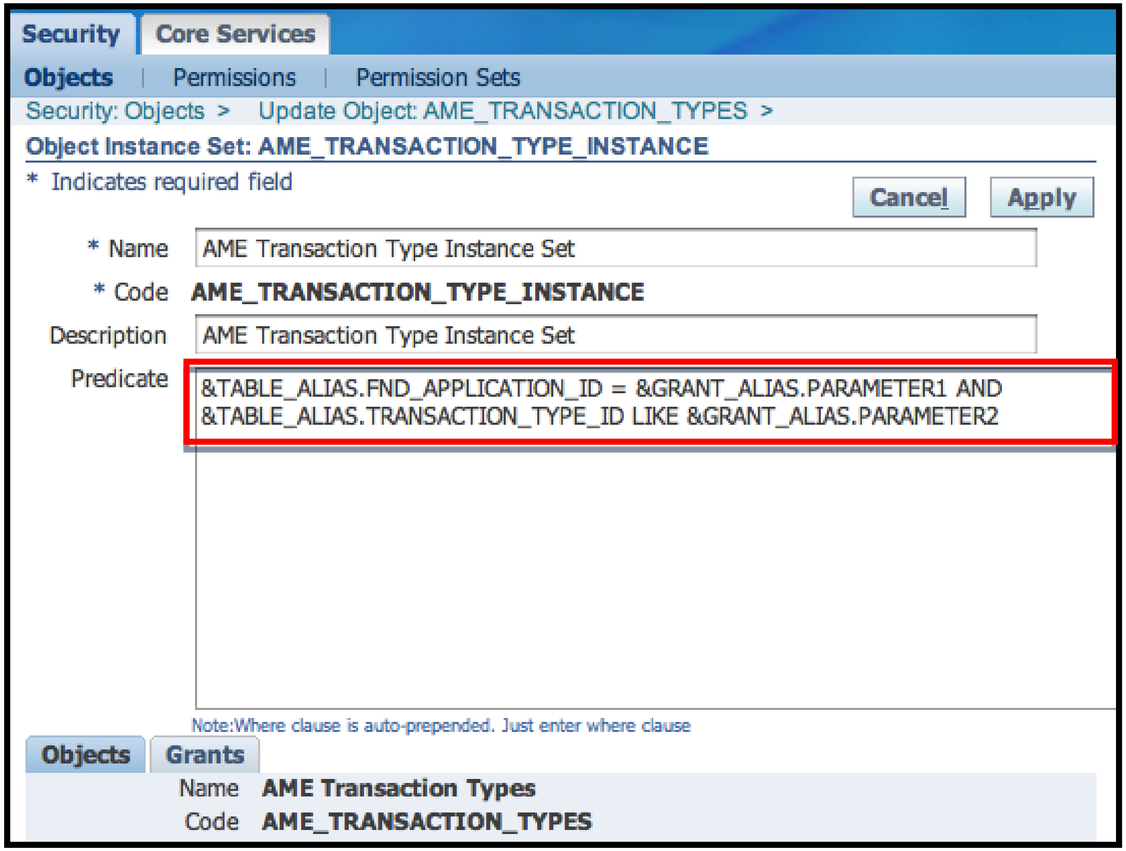
* Name	AME Transaction Types
* Code	AME_TRANSACTION_TYPES
* Application Name	Human Resources
* Database Object	AME_CALLING_APPS
* Description	AME Transaction Types

* Column Name	FND_APPLICATION_ID	* Type	INTEGER
Column Name	TRANSACTION_TYPE_ID	Type	VARCHAR2
Column Name		Type	

Note the Object Instance Sets Tab and Grants Tab

Seeded Objects

- Click on the Object Instance Set tab for this object to view the where clause
  - The predicate allows the user to view/enter the parameters to select the application and transaction type in the grant


Security
Core Services
Objects | Permissions | Permission Sets
Security: Objects > Update Object: AME_TRANSACTION_TYPES >

Object Instance Set: AME_TRANSACTION_TYPE_INSTANCE

* Indicates required field

* Name: AME Transaction Type Instance Set
* Code: AME_TRANSACTION_TYPE_INSTANCE

Description: AME Transaction Type Instance Set

Predicate:
```
&TABLE_ALIAS.FND_APPLICATION_ID = &GRANT_ALIAS.PARAMETER1 AND
&TABLE_ALIAS.TRANSACTION_TYPE_ID LIKE &GRANT_ALIAS.PARAMETER2
```

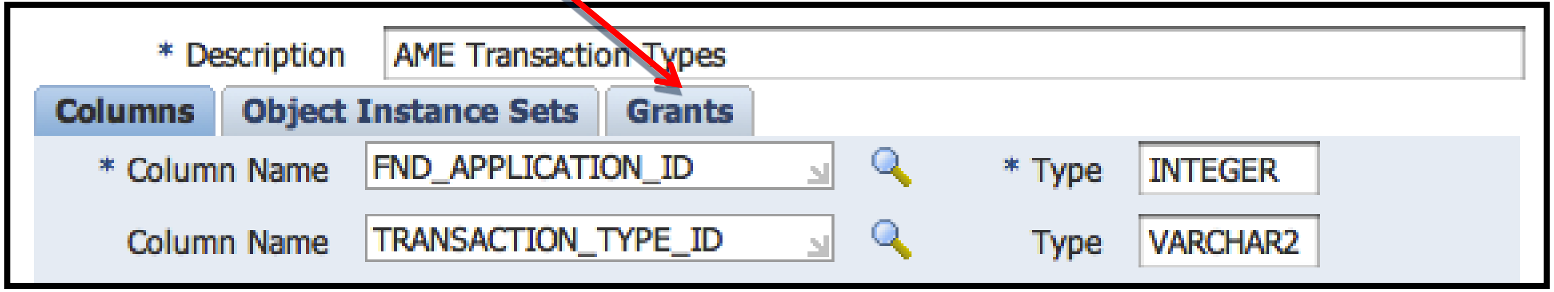
Note:Where clause is auto-prepended. Just enter where clause

Name: AME Transaction Types
Code: AME_TRANSACTION_TYPES

Step 4
Create Grants

Grants

- Create the grant to allow sbehn to perform all AME functions for the payables invoice approval transaction type
- Click on grants tab

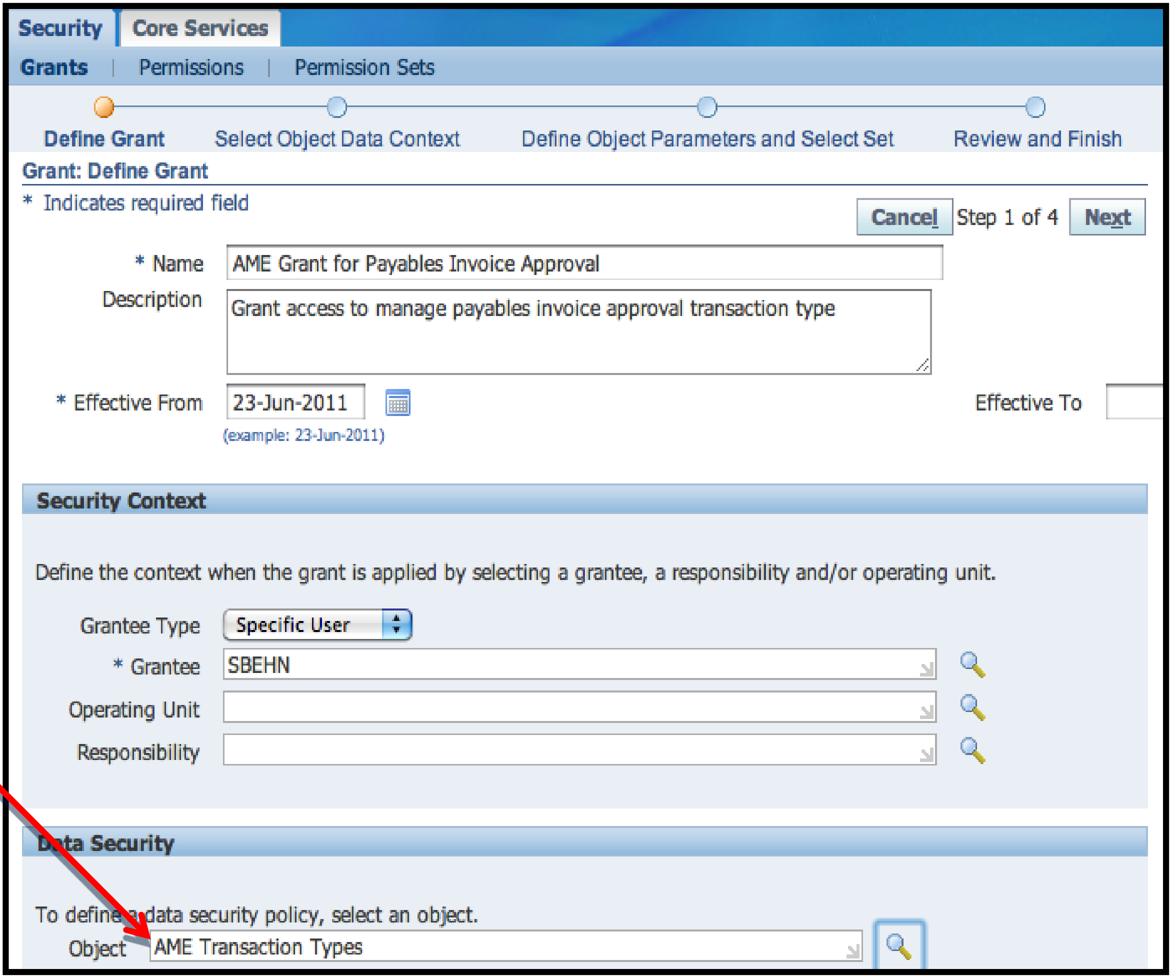


* Description	AME Transaction Types		
* Column Name	FND_APPLICATION_ID	* Type	INTEGER
Column Name	TRANSACTION_TYPE_ID	Type	VARCHAR2

  - Notice this takes you to the same form as you see in the Functional Administrator responsibility
  - We are going to enter an object to establish a Data Security Policy

Grants

- Enter name, description, grantee type, grantee
- Enter the object name
- Click Next



Grant: Define Grant

* Indicates required field

Step 1 of 4

* Name	AME Grant for Payables Invoice Approval
Description	Grant access to manage payables invoice approval transaction type
* Effective From	23-Jun-2011 (example: 23-Jun-2011)
Effective To	

Security Context

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

Grantee Type	Specific User
* Grantee	SBEHN
Operating Unit	
Responsibility	

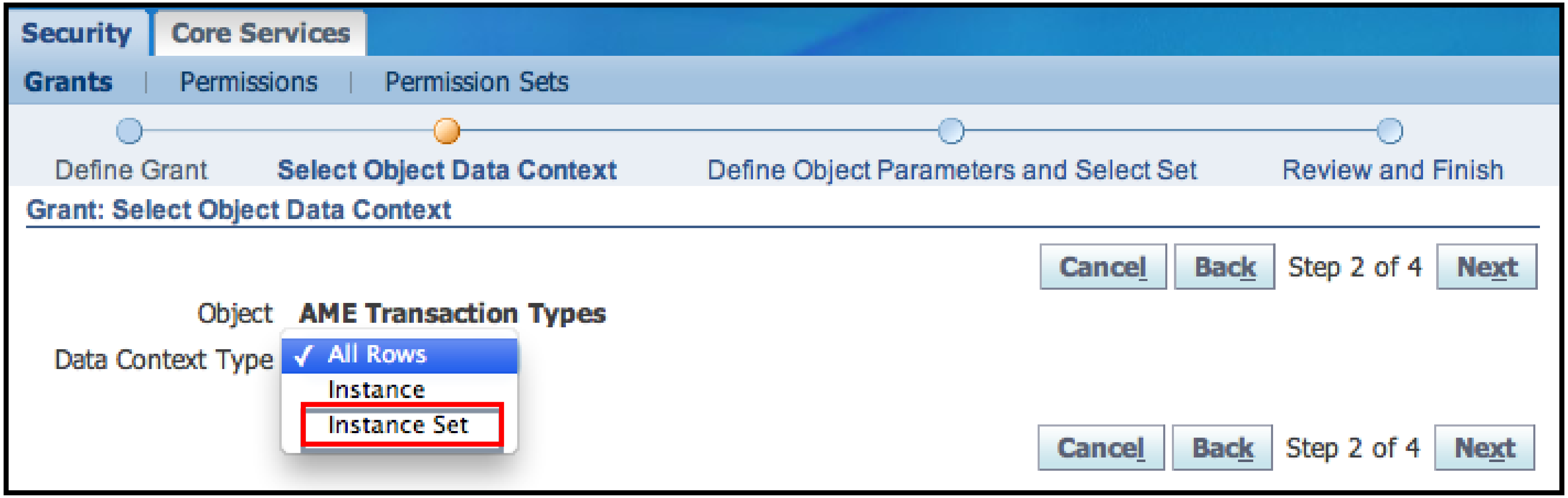
Data Security

To define a data security policy, select an object.

Object	AME Transaction Types

Grants

- Choose the context to limit rows
  - For this example, choose instance set



Security
Core Services
Grants | Permissions | Permission Sets
Define Grant
Select Object Data Context
Define Object Parameters and Select Set
Review and Finish
Cancel
Back
Step 2 of 4
Next
All Rows
Instance
Instance Set

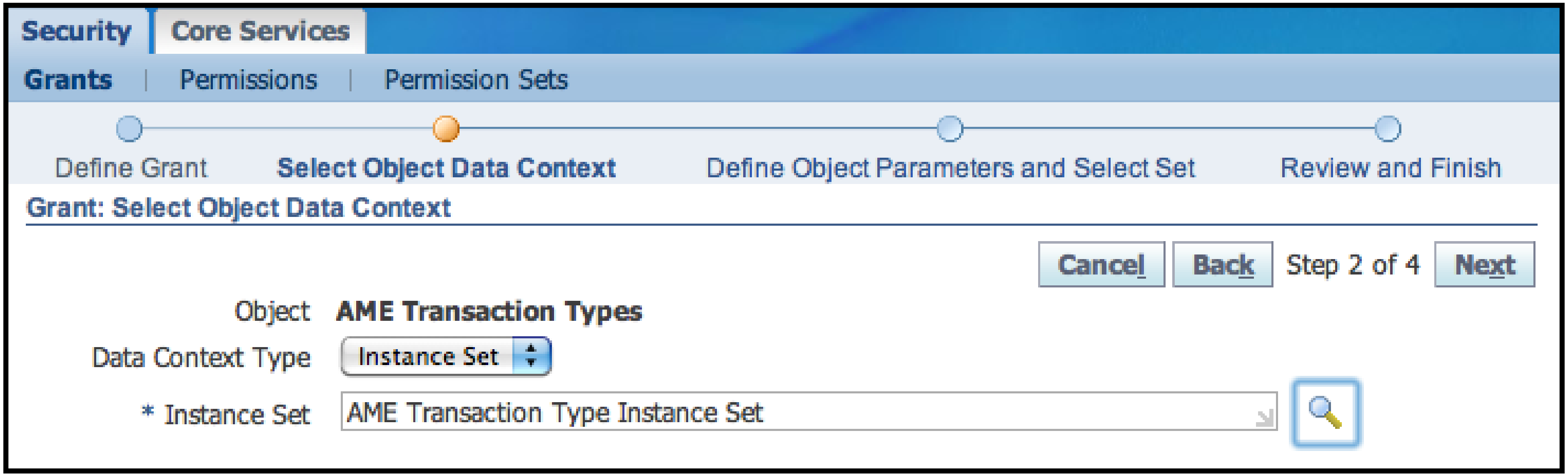
Grant: Select Object Data Context

Object AME Transaction Types

Data Context Type ✓ All Rows

Grants

- We already determined there was an "AME Transaction Type" Instance Set
- Chose this value and Click Next

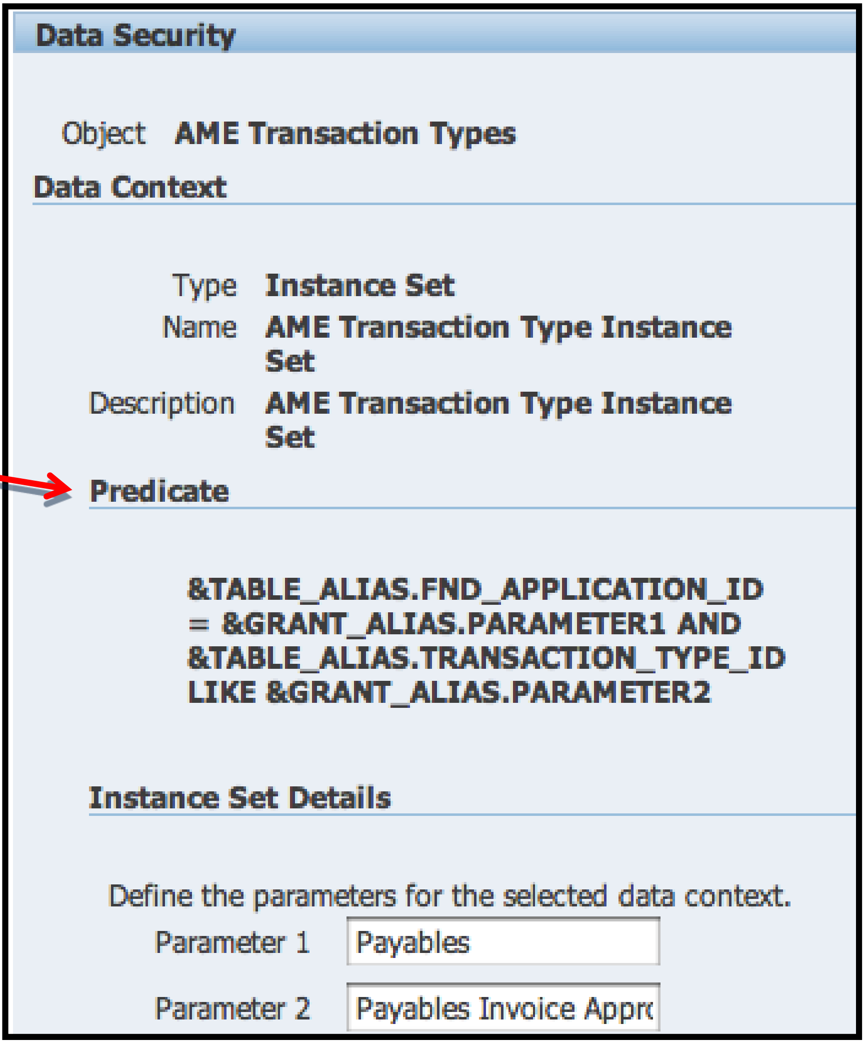

Security
Core Services
Grants | Permissions | Permission Sets
Define Grant
Select Object Data Context
Define Object Parameters and Select Set
Review and Finish
Cancel
Back
Step 2 of 4
Next

Grant: Select Object Data Context

Object	AME Transaction Types
Data Context Type	Instance Set
* Instance Set	AME Transaction Type Instance Set

Grants

- Scroll down the page and enter the values for the parameters we saw earlier in the object instance set
  - The predicate is displayed for reference
    - Parameter 1 is the application (Payables)
    - Parameter 2 is the AME transaction type (Payables Invoice Approval)



Data Security

Object **AME Transaction Types**

Data Context

Type	**Instance Set**
Name	**AME Transaction Type Instance Set**
Description	**AME Transaction Type Instance Set**

Predicate

&TABLE_ALIAS.FND_APPLICATION_ID = &GRANT_ALIAS.PARAMETER1 AND &TABLE_ALIAS.TRANSACTION_TYPE_ID LIKE &GRANT_ALIAS.PARAMETER2

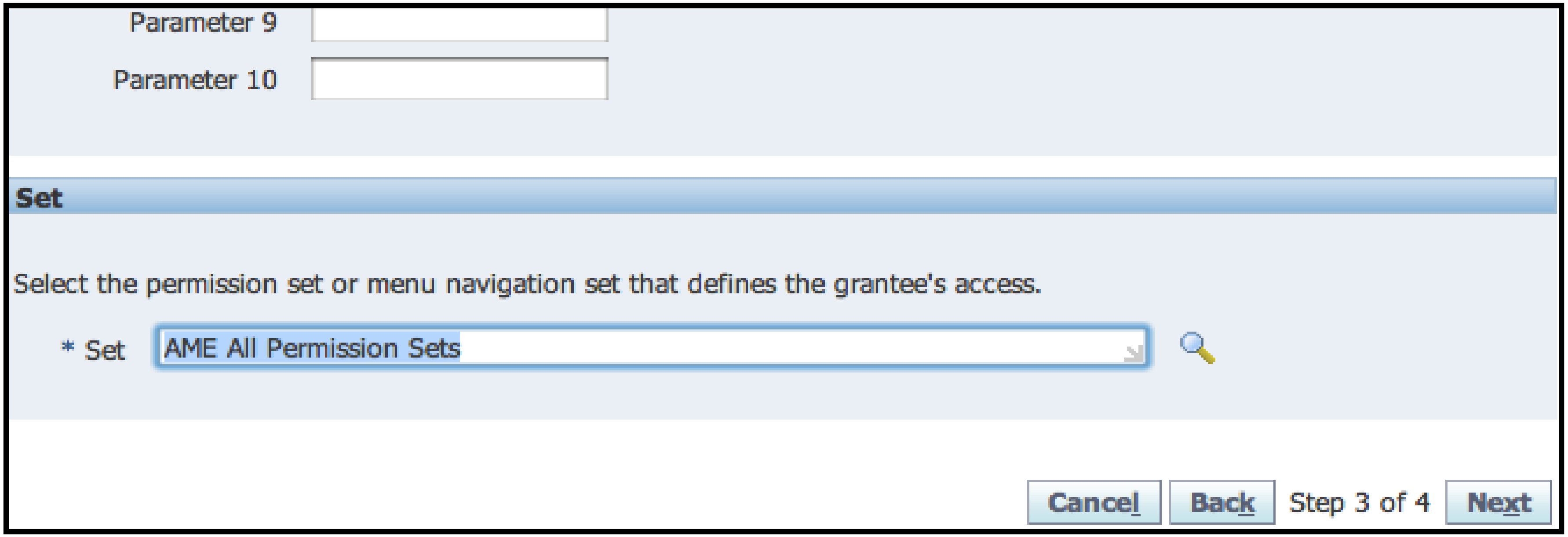
Instance Set Details

Define the parameters for the selected data context.

Parameter 1	Payables
Parameter 2	Payables Invoice Appr(

Grants

- Scroll down and choose the functions the grantee will be allowed to execute for this group of data by selecting the permission set "AME All Permission Sets"



Parameter 9

Parameter 10

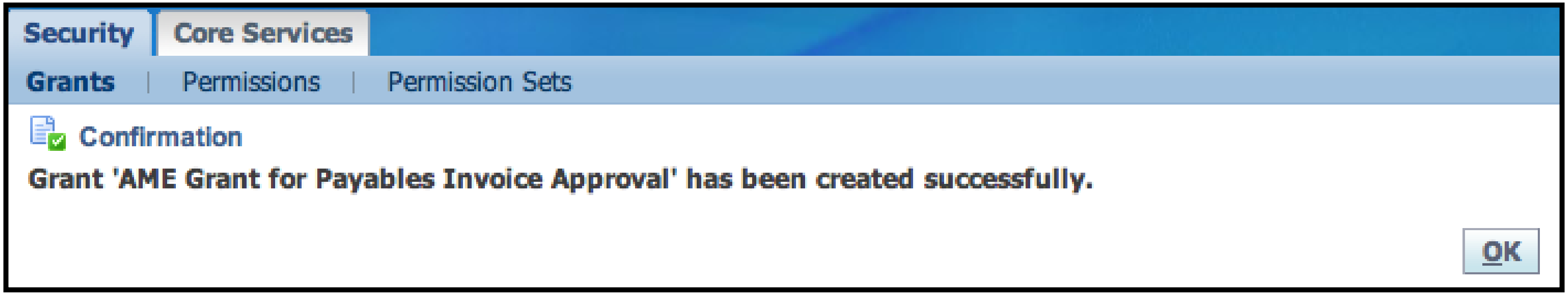
Set

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

* Set: AME All Permission Sets

Grants

- The final page is a review page
- Click finish and the confirmation page will appear
- Now you have access to data and functions you can perform on that data
- Click OK



Confirmation

Grant 'AME Grant for Payables Invoice Approval' has been created successfully.

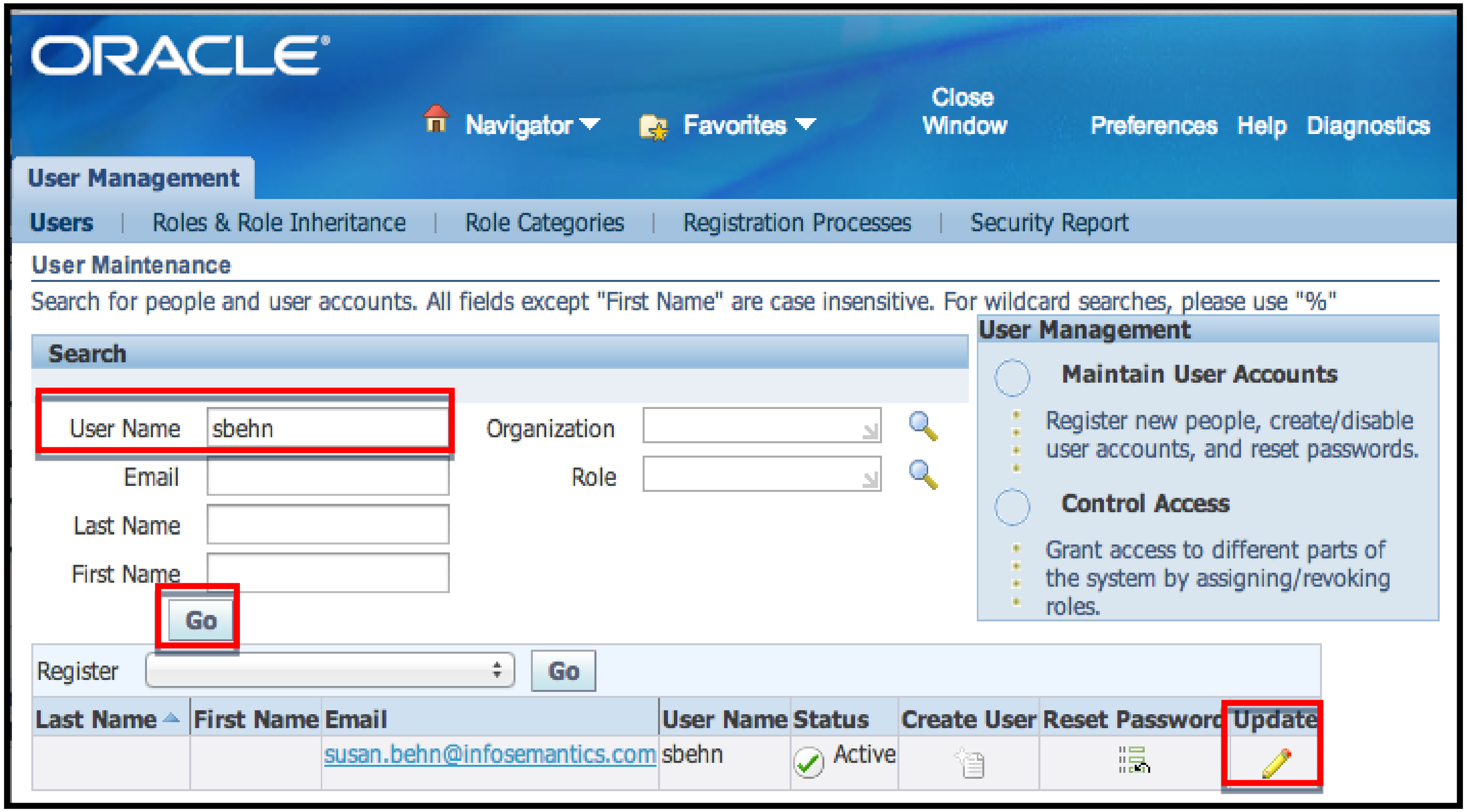
Role Based Access Control – Let's review

- Step 1 – Access to user management
  - We gave sbehn access to user management by assigning the Security Administrator role
- Step 2 - Function security
  - We found the "AME All Permission Sets"
- Step 3 – Data Security
  - We found the "AME Transaction Types" object
- Step 4 – Grants
  - We joined the function and data security together in a grant to allow SBEHN to perform all functions for AME for Payables Invoice Approvals
- But…the user still doesn't have access yet to the responsibility used to manage AME
  - Now the user needs a role to provide the indirect responsibility

Step 5
Assign Roles

Assign Roles

- Assign AME roles to SBEHN the same way we assigned the “Security Administrator” role
- Query the user, click Go, then click the pencil



User Maintenance

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

Search

User Name: sbehn

Email:

Last Name:

First Name:

Organization:

Role:

Go

User Management

Maintain User Accounts

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

Control Access

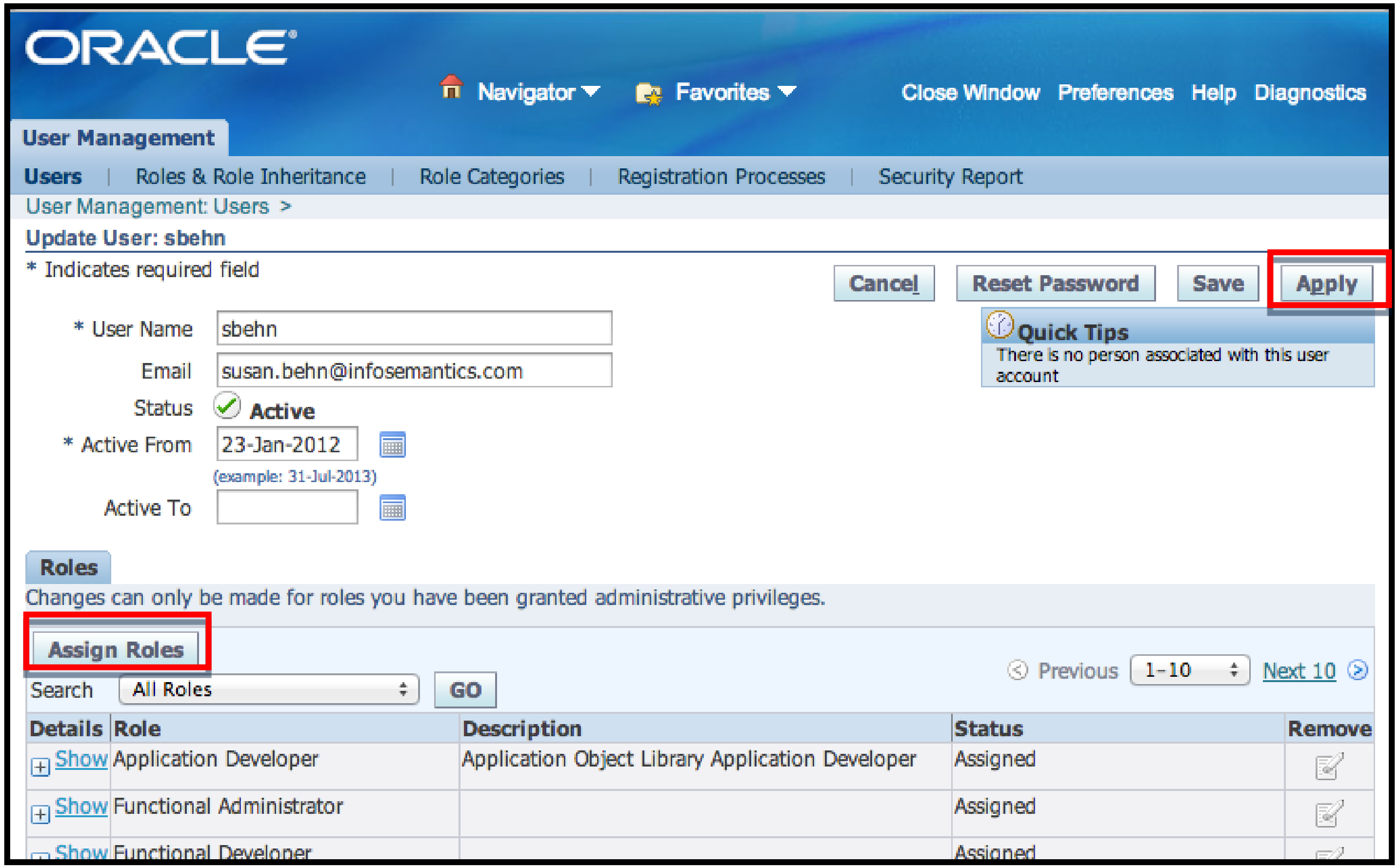
Grant access to different parts of the system by assigning/revoking roles.

Register: Go

Last Name	First Name	Email	User Name	Status	Create User	Reset Password	Update
		susan.behn@infosemantics.com	sbehn	✓ Active			✎

Assign Roles

- Click the “Assign Roles” button, then click Apply (not save)



Update User: sbehn

* Indicates required field

Quick Tips
There is no person associated with this user account

* User Name	sbehn
Email	susan.behn@infosemantics.com
Status	✓ Active
* Active From	23-Jan-2012 (example: 31-Jul-2013)
Active To	

Roles

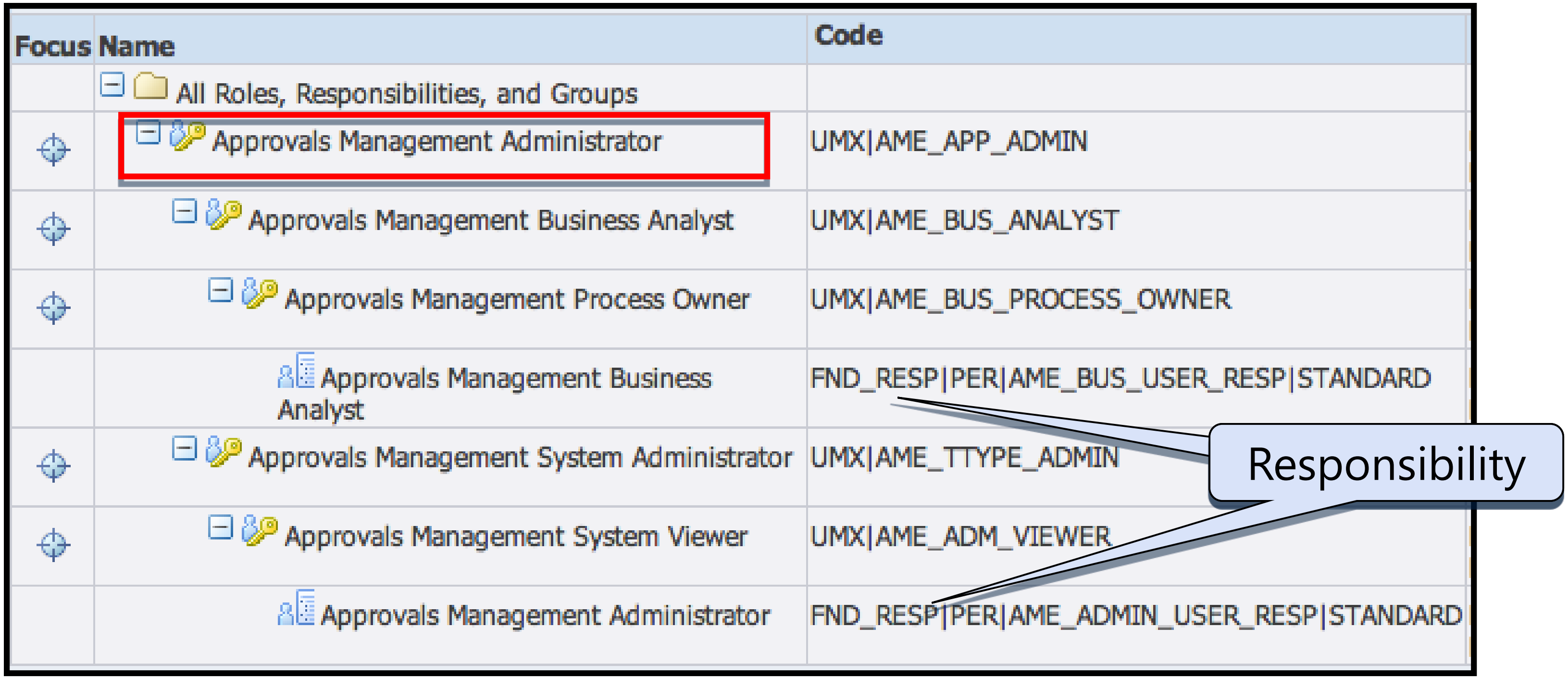
Changes can only be made for roles you have been granted administrative privileges.

Search All Roles

Details	Role	Description	Status	Remove
⊞ Show	Application Developer	Application Object Library Application Developer	Assigned	
⊞ Show	Functional Administrator		Assigned	
⊞ Show	Functional Developer		Assigned	

Seeded Roles

- Find the “Approvals Management Administrator” role and provide justification
  - Grants multiple roles shown in the hierarchy below and two responsibilities having a code starting with “FND_RESP”



Focus	Name	Code
	All Roles, Responsibilities, and Groups	
⌖	Approvals Management Administrator	UMX|AME_APP_ADMIN
⌖	Approvals Management Business Analyst	UMX|AME_BUS_ANALYST
⌖	Approvals Management Process Owner	UMX|AME_BUS_PROCESS_OWNER
	Approvals Management Business Analyst	FND_RESP|PER|AME_BUS_USER_RESP|STANDARD
⌖	Approvals Management System Administrator	UMX|AME_TTYPE_ADMIN
⌖	Approvals Management System Viewer	UMX|AME_ADM_VIEWER
	Approvals Management Administrator	FND_RESP|PER|AME_ADMIN_USER_RESP|STANDARD

Responsibility

Seeded Roles

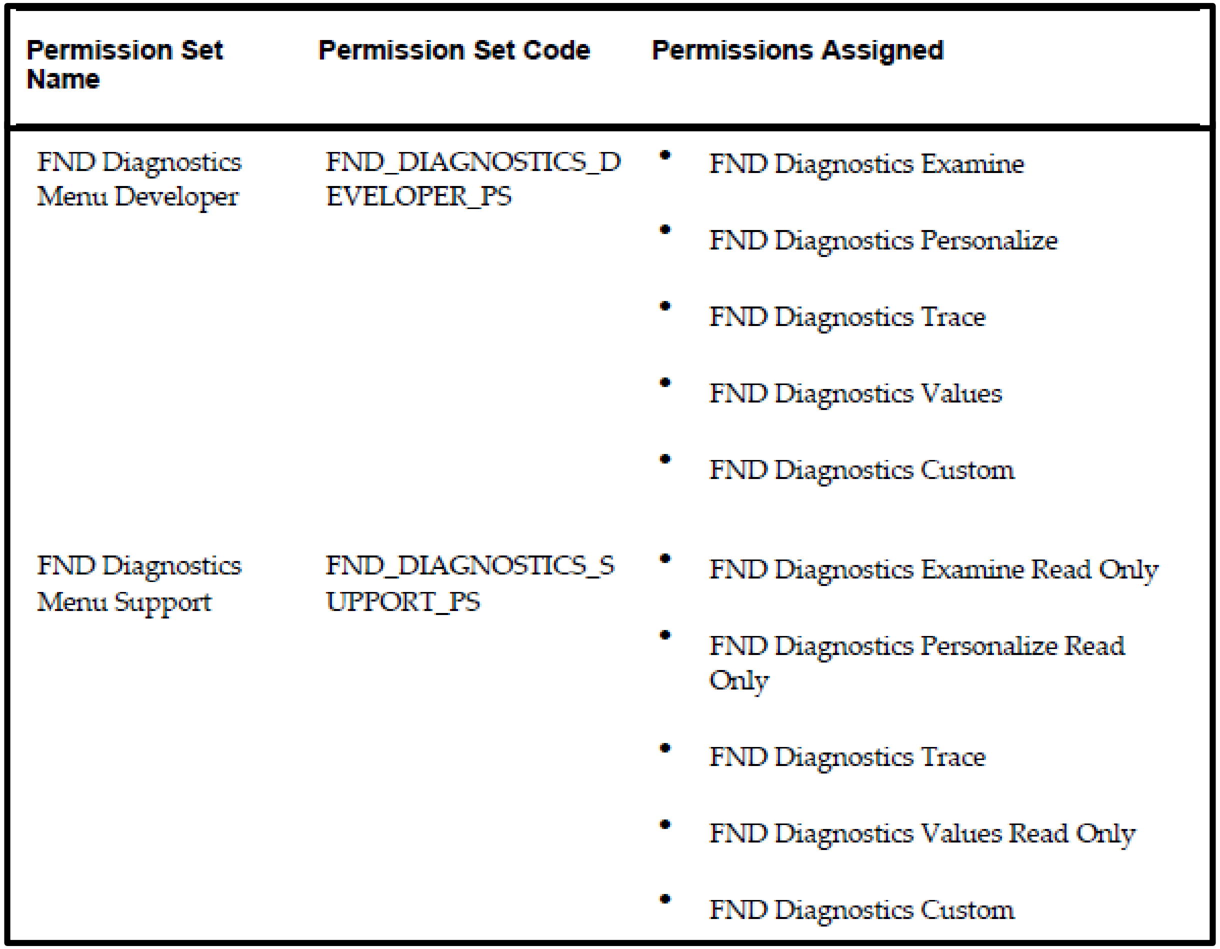
- Below is a partial list of products with seeded roles; This changes frequently
  - Approvals Management
  - Diagnostics
  - Learning Management
  - Territory Management
  - User Management
  - Integration Repository
  - iReceivables
  - iSetup
  - Integrated SOA Gateway (New)
  - Manage Proxies
  - Mobile Application Management
- To see what’s new after patches, look for roles in User Management responsibility or query WF_ALL_ROLES_VL

R12 Examples

Help → Examine (Update and Read-only)

Diagnostics in 12.1 via grants/roles

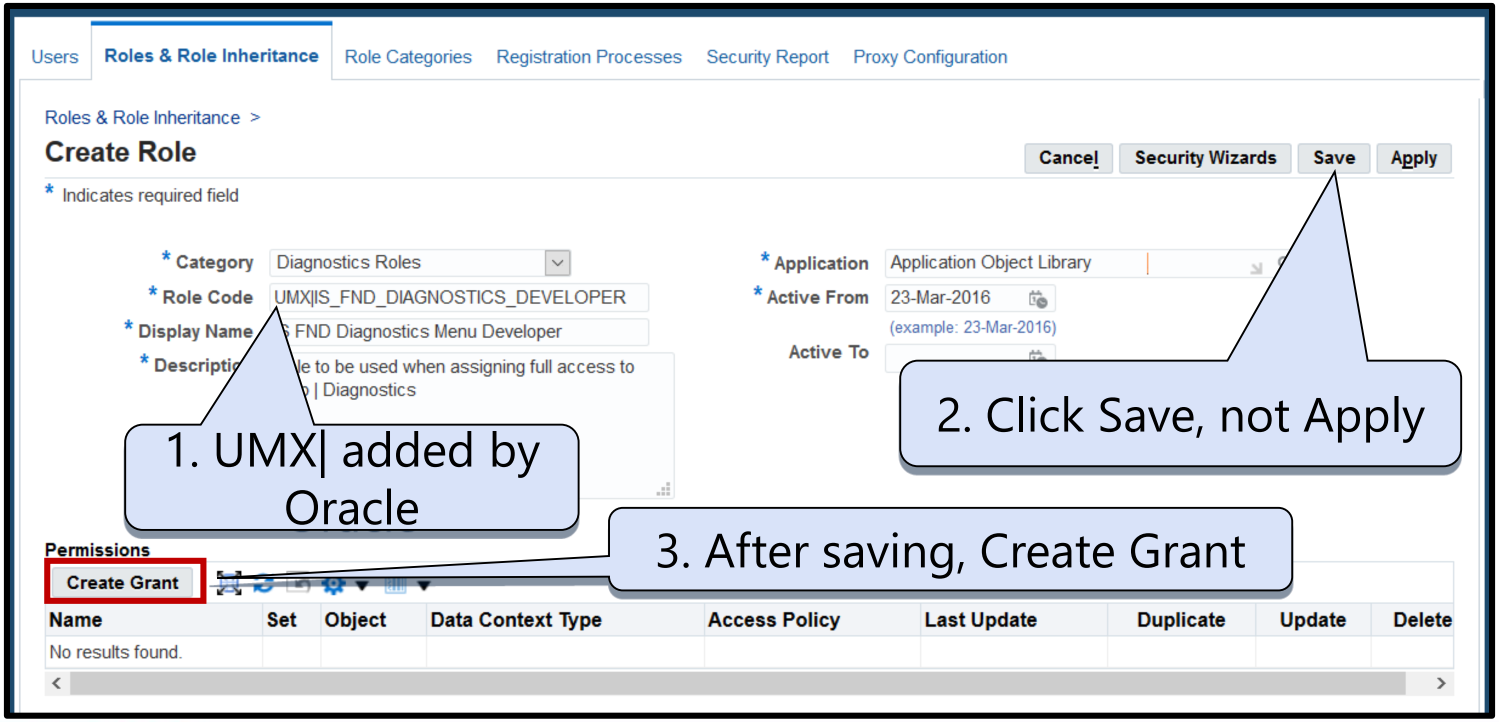
- Sample Seeded Permission Sets



Permission Set Name	Permission Set Code	Permissions Assigned
FND Diagnostics Menu Developer	FND_DIAGNOSTICS_DEVELOPER_PS	• FND Diagnostics Examine • FND Diagnostics Personalize • FND Diagnostics Trace • FND Diagnostics Values • FND Diagnostics Custom
FND Diagnostics Menu Support	FND_DIAGNOSTICS_SUPPORT_PS	• FND Diagnostics Examine Read Only • FND Diagnostics Personalize Read Only • FND Diagnostics Trace • FND Diagnostics Values Read Only • FND Diagnostics Custom

Read-Only Diagnostics in 12.1 via grants/roles

- Create Role
  - Role Code = FND_DIAGNOSTICS_DEVELOPER
    - After saving, "UMX|" will be added to code
- Click "Save, then the "Create Grant" button



* Indicates required field

* Category: Diagnostics Roles
* Role Code: UMX|IS_FND_DIAGNOSTICS_DEVELOPER
* Display Name: S FND Diagnostics Menu Developer
* Descripti...: ...le to be used when assigning full access to ...o | Diagnostics
* Application: Application Object Library
* Active From: 23-Mar-2016 (example: 23-Mar-2016)
Active To:

Name	Set	Object	Data Context Type	Access Policy	Last Update	Duplicate	Update	Delete
No results found.								

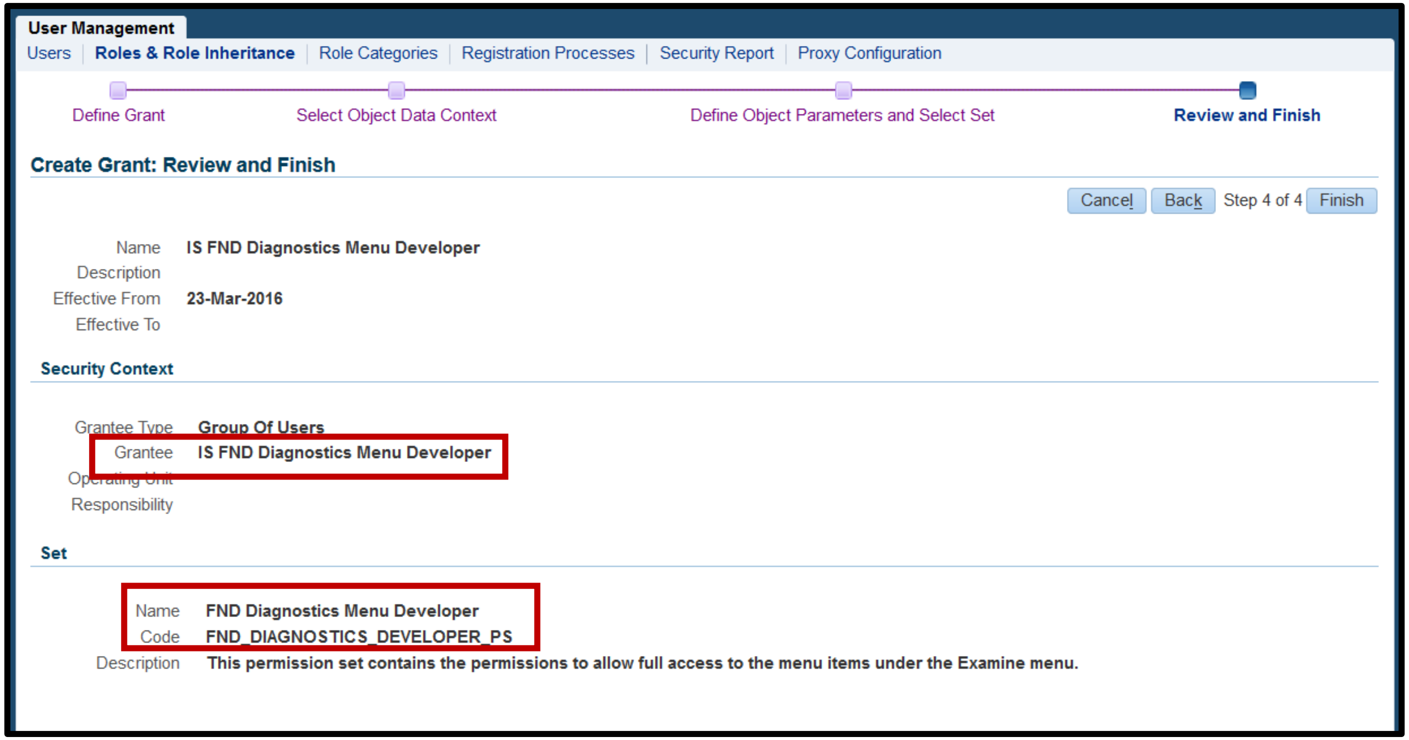
1. UMX| added by Oracle

2. Click Save, not Apply

3. After saving, Create Grant

Read-Only Diagnostics in 12.1 via grants/roles

- Create the Grant
  - The Grantee is the Role just created
  - Select Permission Set from list in slide 46


User Management
Users | Roles & Role Inheritance | Role Categories | Registration Processes | Security Report | Proxy Configuration
Define Grant
Select Object Data Context
Define Object Parameters and Select Set
Review and Finish
Cancel
Back
Step 4 of 4
Finish

Create Grant: Review and Finish

Name IS FND Diagnostics Menu Developer
Description
Effective From 23-Mar-2016
Effective To

Security Context

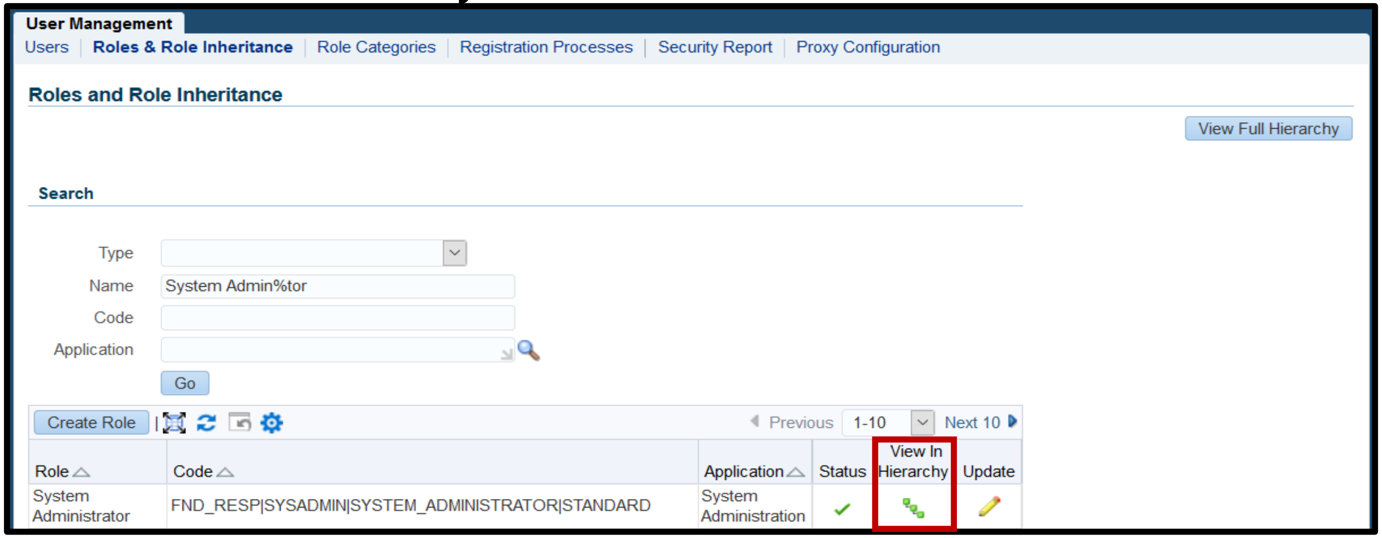
Grantee Type Group Of Users
Grantee IS FND Diagnostics Menu Developer
Operating Unit
Responsibility

Set

Name FND Diagnostics Menu Developer
Code FND_DIAGNOSTICS_DEVELOPER_PS
Description This permission set contains the permissions to allow full access to the menu items under the Examine menu.

Read-Only Diagnostics in 12.1 via grants/roles

- Add new Role to desired Responsibility hierarchy
- This example will give the System Administrator responsibility access to diagnostics
- Click "View in Hierarchy", then the + to add a role



User Management

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

Roles and Role Inheritance

View Full Hierarchy

Search

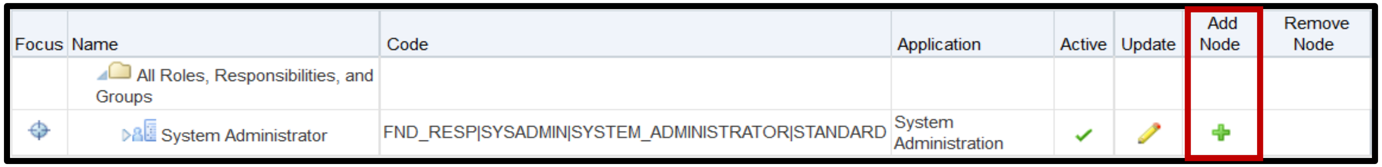
Type	
Name	System Admin%tor
Code	
Application	

Go

Create Role

Previous 1-10 Next 10

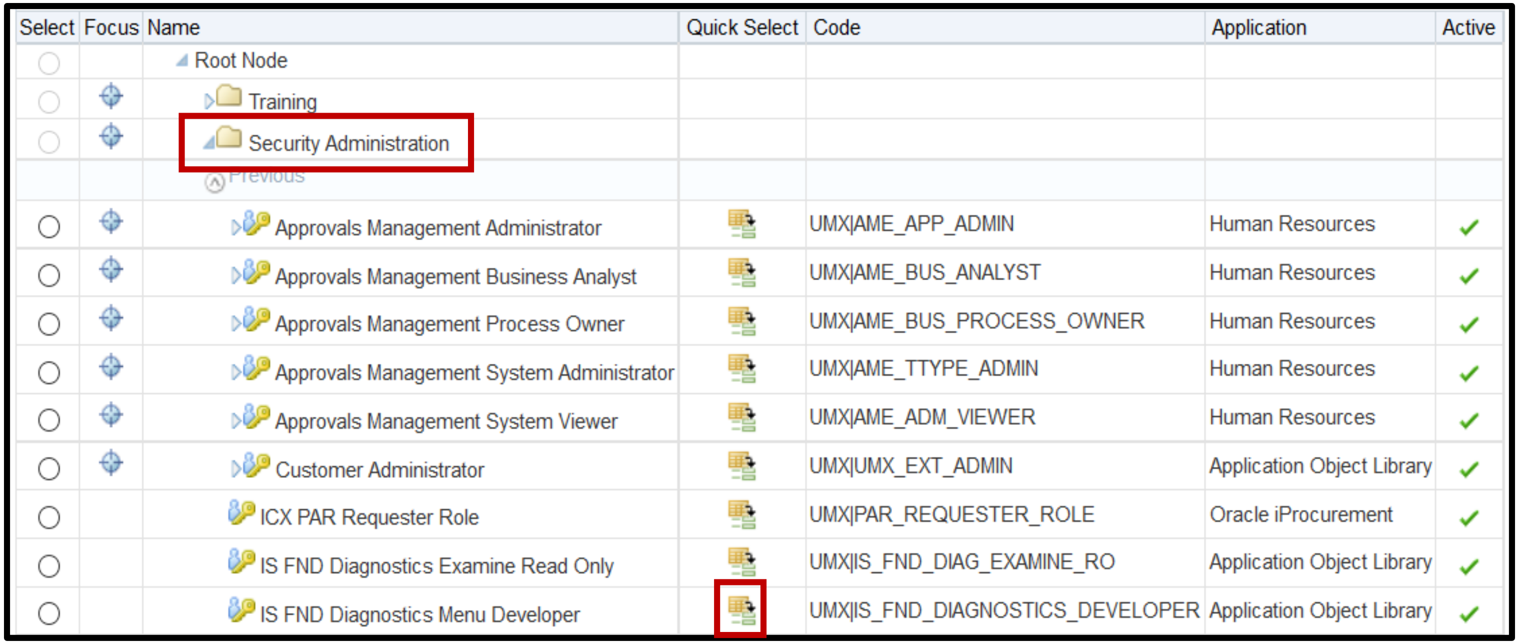
Role	Code	Application	Status	View In Hierarchy	Update
System Administrator	FND_RESP|SYSADMIN|SYSTEM_ADMINISTRATOR|STANDARD	System Administration	✓		



Focus	Name	Code	Application	Active	Update	Add Node	Remove Node
	All Roles, Responsibilities, and Groups						
	System Administrator	FND_RESP|SYSADMIN|SYSTEM_ADMINISTRATOR|STANDARD	System Administration	✓		+	

Read-Only Diagnostics in 12.1 via grants/roles

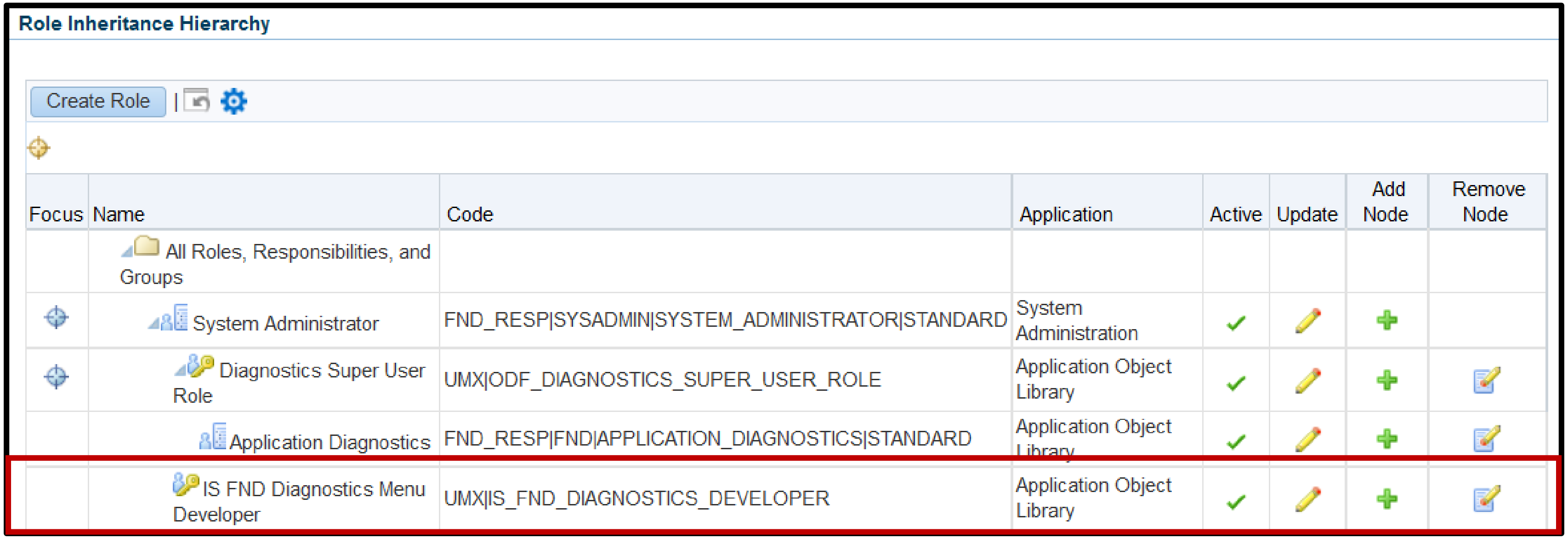
- Find the role just created and quick select



Select	Focus	Name	Quick Select	Code	Application	Active
○		Root Node				
○	⌖	Training				
○	⌖	Security Administration				
		Previous				
○	⌖	Approvals Management Administrator	▤	UMX|AME_APP_ADMIN	Human Resources	✓
○	⌖	Approvals Management Business Analyst	▤	UMX|AME_BUS_ANALYST	Human Resources	✓
○	⌖	Approvals Management Process Owner	▤	UMX|AME_BUS_PROCESS_OWNER	Human Resources	✓
○	⌖	Approvals Management System Administrator	▤	UMX|AME_TTYPE_ADMIN	Human Resources	✓
○	⌖	Approvals Management System Viewer	▤	UMX|AME_ADM_VIEWER	Human Resources	✓
○	⌖	Customer Administrator	▤	UMX|UMX_EXT_ADMIN	Application Object Library	✓
○		ICX PAR Requester Role	▤	UMX|PAR_REQUESTER_ROLE	Oracle iProcurement	✓
○		IS FND Diagnostics Examine Read Only	▤	UMX|IS_FND_DIAG_EXAMINE_RO	Application Object Library	✓
○		IS FND Diagnostics Menu Developer	▤	UMX|IS_FND_DIAGNOSTICS_DEVELOPER	Application Object Library	✓

Read-Only Diagnostics in 12.1 via grants/roles

- Updated view of hierarchy with added role



Role Inheritance Hierarchy

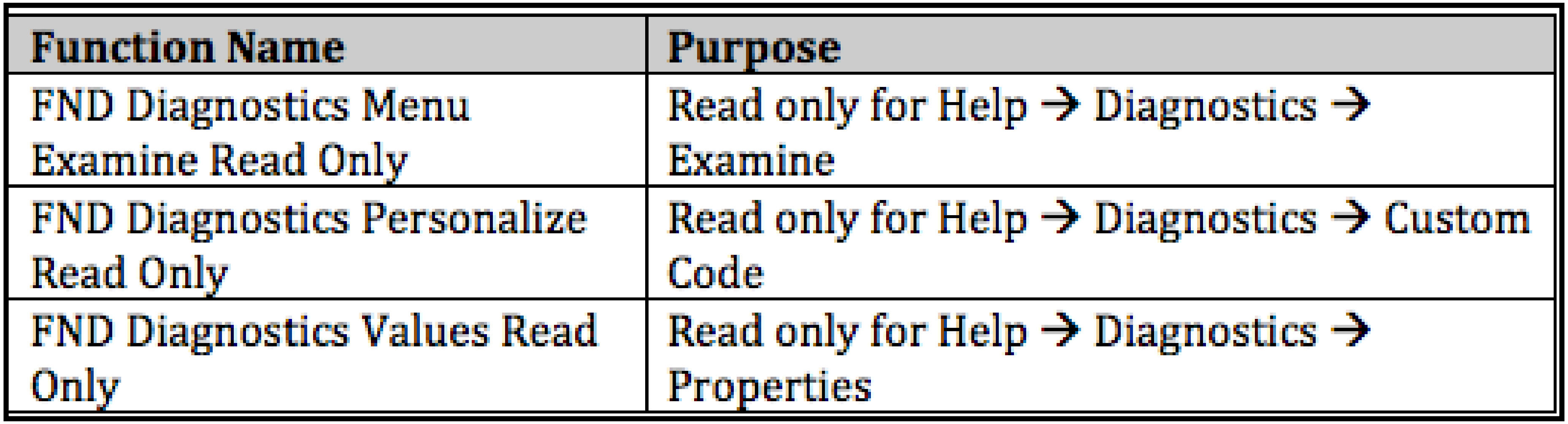
Focus	Name	Code	Application	Active	Update	Add Node	Remove Node
	All Roles, Responsibilities, and Groups						
⌖	System Administrator	FND_RESP|SYSADMIN|SYSTEM_ADMINISTRATOR|STANDARD	System Administration	✓	✎	+	
⌖	Diagnostics Super User Role	UMX|ODF_DIAGNOSTICS_SUPER_USER_ROLE	Application Object Library	✓	✎	+	📝
	Application Diagnostics	FND_RESP|FND|APPLICATION_DIAGNOSTICS|STANDARD	Application Object Library	✓	✎	+	📝
	IS FND Diagnostics Menu Developer	UMX|IS_FND_DIAGNOSTICS_DEVELOPER	Application Object Library	✓	✎	+	📝

Diagnostics in 12.1 via grants/roles

- More Information
    - System Administrator's Guide – 12.1, Appendix F
        - Not in 12.2 Guide
        - https://download.oracle.com/docs/cd/B53825_06/current/acrobat/121sacg.pdf
    - MOS Note 1223753.1 – Why Can't Users Enable Forms Trace in 12.1.3
    - MOS Note 2011837.1 – Create and Assign a Role Which Gives users Read Only Access to Diagnostics

Read-Only Diagnostics in 12.1.3 Function Security (Old way-outside of UMX)

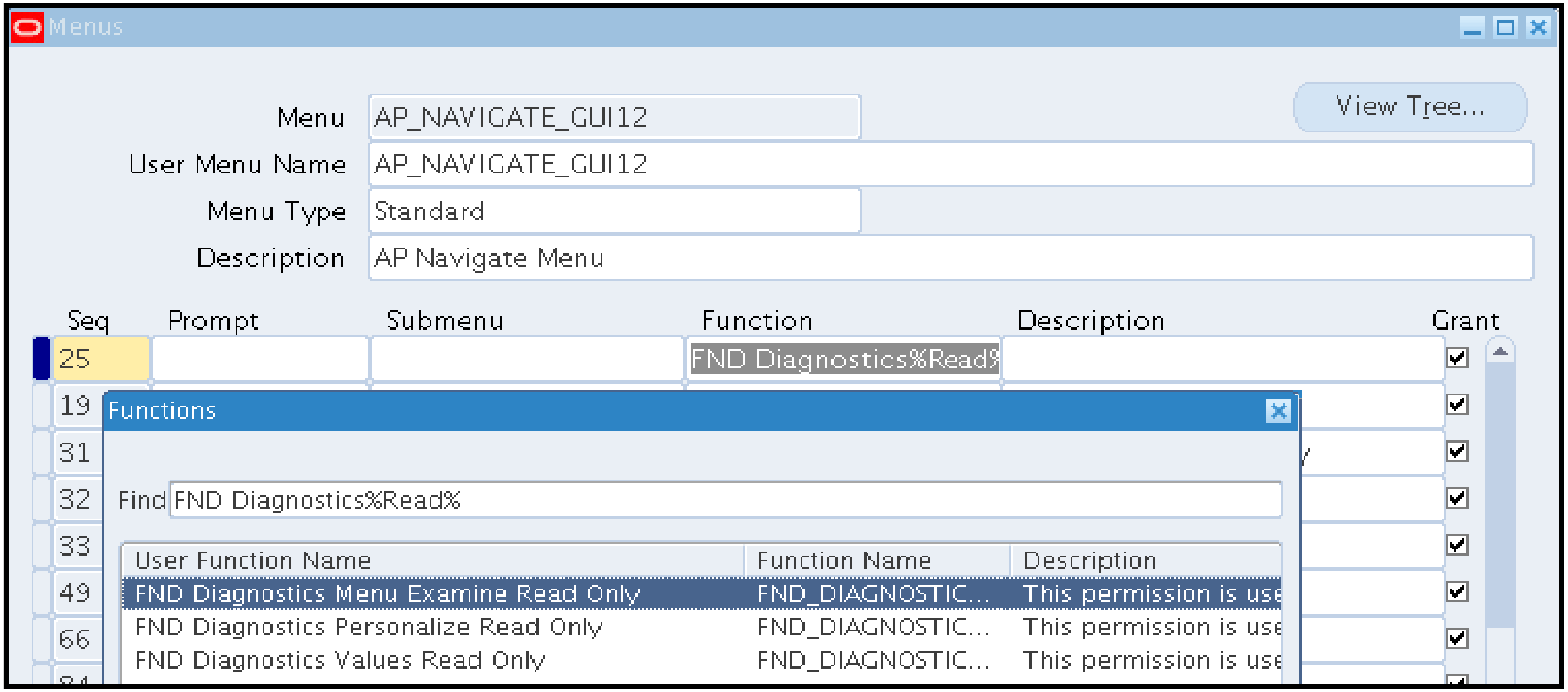
- Set profile option “Hide Diagnostics Menu Entry” to “No”
- Assign one or more of the read only sub-functions to the menu where this functionality is needed
- Apps password will not be requested in read-only mode



Function Name	Purpose
FND Diagnostics Menu Examine Read Only	Read only for Help → Diagnostics → Examine
FND Diagnostics Personalize Read Only	Read only for Help → Diagnostics → Custom Code
FND Diagnostics Values Read Only	Read only for Help → Diagnostics → Properties

Read-Only Diagnostics in 12.1.3 Function Security (Old way-outside of UMX)

- Example - Payables, Vision Operations (USA) responsibility linked to menu AP_NAVIGATE_GUI12
  - Leave prompt and Submenu null



Menu	AP_NAVIGATE_GUI12
User Menu Name	AP_NAVIGATE_GUI12
Menu Type	Standard
Description	AP Navigate Menu

Seq	Prompt	Submenu	Function	Description	Grant
25			FND Diagnostics%Read%		☑
19					☑
31					☑
32					☑
33					☑
49					☑
66					☑

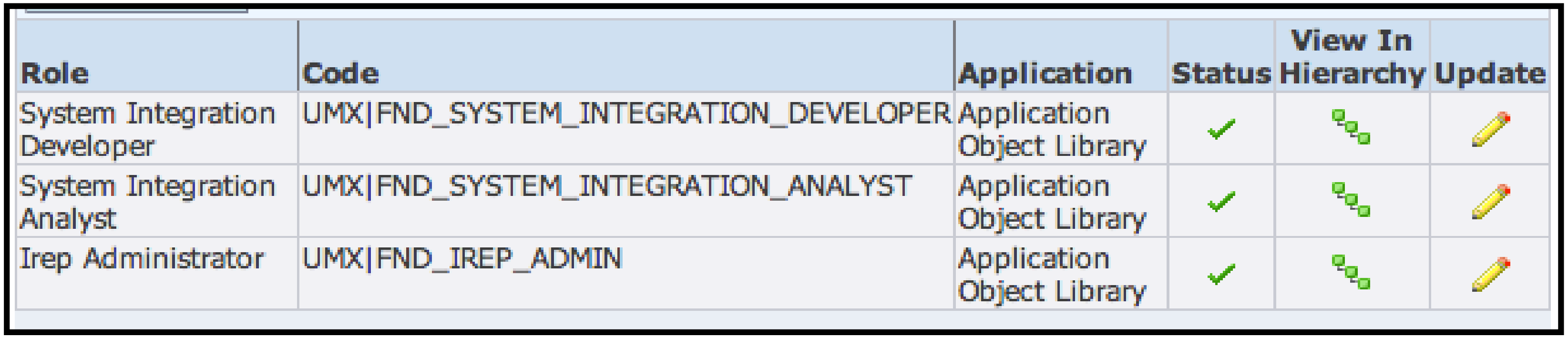
Find FND Diagnostics%Read%

User Function Name	Function Name	Description
FND Diagnostics Menu Examine Read Only	FND_DIAGNOSTIC...	This permission is use
FND Diagnostics Personalize Read Only	FND_DIAGNOSTIC...	This permission is use
FND Diagnostics Values Read Only	FND_DIAGNOSTIC...	This permission is use

Integration Repository

Access to Integration Repository

- Release 11i
  - http://irep.oracle.com/
    - As of March, 2014 – the above link is not working
- Early R12
  - Assign Responsibility – Integrated SOA Gateway
- Release 12.1+
  - Assign one of following roles

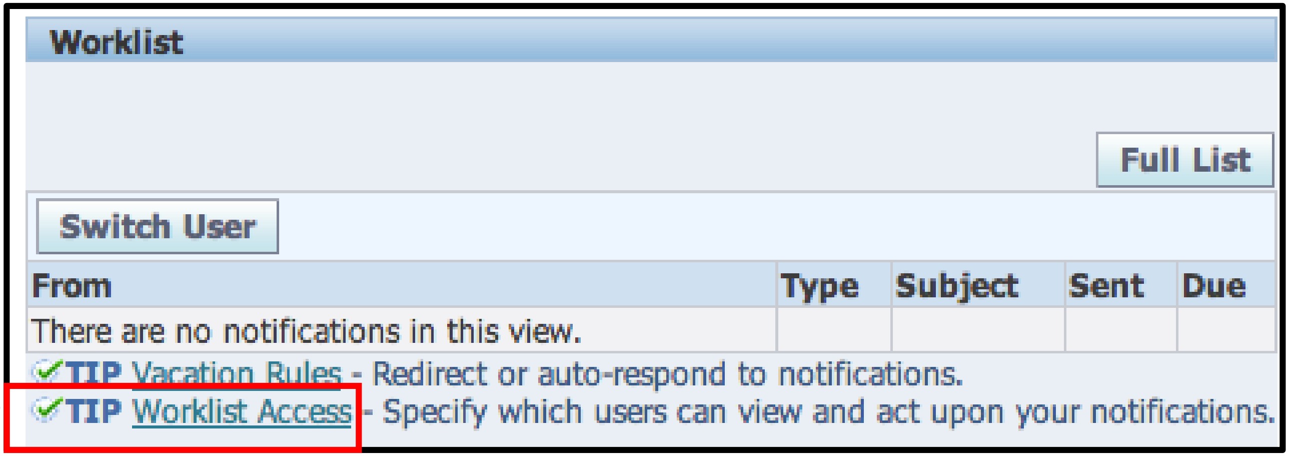


Role	Code	Application	Status	View In Hierarchy	Update
System Integration Developer	UMX|FND_SYSTEM_INTEGRATION_DEVELOPER	Application Object Library	✓	🖧	✎
System Integration Analyst	UMX|FND_SYSTEM_INTEGRATION_ANALYST	Application Object Library	✓	🖧	✎
Irep Administrator	UMX|FND_IREP_ADMIN	Application Object Library	✓	🖧	✎

Grant Worklist Access

Grant Worklist Access

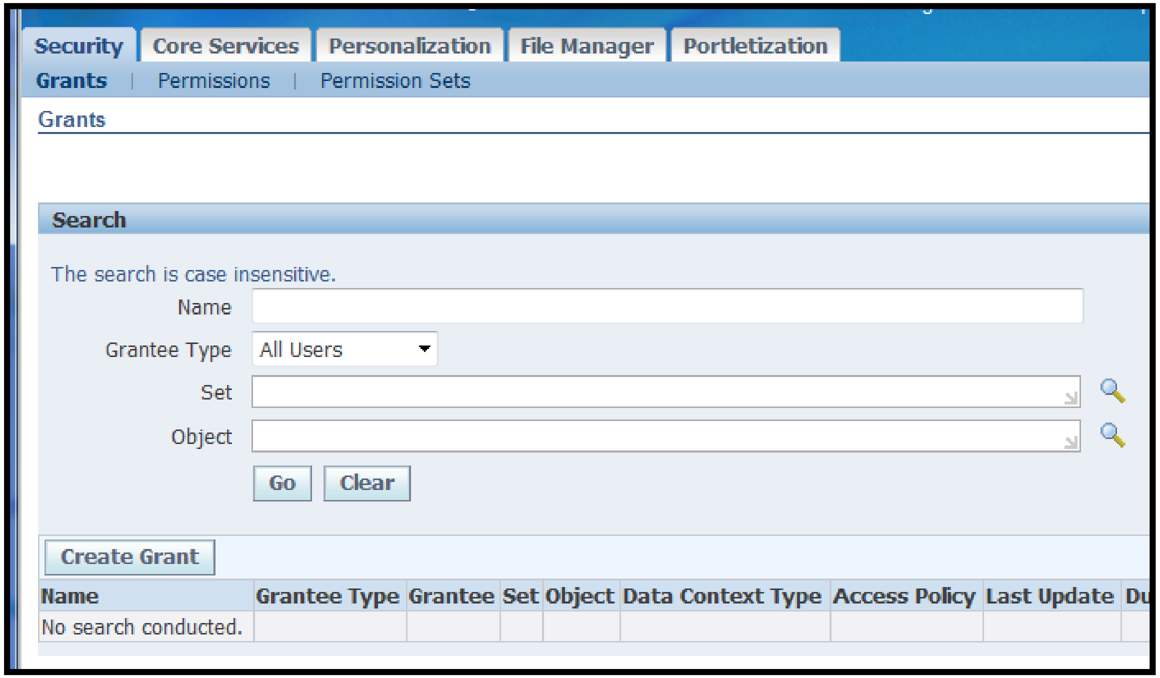
- From Form – Click "Worklist Access" link
  - Button no longer exists in 12.2.4
- 12.2.4+
  - From Functional Administrator or Responsibility
    - Grants Tab → Create Grant



From	Type	Subject	Sent	Due
There are no notifications in this view.				

✓TIP Vacation Rules - Redirect or auto-respond to notifications.

✓TIP Worklist Access - Specify which users can view and act upon your notifications.



The search is case insensitive.

Name

Grantee Type: All Users

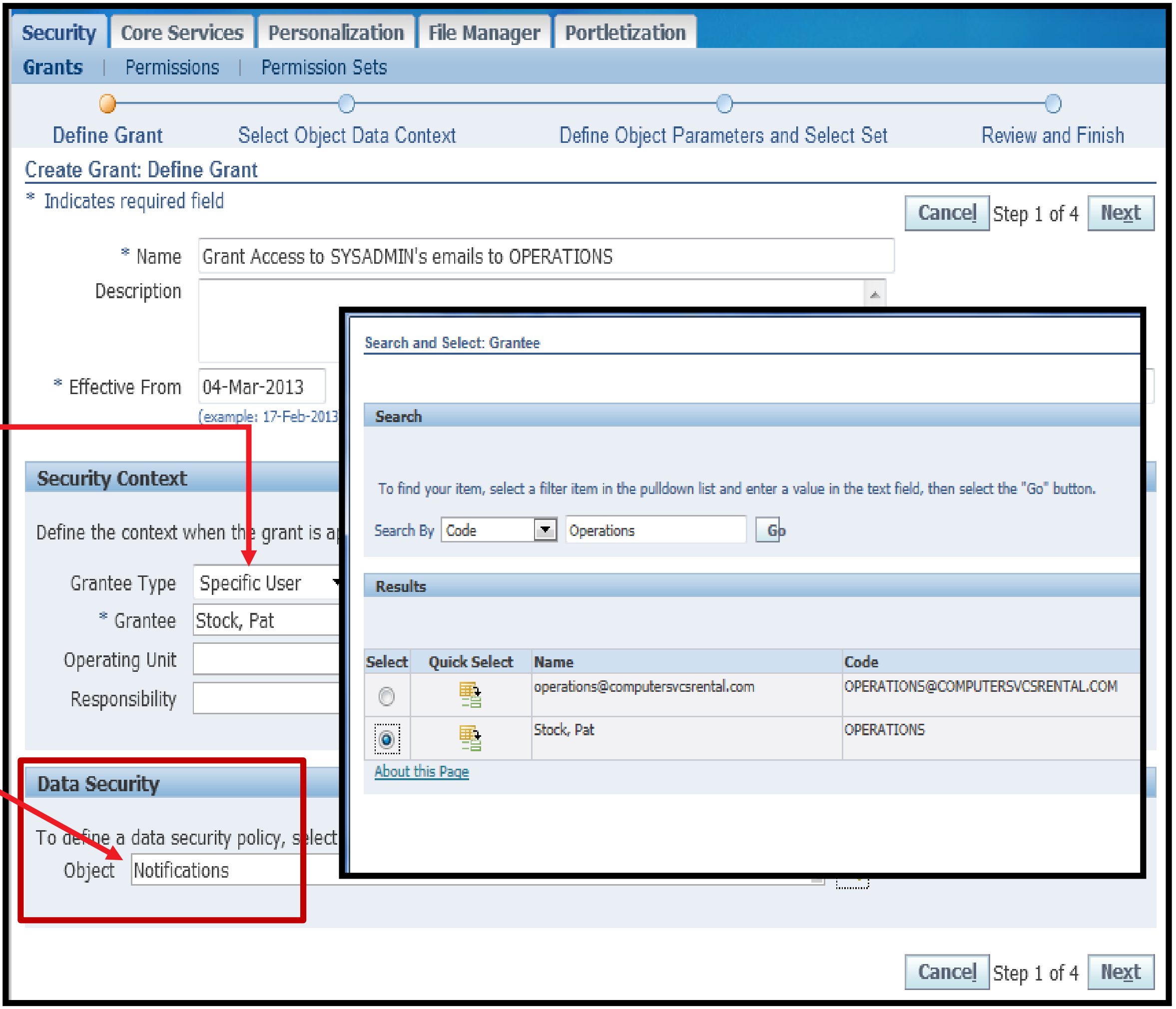
Set

Object

Name	Grantee Type	Grantee	Set	Object	Data Context Type	Access Policy	Last Update	Du
No search conducted.								

Grant Worklist Access

- Select specific user
  - This is the user who gets the access
- Data Security object is "Notifications"



Create Grant: Define Grant

* Indicates required field

* Name	Grant Access to SYSADMIN's emails to OPERATIONS
Description	
* Effective From	04-Mar-2013 (example: 17-Feb-2013

Security Context

Define the context when the grant is a

Grantee Type	Specific User
* Grantee	Stock, Pat
Operating Unit	
Responsibility	

Data Security

To define a data security policy, select

Object: Notifications

Search and Select: Grantee

Search

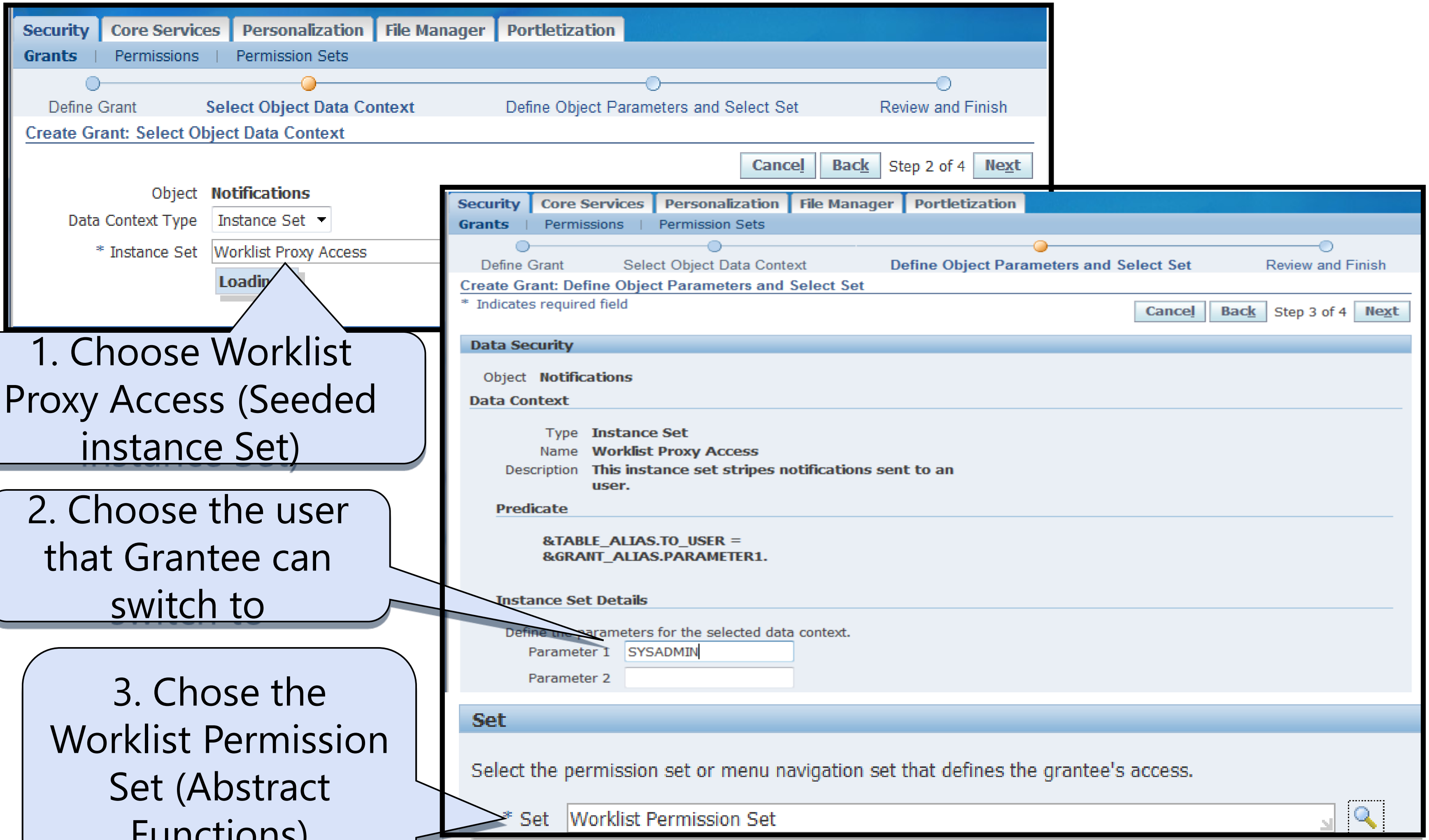
To find your item, select a filter item in the pulldown list and enter a value in the text field, then select the "Go" button.

Search By: Code | Operations | Go

Results

Select	Quick Select	Name	Code
○		operations@computersvcsrental.com	OPERATIONS@COMPUTERSVCSRENTAL.COM
●		Stock, Pat	OPERATIONS

Grant Worklist Access



Create Grant: Select Object Data Context

Step 2 of 4

Object **Notifications**

Data Context Type: Instance Set

* Instance Set: Worklist Proxy Access

Loadin

Create Grant: Define Object Parameters and Select Set

* Indicates required field

Step 3 of 4

Data Security

Object **Notifications**

Data Context

Type **Instance Set**

Name **Worklist Proxy Access**

Description **This instance set stripes notifications sent to an user.**

Predicate

&TABLE_ALIAS.TO_USER = &GRANT_ALIAS.PARAMETER1.

Instance Set Details

Define the parameters for the selected data context.

Parameter 1: SYSADMIN

Parameter 2:

Set

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

* Set: Worklist Permission Set

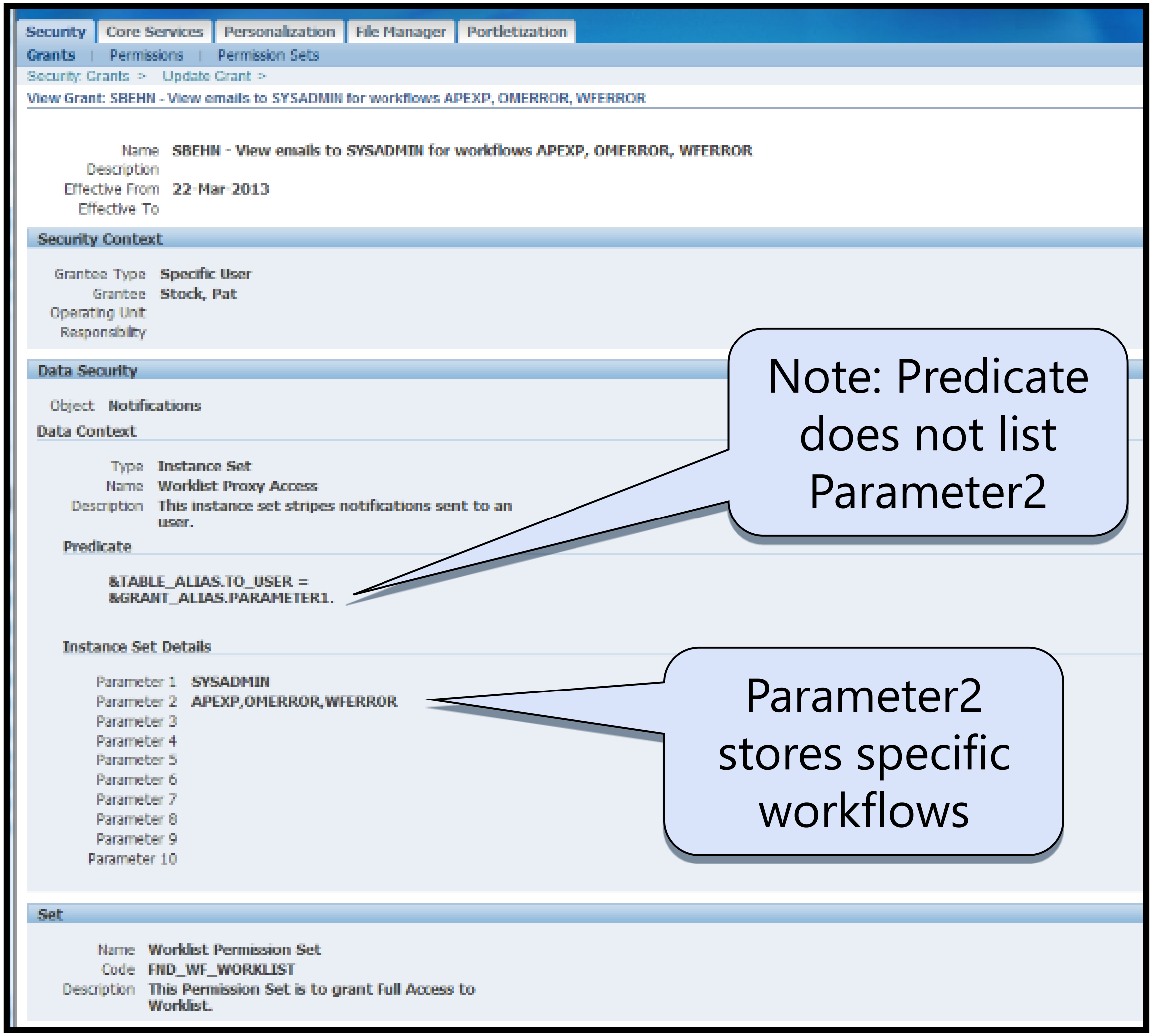
1. Choose Worklist Proxy Access (Seeded instance Set)

2. Choose the user that Grantee can switch to

3. Chose the Worklist Permission Set (Abstract Functions)

Grant Worklist Access

- By default, notifications are limited to active workflows or those in Lookup type WF_RR_ITEM_TYPES
- To limit to specific workflows, enter workflow types in parameter2 separated by ; (hidden parameter)


Security
Core Services
Personalization
File Manager
Portletization
Grants | Permissions | Permission Sets
Security: Grants > Update Grant >

View Grant: SBEHN - View emails to SYSADMIN for workflows APEXP, OMERROR, WFERROR

Name SBEHN - View emails to SYSADMIN for workflows APEXP, OMERROR, WFERROR
Description
Effective From 22-Mar-2013
Effective To

Security Context

Grantee Type Specific User
Grantee Stock, Pat
Operating Unit
Responsibility

Data Security

Object Notifications

Data Context

Type Instance Set
Name Worklist Proxy Access
Description This instance set stripes notifications sent to an user.

Predicate

&TABLE_ALIAS.TO_USER = &GRANT_ALIAS.PARAMETER1.

Instance Set Details

Parameter 1 SYSADMIN
Parameter 2 APEXP,OMERROR,WFERROR
Parameter 3
Parameter 4
Parameter 5
Parameter 6
Parameter 7
Parameter 8
Parameter 9
Parameter 10

Set

Name Worklist Permission Set
Code FND_WF_WORKLIST
Description This Permission Set is to grant Full Access to Worklist.

Note: Predicate does not list Parameter2

Parameter2 stores specific workflows

Poll Question

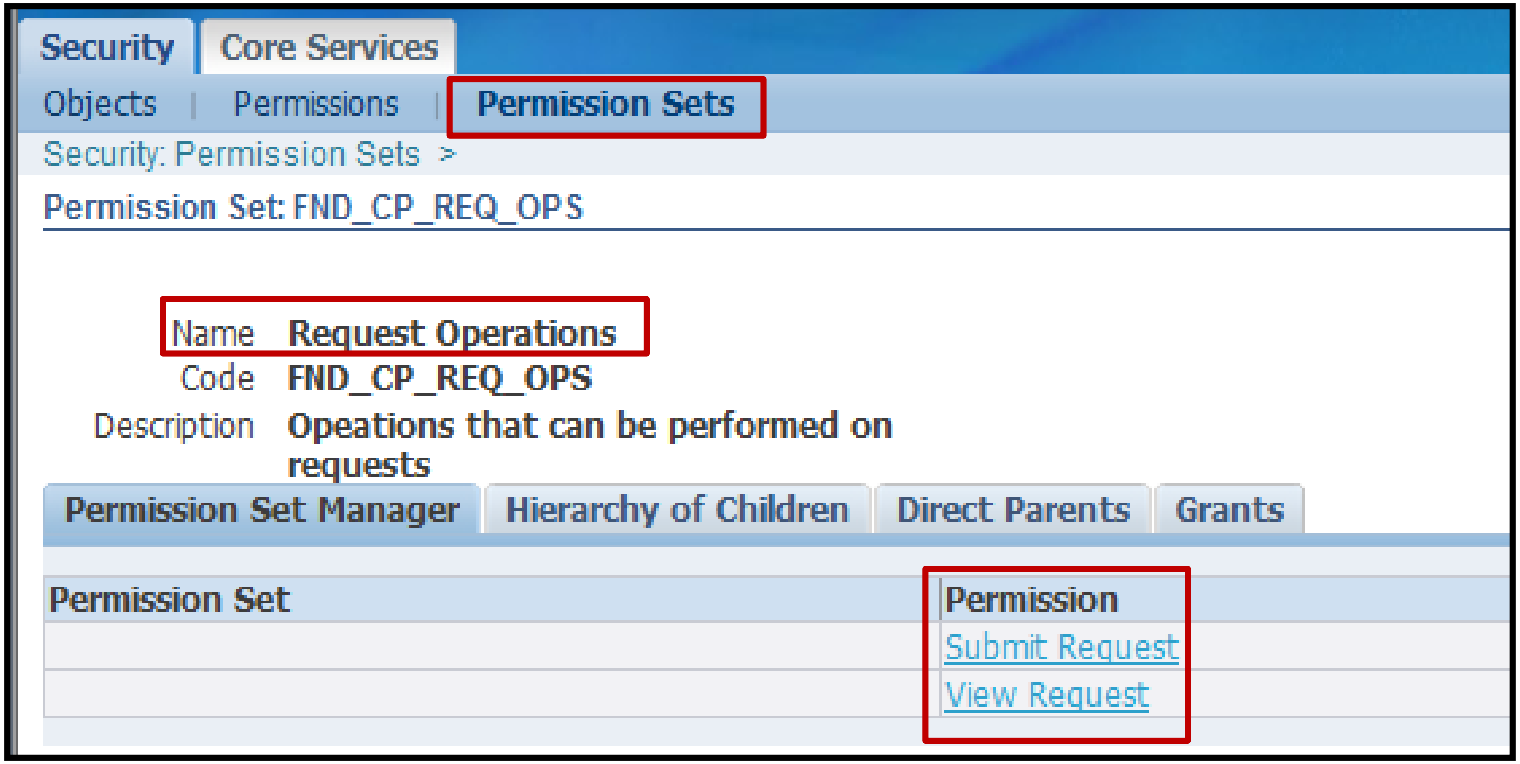
View Concurrent Requests

Access to Concurrent Requests

- Profile Option “Concurrent Report Access Level” is obsolete in 12.1
  - Allowed users to see all concurrent requests in a responsibility
- This functionality is replaced by RBAC permissions
  - See My Oracle Support ID 737547.1

View Others Requests- Permission Set / Permission

- Function Security - The **Request Operations** permission set includes permissions to submit and view requests



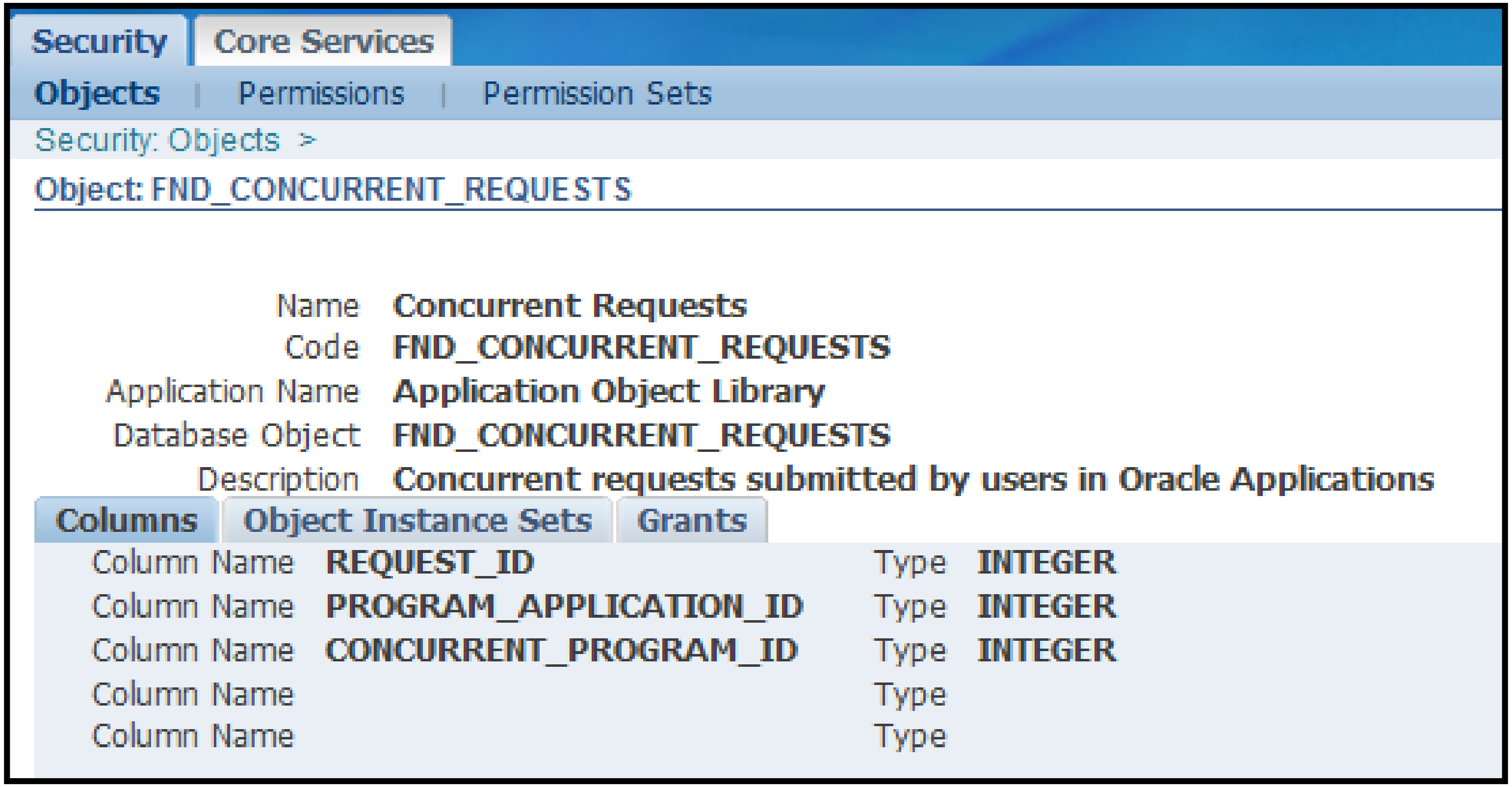
Permission Set: FND_CP_REQ_OPS

Name Request Operations
Code FND_CP_REQ_OPS
Description Opeations that can be performed on requests

Permission Set	Permission
	Submit Request
	View Request

View Others Requests Object – Concurrent Requests

- Data Security - The Concurrent Requests data object shown below is seeded



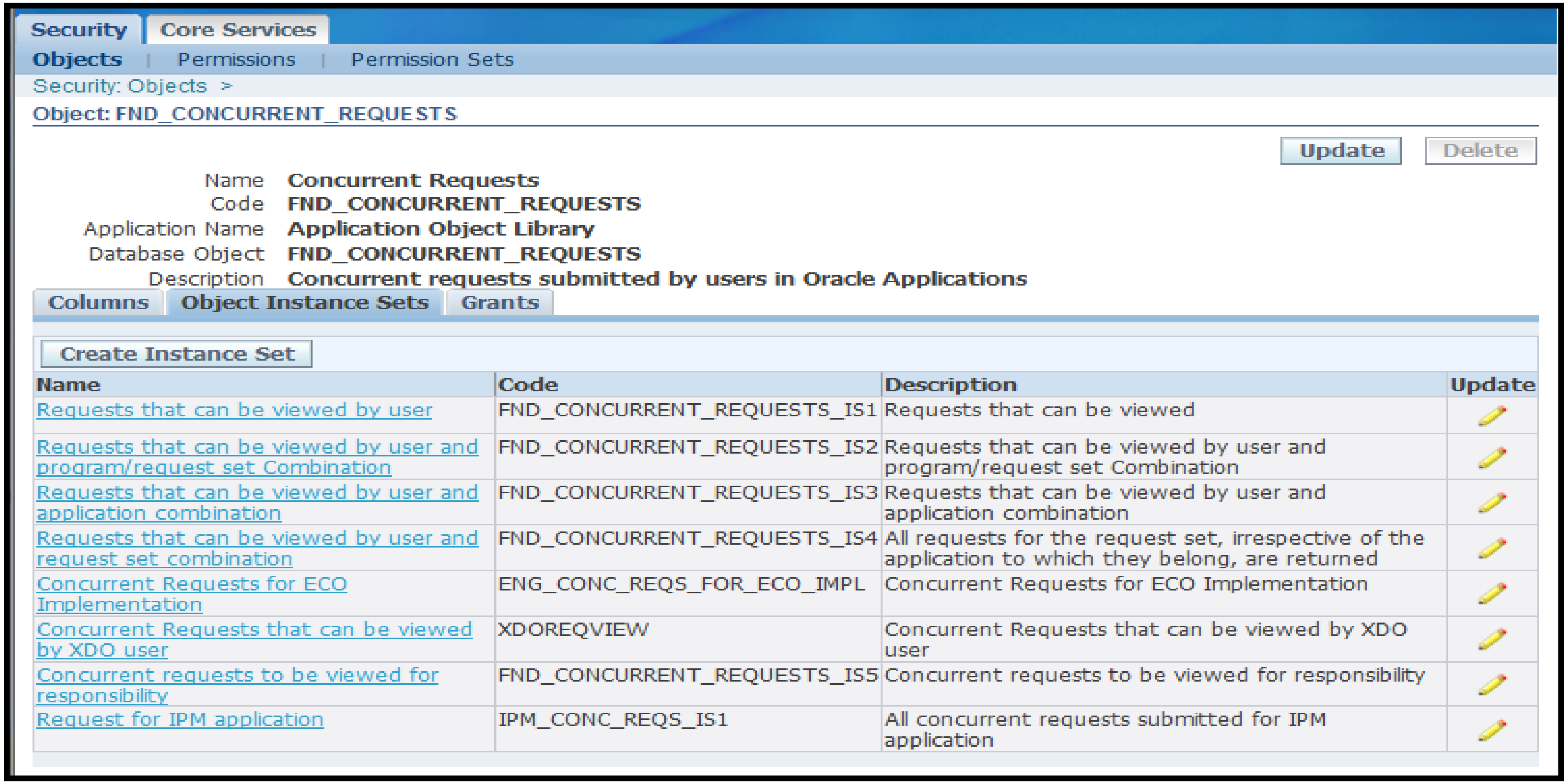
Object: FND_CONCURRENT_REQUESTS

Name Concurrent Requests
Code FND_CONCURRENT_REQUESTS
Application Name Application Object Library
Database Object FND_CONCURRENT_REQUESTS
Description Concurrent requests submitted by users in Oracle Applications

Column Name	REQUEST_ID	Type	INTEGER
Column Name	PROGRAM_APPLICATION_ID	Type	INTEGER
Column Name	CONCURRENT_PROGRAM_ID	Type	INTEGER
Column Name		Type	
Column Name		Type	

View Others Requests-Instance Sets

- Data Security "where clause" - Several object instance sets are seeded and well described or you can create your own



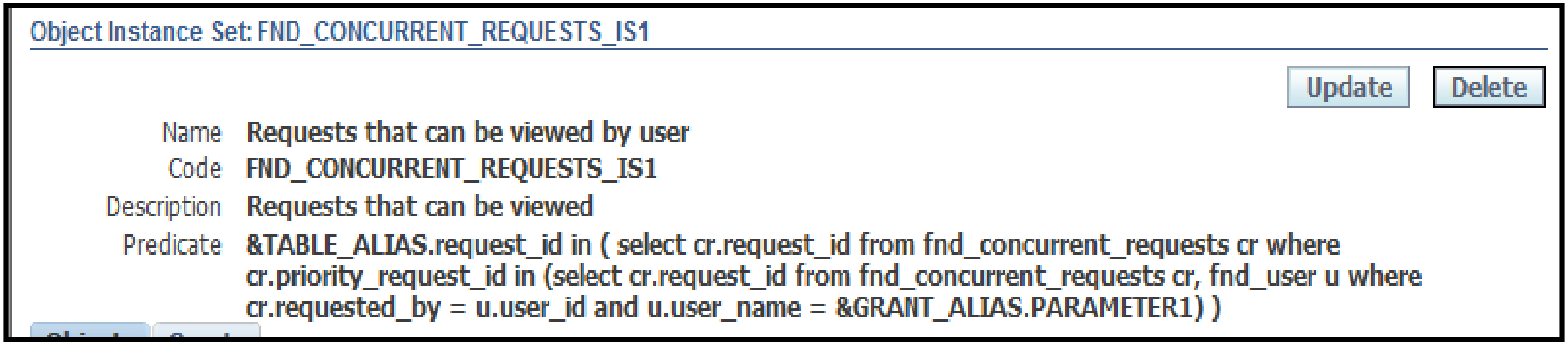
Object: FND_CONCURRENT_REQUESTS

Name	**Concurrent Requests**
Code	**FND_CONCURRENT_REQUESTS**
Application Name	**Application Object Library**
Database Object	**FND_CONCURRENT_REQUESTS**
Description	**Concurrent requests submitted by users in Oracle Applications**

Name	Code	Description	Update
Requests that can be viewed by user	FND_CONCURRENT_REQUESTS_IS1	Requests that can be viewed	✎
Requests that can be viewed by user and program/request set Combination	FND_CONCURRENT_REQUESTS_IS2	Requests that can be viewed by user and program/request set Combination	✎
Requests that can be viewed by user and application combination	FND_CONCURRENT_REQUESTS_IS3	Requests that can be viewed by user and application combination	✎
Requests that can be viewed by user and request set combination	FND_CONCURRENT_REQUESTS_IS4	All requests for the request set, irrespective of the application to which they belong, are returned	✎
Concurrent Requests for ECO Implementation	ENG_CONC_REQS_FOR_ECO_IMPL	Concurrent Requests for ECO Implementation	✎
Concurrent Requests that can be viewed by XDO user	XDOREQVIEW	Concurrent Requests that can be viewed by XDO user	✎
Concurrent requests to be viewed for responsibility	FND_CONCURRENT_REQUESTS_IS5	Concurrent requests to be viewed for responsibility	✎
Request for IPM application	IPM_CONC_REQS_IS1	All concurrent requests submitted for IPM application	✎

View Others Requests - Seeded Instance Sets

- Examples of seeded object instance sets
  - View all my requests from any responsibility
    - More efficient then trying to remember where you ran a request

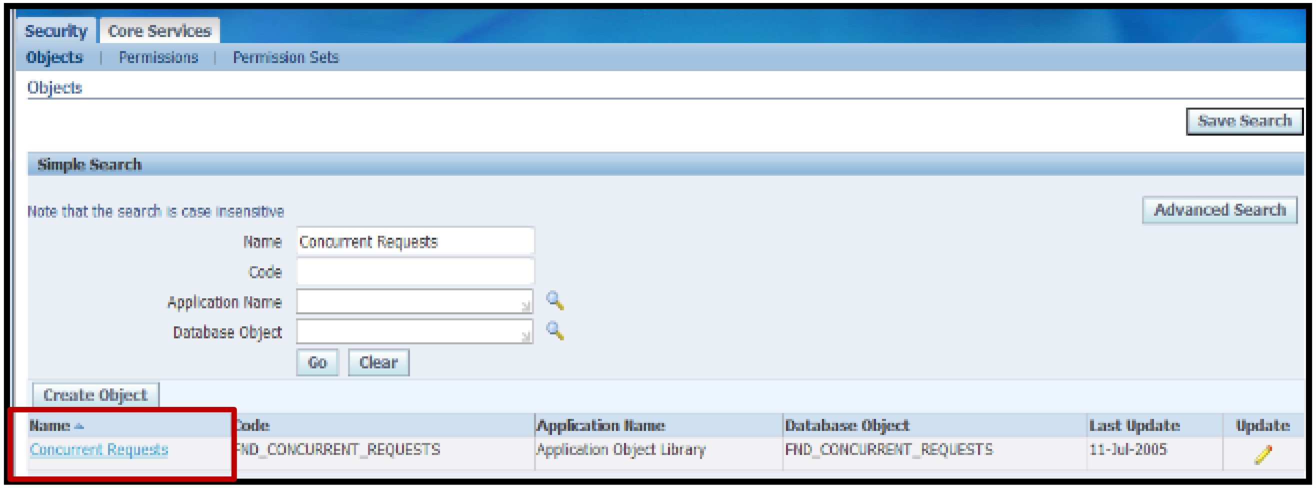


Object Instance Set: FND_CONCURRENT_REQUESTS_IS1

Name	Requests that can be viewed by user
Code	FND_CONCURRENT_REQUESTS_IS1
Description	Requests that can be viewed
Predicate	&TABLE_ALIAS.request_id in (select cr.request_id from fnd_concurrent_requests cr where cr.priority_request_id in (select cr.request_id from fnd_concurrent_requests cr, fnd_user u where cr.requested_by = u.user_id and u.user_name = &GRANT_ALIAS.PARAMETER1))

View Others Requests - Create Instance Sets

- Must create instance set to achieve exact replacement of obsolete profile option
- MOS ID 804296.1 “R12: How To Configure Access To Request Output Of The Same Responsibility”
- From Functional Developer → Objects
  - Query the Object “Concurrent Requests”
  - Click the link in the Name column



Objects

Simple Search

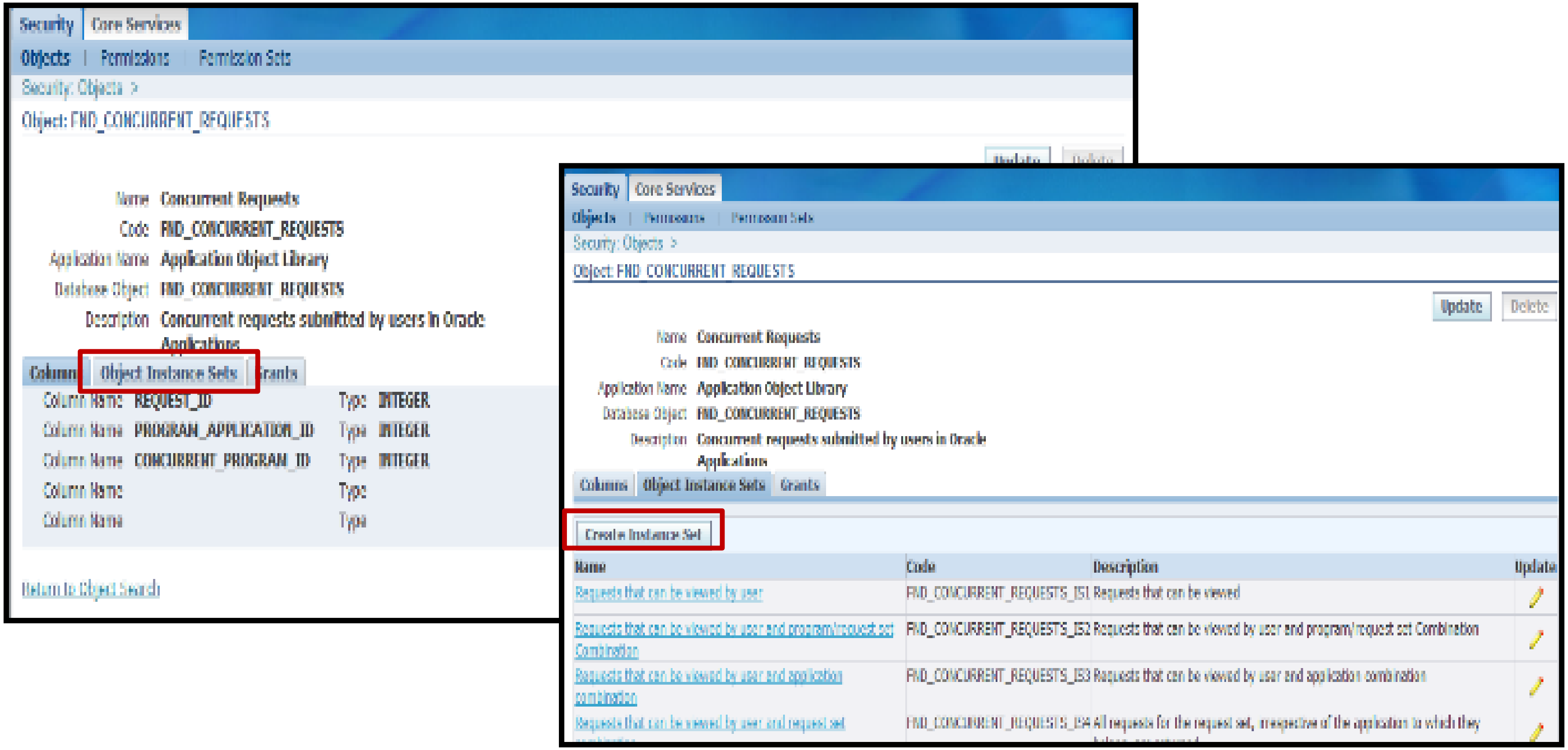
Note that the search is case insensitive

Name	Concurrent Requests
Code	
Application Name	
Database Object	

Name ▲	ode	Application Name	Database Object	Last Update	Update
Concurrent Requests	ND_CONCURRENT_REQUESTS	Application Object Library	FND_CONCURRENT_REQUESTS	11-Jul-2005	✎

View Others Requests - Create Instance Sets

- Click on the Object Instance Sets tab
- Then click the “Create Instance Set” button



Security | Core Services

Objects | Permissions | Permission Sets

Security: Objects >

Object: FND_CONCURRENT_REQUESTS

Name Concurrent Requests

Code FND_CONCURRENT_REQUESTS

Application Name Application Object Library

Database Object FND_CONCURRENT_REQUESTS

Description Concurrent requests submitted by users in Oracle Applications

Column Name	REQUEST_ID	Type	INTEGER
Column Name	PROGRAM_APPLICATION_ID	Type	INTEGER
Column Name	CONCURRENT_PROGRAM_ID	Type	INTEGER
Column Name		Type	
Column Name		Type	

Security | Core Services

Objects | Permissions | Permission Sets

Security: Objects >

Object: FND_CONCURRENT_REQUESTS

Name Concurrent Requests

Code FND_CONCURRENT_REQUESTS

Application Name Application Object Library

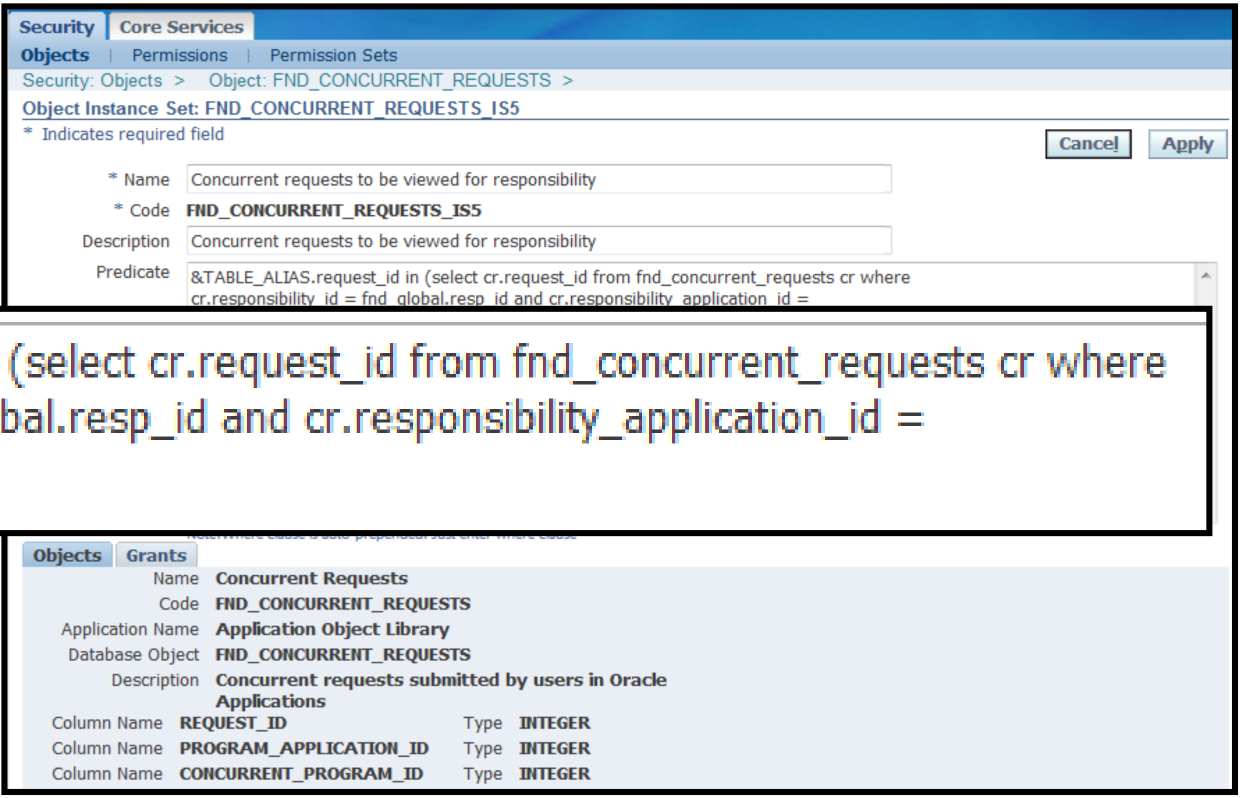
Database Object FND_CONCURRENT_REQUESTS

Description Concurrent requests submitted by users in Oracle Applications

Name	Code	Description	Update
Requests that can be viewed by user	FND_CONCURRENT_REQUESTS_IS1	Requests that can be viewed	✎
Requests that can be viewed by user and program/request set Combination	FND_CONCURRENT_REQUESTS_IS2	Requests that can be viewed by user and program/request set Combination	✎
Requests that can be viewed by user and application combination	FND_CONCURRENT_REQUESTS_IS3	Requests that can be viewed by user and application combination	✎
Requests that can be viewed by user and request set	FND_CONCURRENT_REQUESTS_IS4	All requests for the request set, irrespective of the application to which they	✎

View Others Requests-Create Instance Sets

- Create the instance set exactly as shown below



Security
Core Services
Objects | Permissions | Permission Sets
Security: Objects > Object: FND_CONCURRENT_REQUESTS >
Cancel
Apply

Object Instance Set: FND_CONCURRENT_REQUESTS_IS5

* Indicates required field

* Name: Concurrent requests to be viewed for responsibility

* Code: FND_CONCURRENT_REQUESTS_IS5

Description: Concurrent requests to be viewed for responsibility

Predicate: &TABLE_ALIAS.request_id in (select cr.request_id from fnd_concurrent_requests cr where cr.responsibility_id = fnd_global.resp_id and cr.responsibility_application_id =

&TABLE_ALIAS.request_id in (select cr.request_id from fnd_concurrent_requests cr where cr.responsibility_id = fnd_global.resp_id and cr.responsibility_application_id = fnd_global.resp_appl_id)

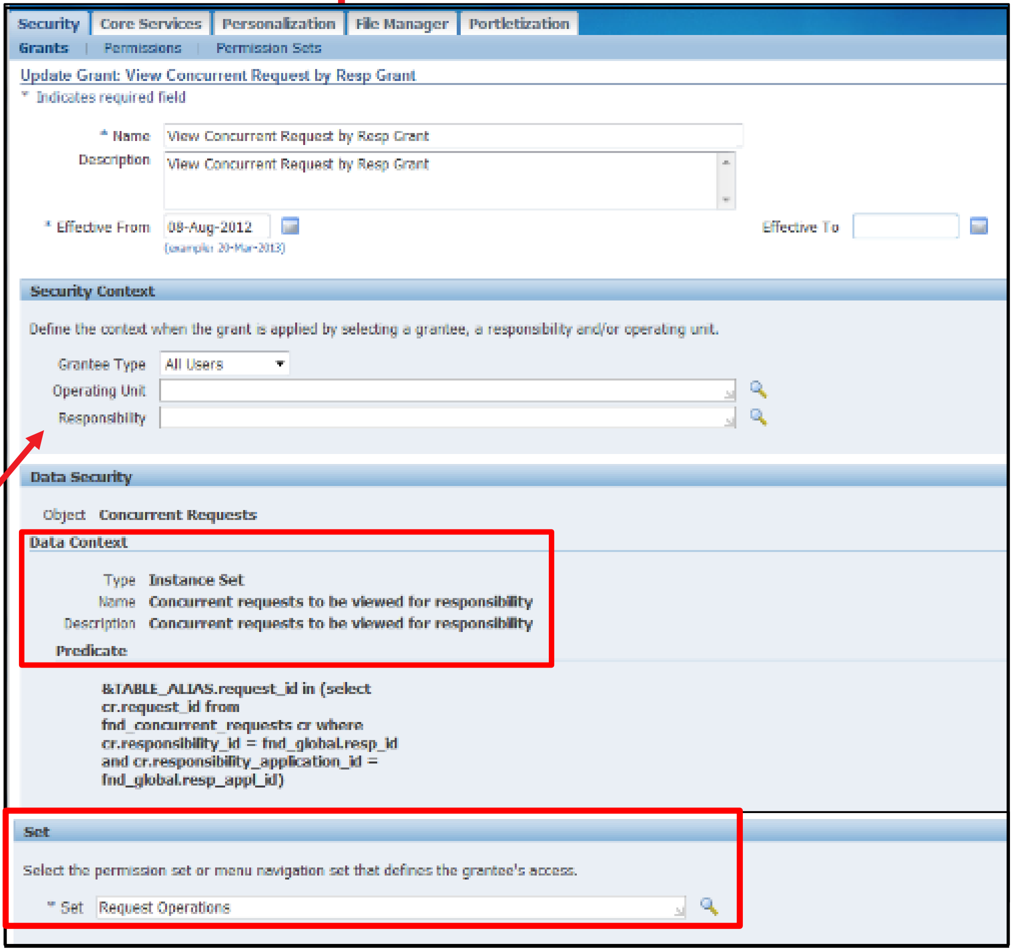
Objects | Grants

Name	Concurrent Requests
Code	FND_CONCURRENT_REQUESTS
Application Name	Application Object Library
Database Object	FND_CONCURRENT_REQUESTS
Description	Concurrent requests submitted by users in Oracle Applications

Column Name	REQUEST_ID	Type	INTEGER
Column Name	PROGRAM_APPLICATION_ID	Type	INTEGER
Column Name	CONCURRENT_PROGRAM_ID	Type	INTEGER

View Others Requests
Site Level – Grant for All Responsibilities

- Create a grant with this new object instance set and the "Request Operations" function security permission set to allow the grantee to see all requests in that responsibility
- You can also choose to limit this to a specific responsibility or operating unit



Update Grant: View Concurrent Request by Resp Grant

* Indicates required field

* Name: View Concurrent Request by Resp Grant

Description: View Concurrent Request by Resp Grant

* Effective From: 08-Aug-2012 (example: 20-Mar-2013)

Effective To:

Security Context

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

Grantee Type: All Users

Operating Unit:

Responsibility:

Data Security

Object: Concurrent Requests

Data Context

Type: Instance Set

Name: Concurrent requests to be viewed for responsibility

Description: Concurrent requests to be viewed for responsibility

Predicate

```
&TABLE_ALIAS.request_id in (select
cr.request_id from
fnd_concurrent_requests cr where
cr.responsibility_id = fnd_global.resp_id
and cr.responsibility_application_id =
fnd_global.resp_appl_id)
```

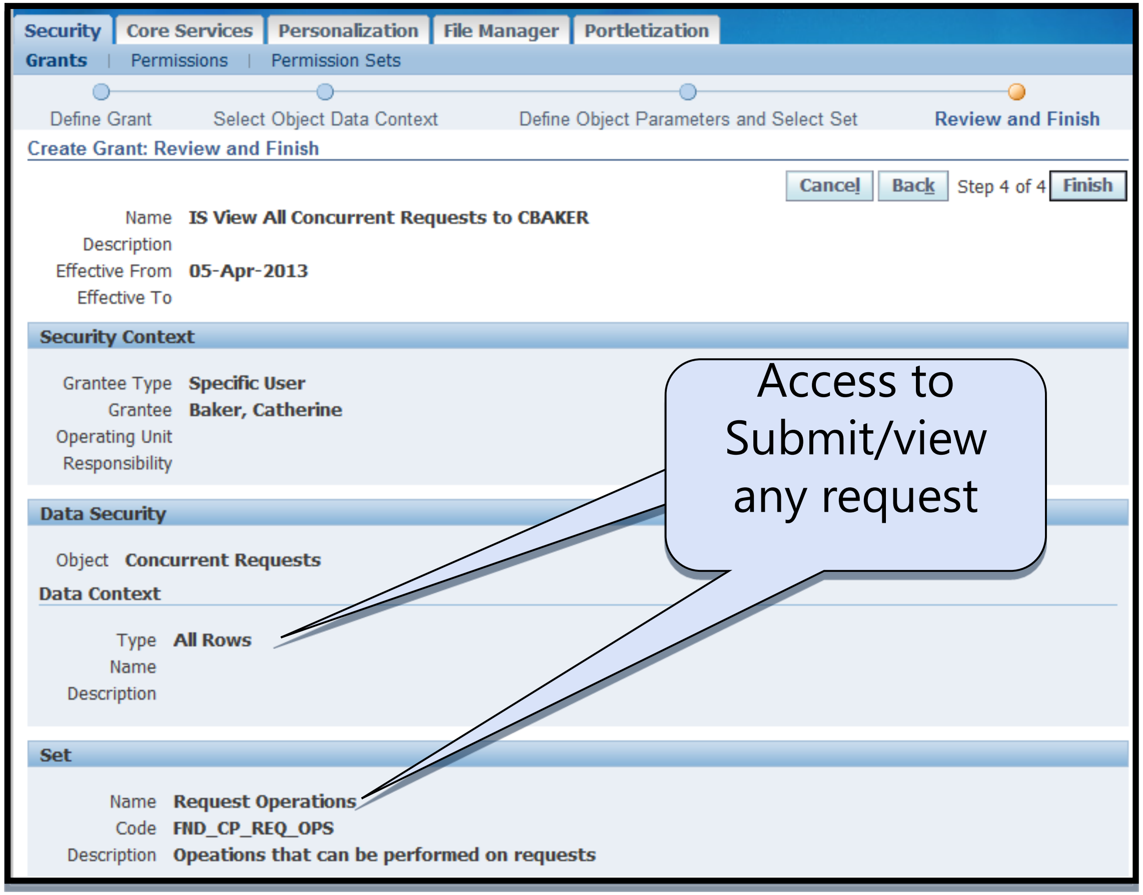
Set

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

* Set: Request Operations

View Others Requests – Help Desk Support

- Recommended only for help desk/support users
- Can see any request from any responsibility



Create Grant: Review and Finish

Name IS View All Concurrent Requests to CBAKER
Description
Effective From 05-Apr-2013
Effective To

Security Context

Grantee Type Specific User
Grantee Baker, Catherine
Operating Unit
Responsibility

Data Security

Object Concurrent Requests

Data Context

Type All Rows
Name
Description

Set

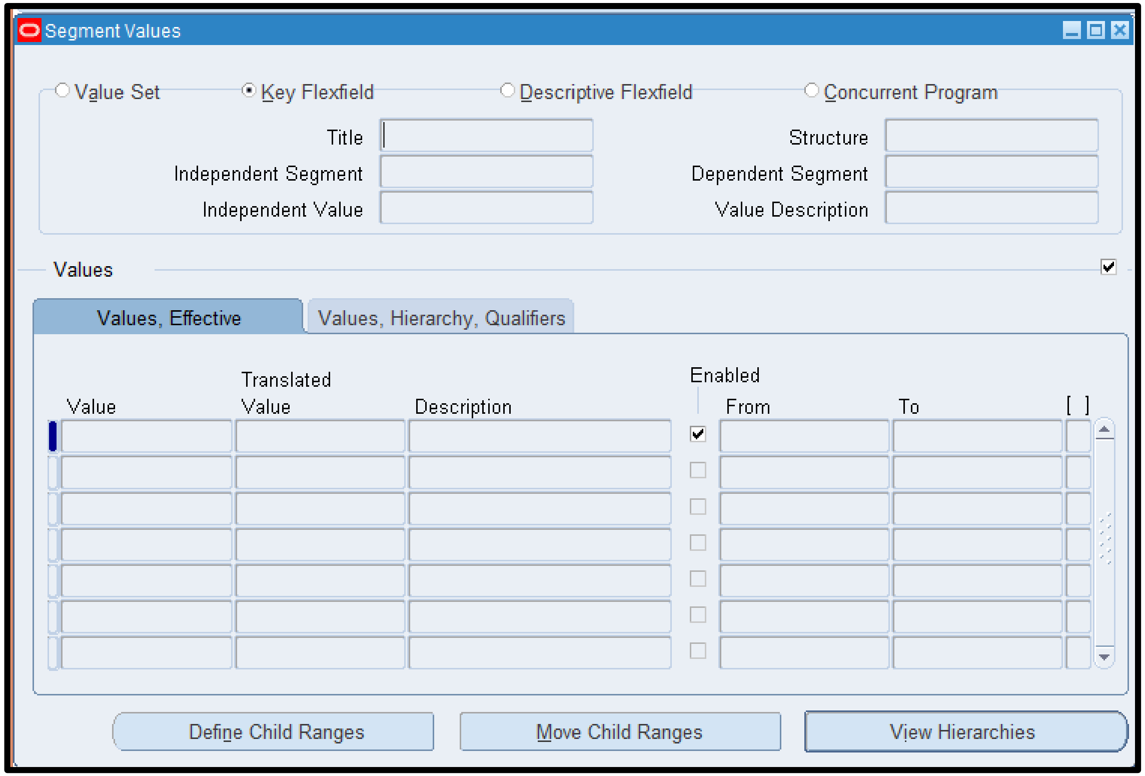
Name Request Operations
Code FND_CP_REQ_OPS
Description Opeations that can be performed on requests

Access to Submit/view any request

Flexfield Security Required in 12.2

Flexfield Value Set Security – FNDFFMSV – 12.2

- Upon upgrade, users will not have access to any records in this form
- Many ways to get to this form…our example
  - GL→Setup→Financials→Flexfields→Validation→Values



Segment Values

○ Value Set ● Key Flexfield ○ Descriptive Flexfield ○ Concurrent Program

Title		Structure	
Independent Segment		Dependent Segment	
Independent Value		Value Description	

Values ☑

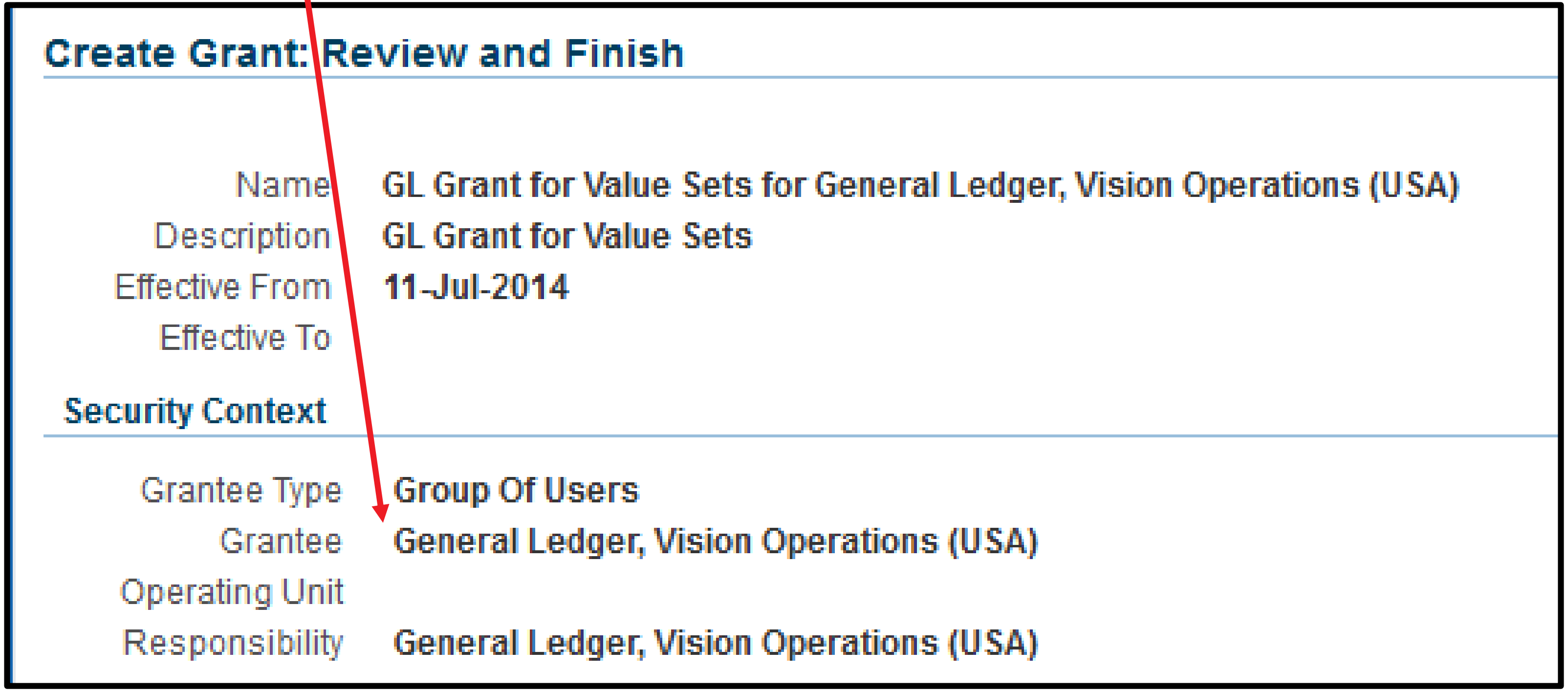
Value	Translated Value	Description	Enabled	From	To	[ ]
			☑			
			□			
			□			
			□			
			□			
			□			
			□			

Function and Data Security

- Must set up function security to define what the user can do in the form
  - Grant by flexfield, report or value set
  - Grant to application, user, group
- Affects **ALL** Independent and Dependent value sets
- Affects what privileges users have in the Segment Values form
- Note: Even if you create a new value set, you still won't be able to assign values to that set until security is set up

Grant access to the data

- Functional Adminstrator→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

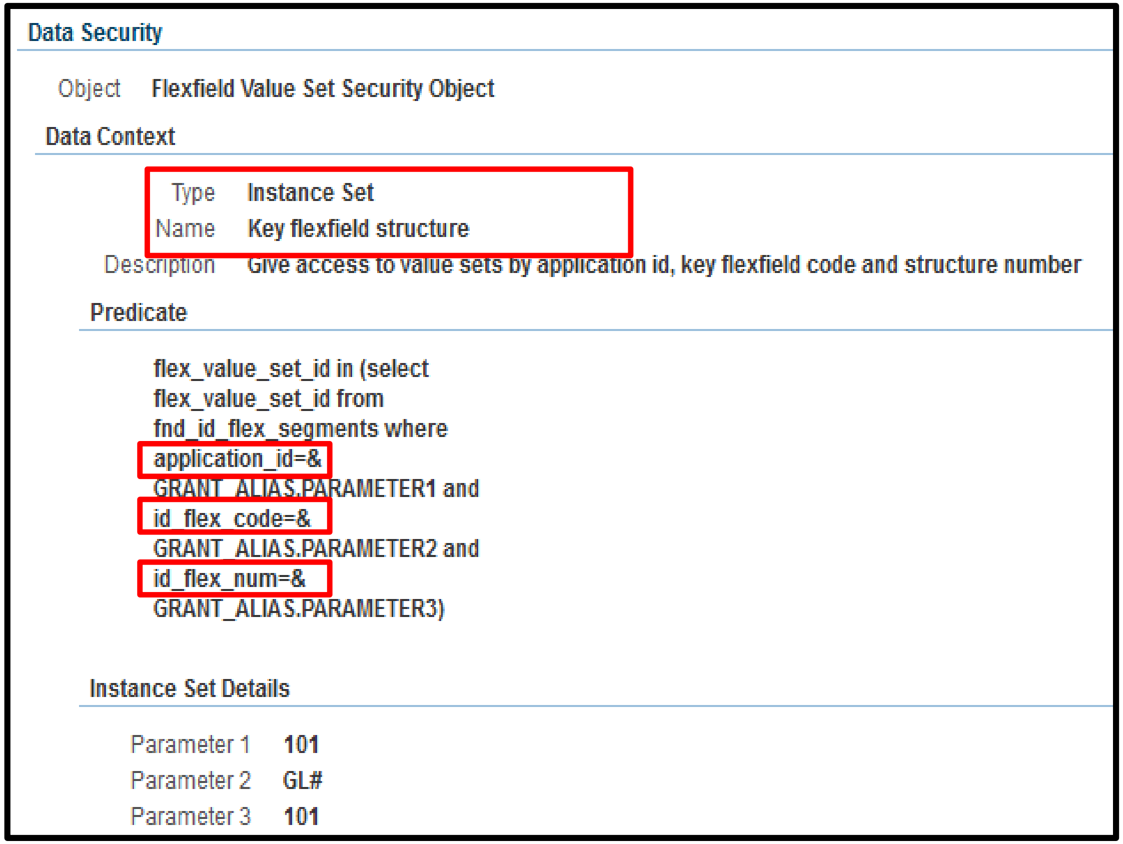
Name	GL Grant for Value Sets for General Ledger, Vision Operations (USA)
Description	GL Grant for Value Sets
Effective From	11-Jul-2014
Effective To	

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

- Key flexfield structure instance set allow you to dictate app id, key flexfield code and/or structure number



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

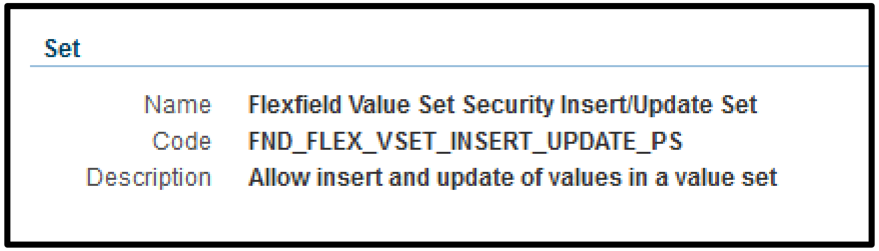
```
flex_value_set_id in (select
flex_value_set_id from
fnd_id_flex_segments where
application_id=&
GRANT_ALIAS.PARAMETER1 and
id_flex_code=&
GRANT_ALIAS.PARAMETER2 and
id_flex_num=&
GRANT_ALIAS.PARAMETER3)
```

Instance Set Details

Parameter 1	101
Parameter 2	GL#
Parameter 3	101

Function Security Permission set

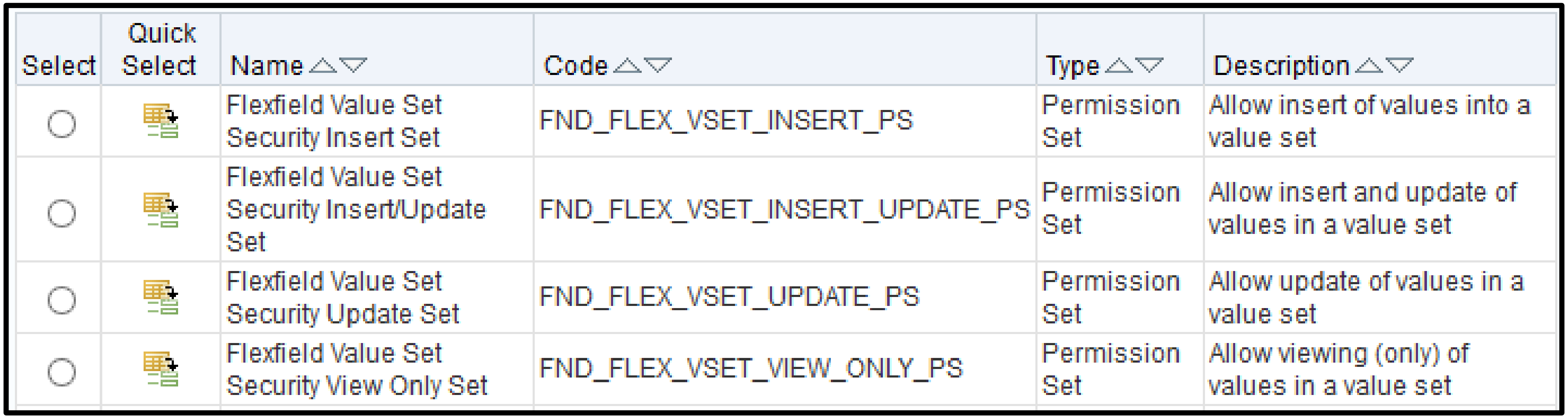
- For this example, I chose to allow insert or update



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

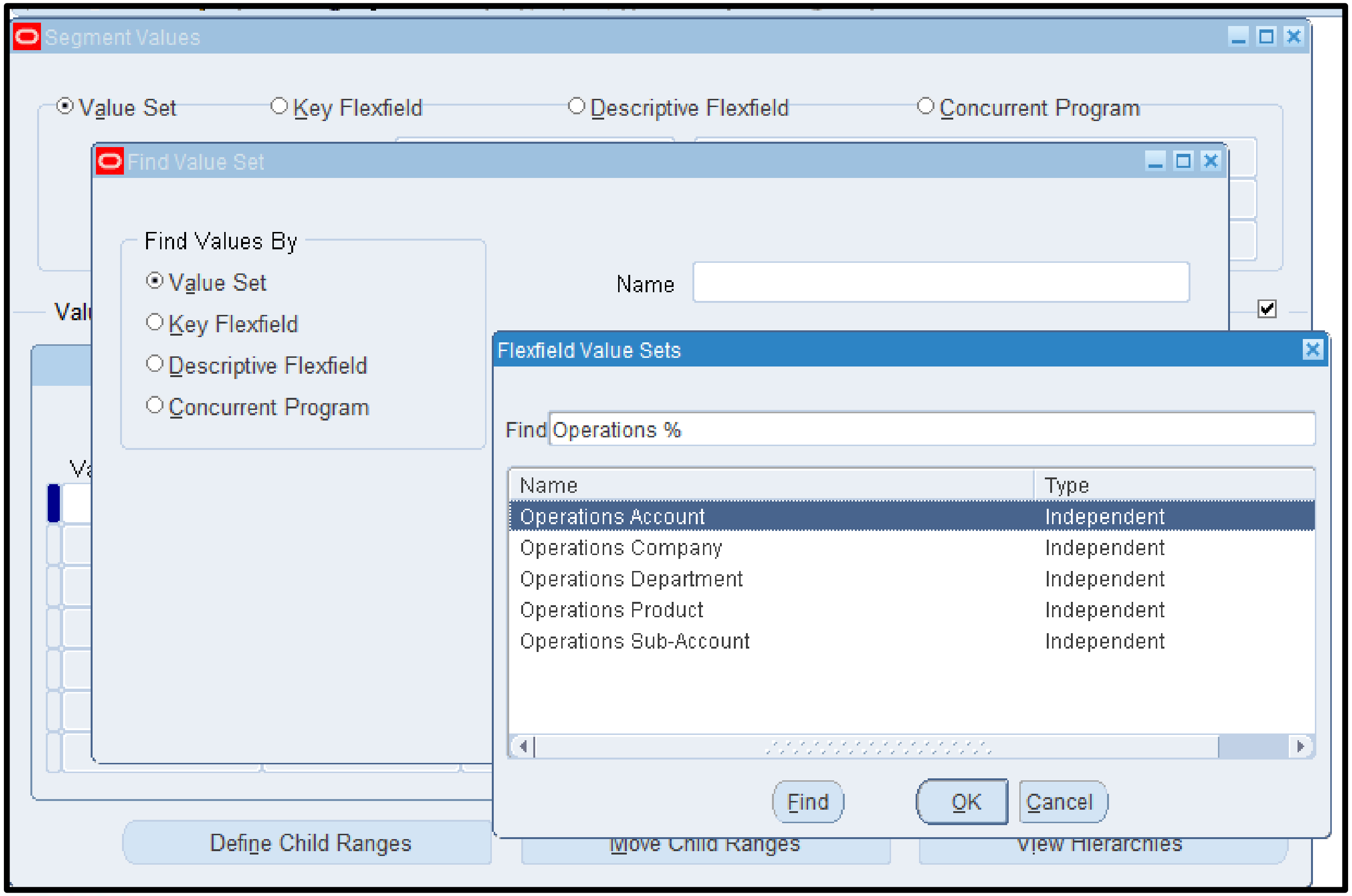
- Seeded permission sets for function security for flexfields



Select	Quick Select	Name △▽	Code △▽	Type △▽	Description △▽
○		Flexfield Value Set Security Insert Set	FND_FLEX_VSET_INSERT_PS	Permission Set	Allow insert of values into a value set
○		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
○		Flexfield Value Set Security Update Set	FND_FLEX_VSET_UPDATE_PS	Permission Set	Allow update of values in a value set
○		Flexfield Value Set Security View Only Set	FND_FLEX_VSET_VIEW_ONLY_PS	Permission Set	Allow viewing (only) of values in a value set

Results

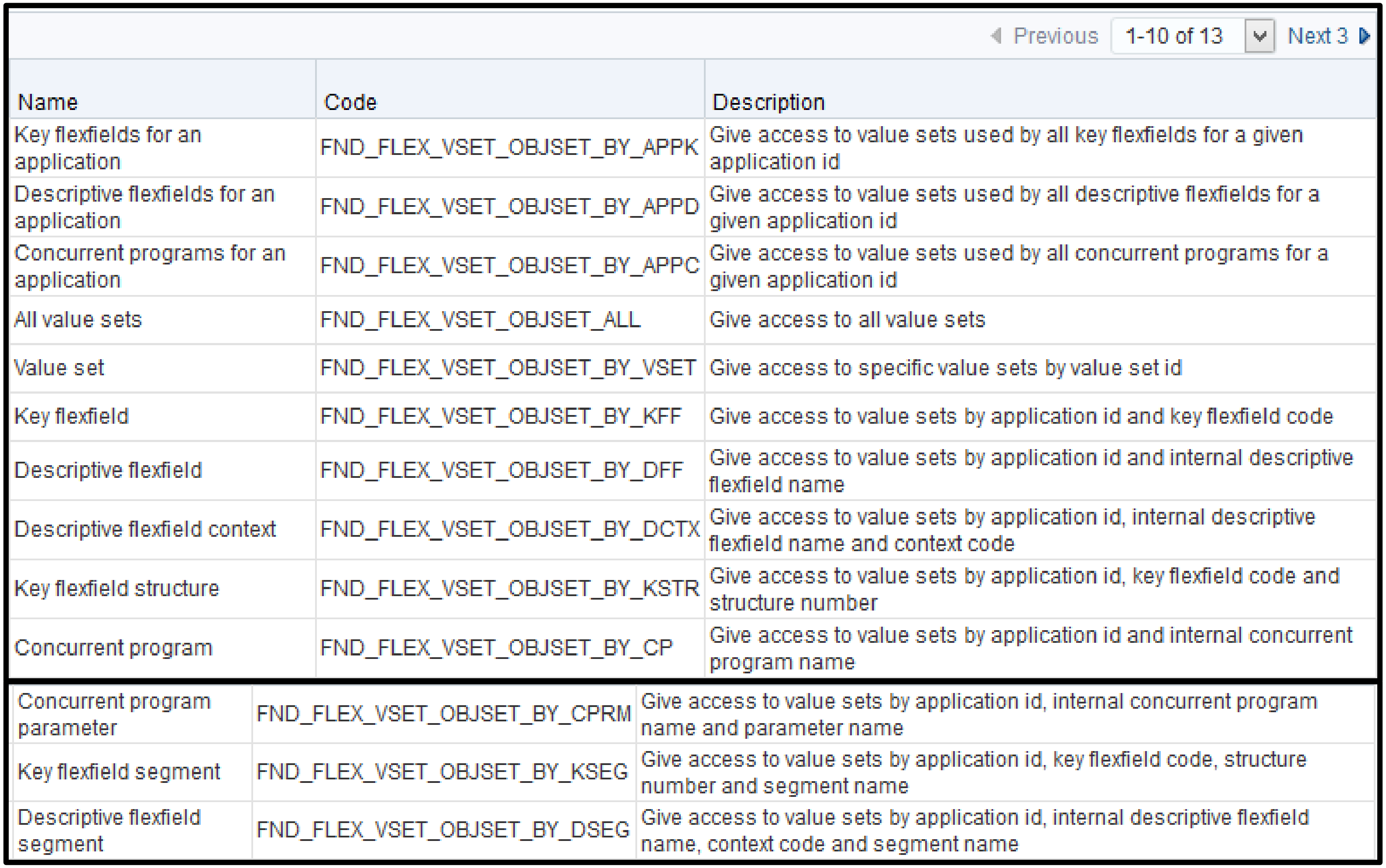
- Now I have access to all the value sets for the accounting flexfield



Find Operations %

Name	Type
Operations Account	Independent
Operations Company	Independent
Operations Department	Independent
Operations Product	Independent
Operations Sub-Account	Independent

Other Related Data Security Instance Sets

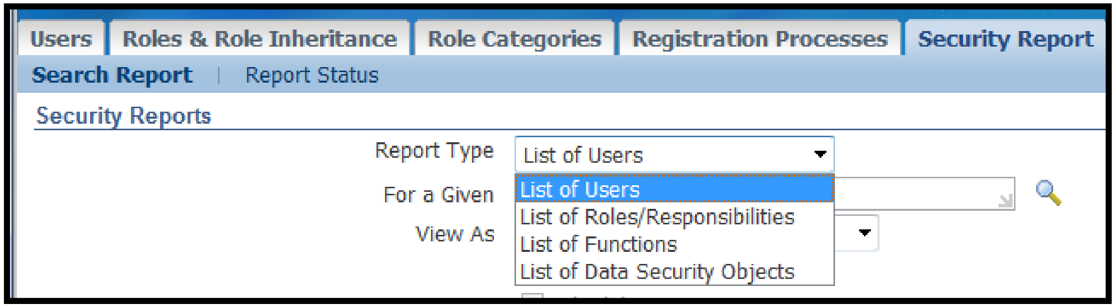


Name	Code	Description
Key flexfields for an application	FND_FLEX_VSET_OBJSET_BY_APPK	Give access to value sets used by all key flexfields for a given application id
Descriptive flexfields for an application	FND_FLEX_VSET_OBJSET_BY_APPD	Give access to value sets used by all descriptive flexfields for a given application id
Concurrent programs for an application	FND_FLEX_VSET_OBJSET_BY_APPC	Give access to value sets used by all concurrent programs for a given application id
All value sets	FND_FLEX_VSET_OBJSET_ALL	Give access to all value sets
Value set	FND_FLEX_VSET_OBJSET_BY_VSET	Give access to specific value sets by value set id
Key flexfield	FND_FLEX_VSET_OBJSET_BY_KFF	Give access to value sets by application id and key flexfield code
Descriptive flexfield	FND_FLEX_VSET_OBJSET_BY_DFF	Give access to value sets by application id and internal descriptive flexfield name
Descriptive flexfield context	FND_FLEX_VSET_OBJSET_BY_DCTX	Give access to value sets by application id, internal descriptive flexfield name and context code
Key flexfield structure	FND_FLEX_VSET_OBJSET_BY_KSTR	Give access to value sets by application id, key flexfield code and structure number
Concurrent program	FND_FLEX_VSET_OBJSET_BY_CP	Give access to value sets by application id and internal concurrent program name
Concurrent program parameter	FND_FLEX_VSET_OBJSET_BY_CPRM	Give access to value sets by application id, internal concurrent program name and parameter name
Key flexfield segment	FND_FLEX_VSET_OBJSET_BY_KSEG	Give access to value sets by application id, key flexfield code, structure number and segment name
Descriptive flexfield segment	FND_FLEX_VSET_OBJSET_BY_DSEG	Give access to value sets by application id, internal descriptive flexfield name, context code and segment name

Security Reports

Security Reports

- User Management→Security Reports→Search Reports Tab
  - Choose Report Type - screen changes by type



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

Search Report | Report Status

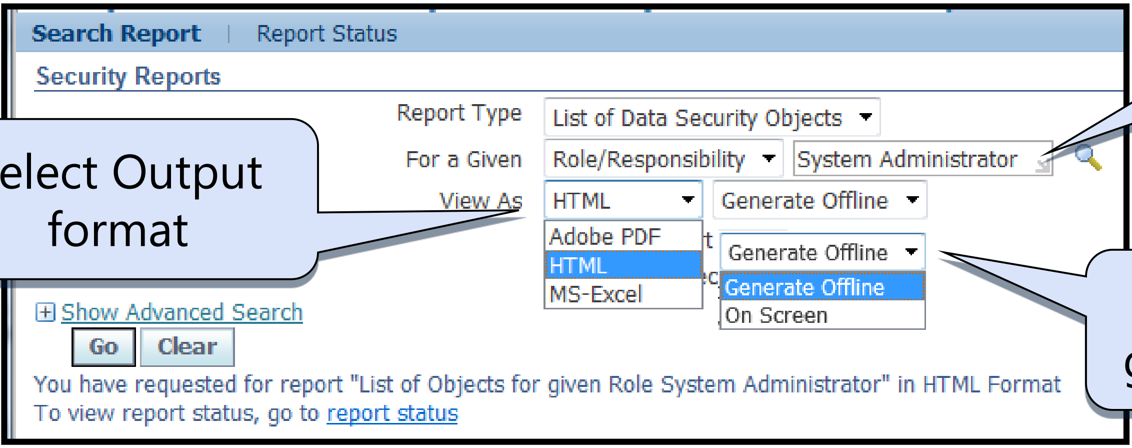
Security Reports

Report Type: List of Users

For a Given

View As

List of Users
List of Roles/Responsibilities
List of Functions
List of Data Security Objects



Search Report | Report Status

Security Reports

Report Type: List of Data Security Objects

For a Given: Role/Responsibility | System Administrator

View As: HTML | Generate Offline

Adobe PDF
HTML
MS-Excel

Generate Offline
On Screen

⊞ Show Advanced Search

Go | Clear

You have requested for report "List of Objects for given Role System Administrator" in HTML Format
To view report status, go to report status

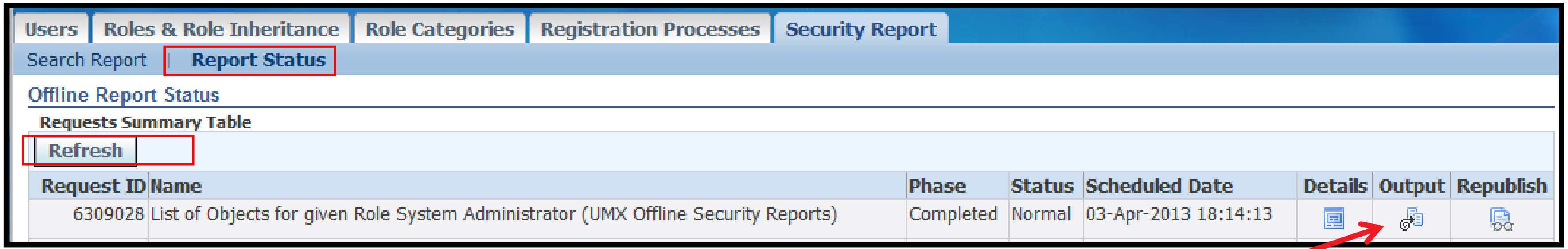
MUST specify Role/Responsibility

Select Output format

Choose Offline to get underlying SQL

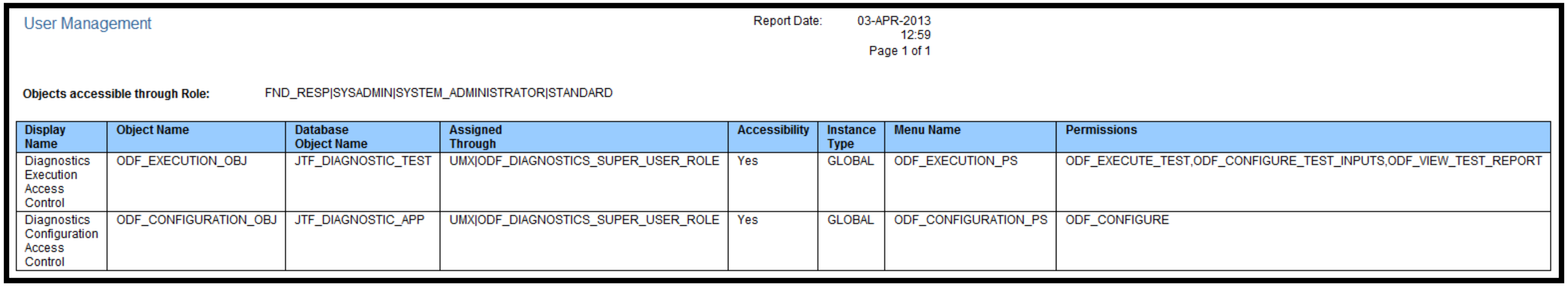
Security Reports

- Report Status Tab – Click Refresh



Request ID	Name	Phase	Status	Scheduled Date	Details	Output	Republish
6309028	List of Objects for given Role System Administrator (UMX Offline Security Reports)	Completed	Normal	03-Apr-2013 18:14:13			

- Then Click Output icon



User Management

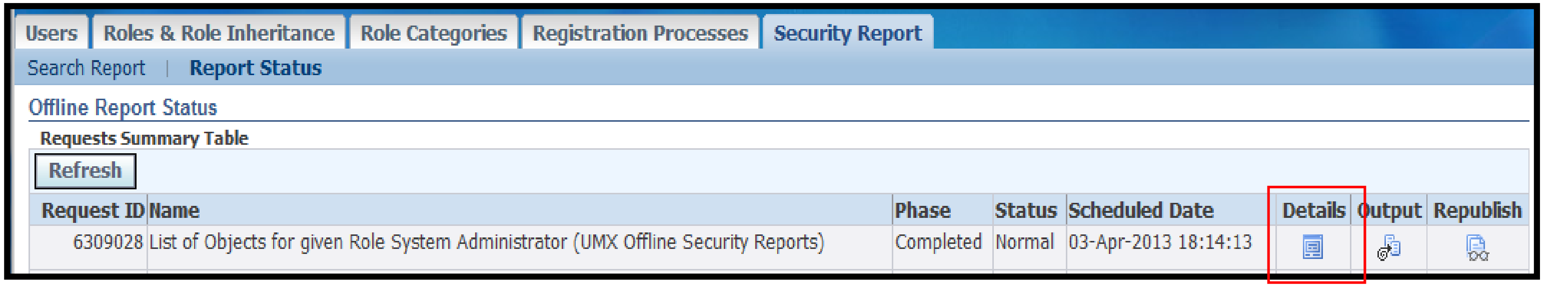
Report Date: 03-APR-2013
12:59
Page 1 of 1

Objects accessible through Role: FND_RESP|SYSADMIN|SYSTEM_ADMINISTRATOR|STANDARD

Display Name	Object Name	Database Object Name	Assigned Through	Accessibility	Instance Type	Menu Name	Permissions
Diagnostics Execution Access Control	ODF_EXECUTION_OBJ	JTF_DIAGNOSTIC_TEST	UMX|ODF_DIAGNOSTICS_SUPER_USER_ROLE	Yes	GLOBAL	ODF_EXECUTION_PS	ODF_EXECUTE_TEST,ODF_CONFIGURE_TEST_INPUTS,ODF_VIEW_TEST_REPORT
Diagnostics Configuration Access Control	ODF_CONFIGURATION_OBJ	JTF_DIAGNOSTIC_APP	UMX|ODF_DIAGNOSTICS_SUPER_USER_ROLE	Yes	GLOBAL	ODF_CONFIGURATION_PS	ODF_CONFIGURE

Security Reports

- For Log (and query), click Details, then View Log

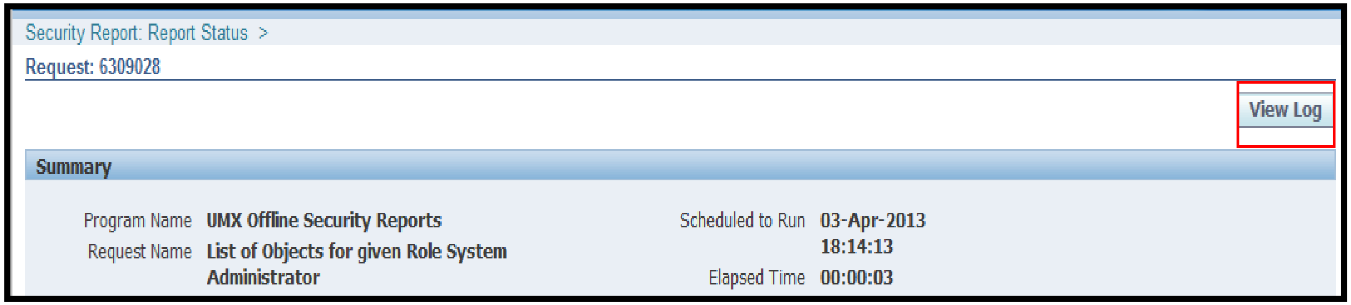


Offline Report Status

Requests Summary Table

Refresh

Request ID	Name	Phase	Status	Scheduled Date	Details	Output	Republish
6309028	List of Objects for given Role System Administrator (UMX Offline Security Reports)	Completed	Normal	03-Apr-2013 18:14:13			



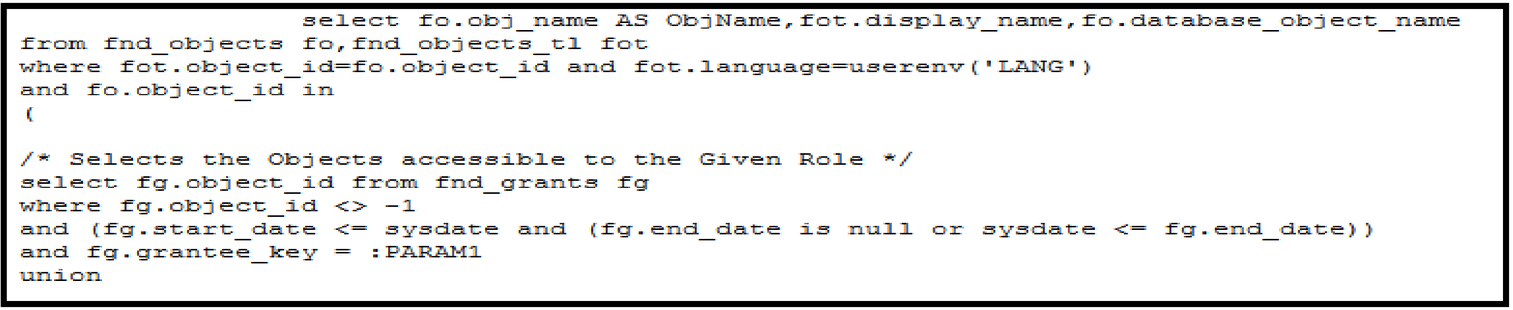
Request: 6309028

View Log

Summary

Program Name UMX Offline Security Reports
Request Name List of Objects for given Role System Administrator
Scheduled to Run 03-Apr-2013 18:14:13
Elapsed Time 00:00:03

Partial view of log



```
                 select fo.obj_name AS ObjName,fot.display_name,fo.database_object_name
from fnd_objects fo,fnd_objects_tl fot
where fot.object_id=fo.object_id and fot.language=userenv('LANG')
and fo.object_id in
(

/* Selects the Objects accessible to the Given Role */
select fg.object_id from fnd_grants fg
where fg.object_id <> -1
and (fg.start_date <= sysdate and (fg.end_date is null or sysdate <= fg.end_date))
and fg.grantee_key = :PARAM1
union
```

Poll Question

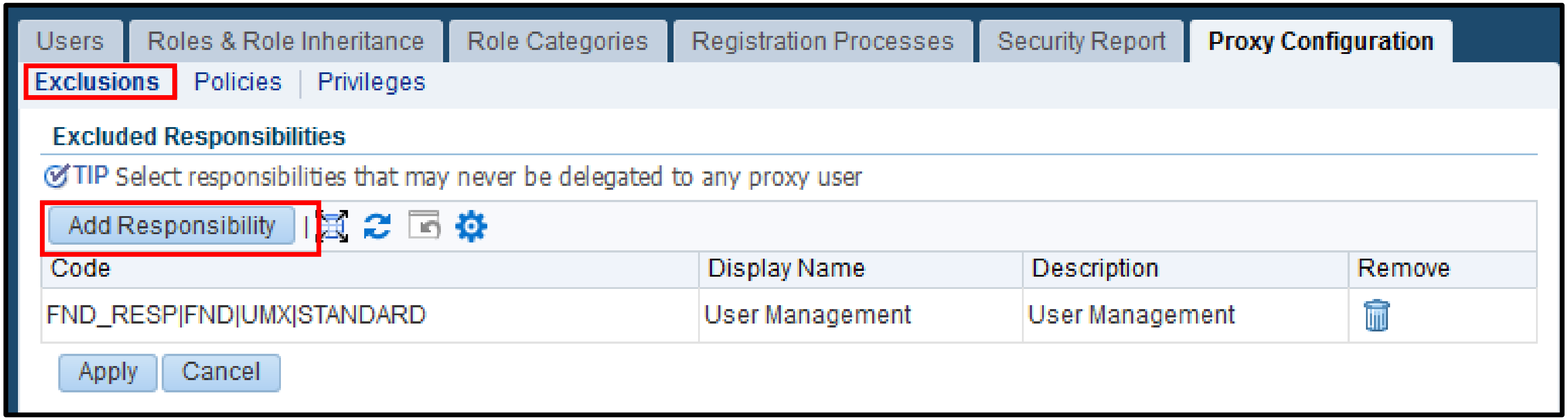
Proxy User Access Newest Features and Controls

Proxies

- Proxy authority can be granted to another user for a specific time period
  - Cover vacation/leave of absence/emergencies
- If you choose not to use this functionality, make sure you have good procedures for emergency access
  - The reality is the help desk or sysadmin uses override capabilities to get transactions pushed through which is a larger audit issue
- 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+ - Exclusions

- User Management → Proxy Configuration → Exclusions (What can be delegated)
  - Identify responsibilities which can never be delegated
    - Click the Add Responsibility button and add any responsibility that should never be delegated



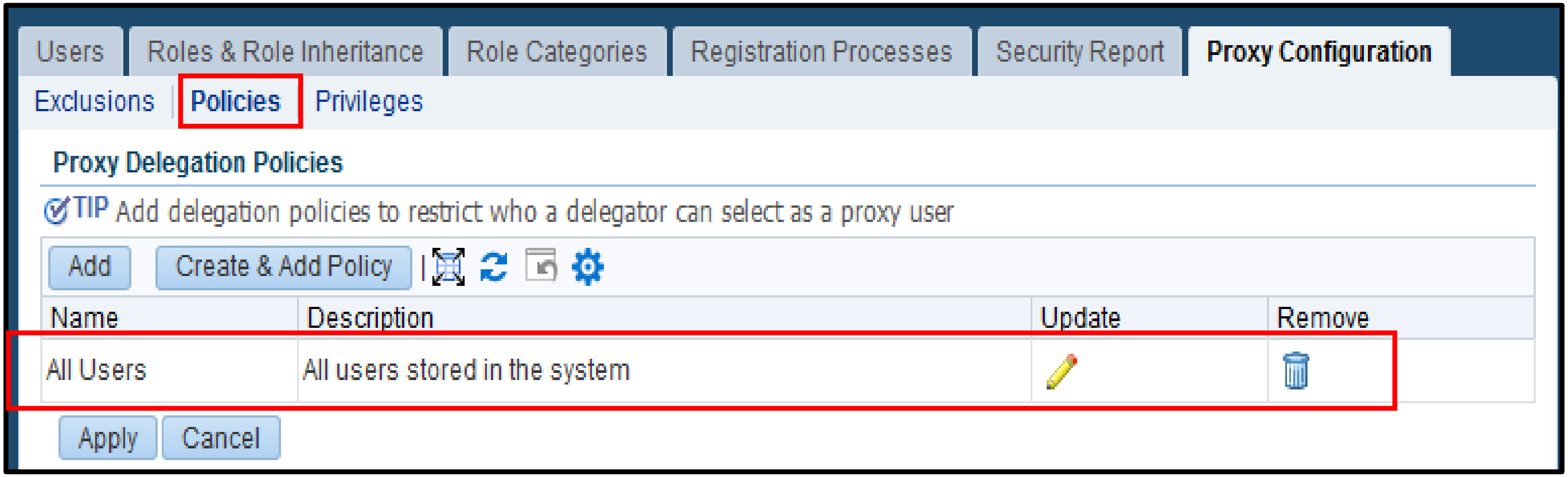
Excluded Responsibilities

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

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

Proxy Configuration – 12.2.4+ - Policies

- User Management → Proxy Configuration → Policies (Who can you delegate to?)
  - By default, you can delegate proxy access to any user which is an audit issue and should be removed



Proxy Delegation Policies

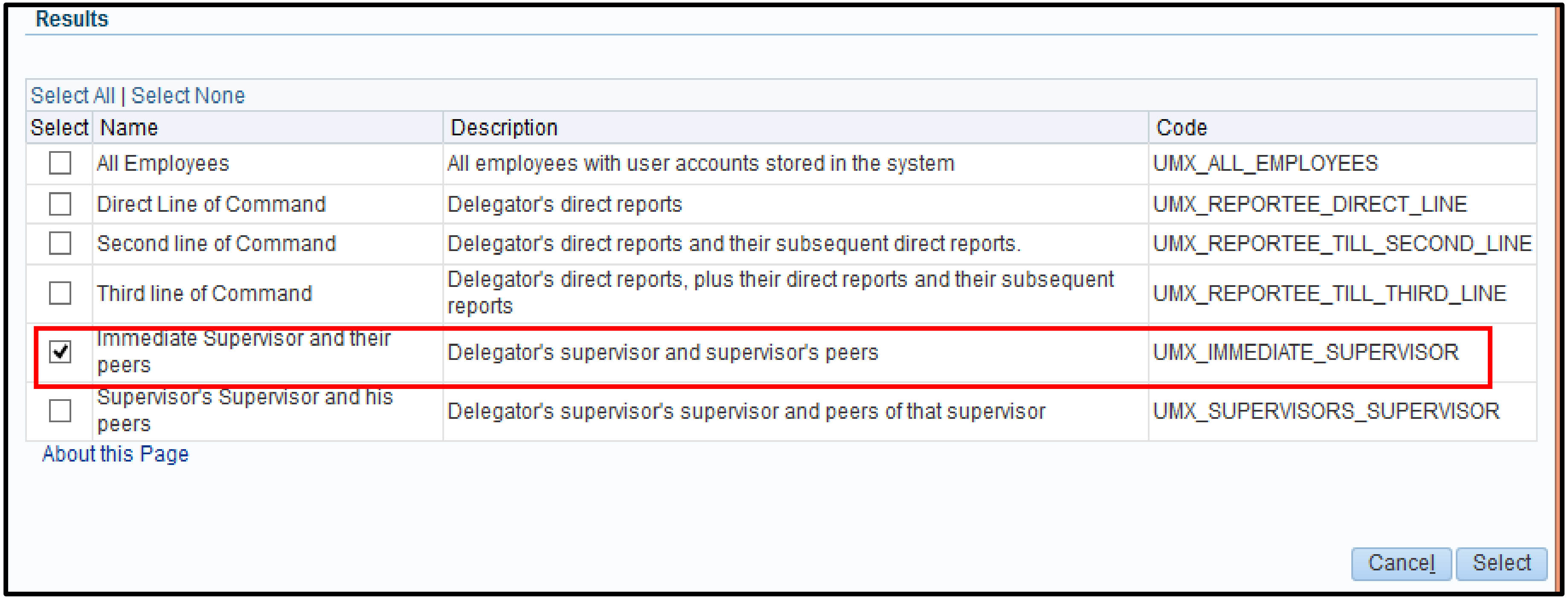
TIP Add delegation policies to restrict who a delegator can select as a proxy user

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

- In the next example, we will only allow a user to delegate only to their direct supervisor and peers of that supervisor

Proxy Configuration – 12.2.4+ - Policies

- Click the add button; Enter % to see all seeded policies
  - Check the policy desired and click the select button



Results

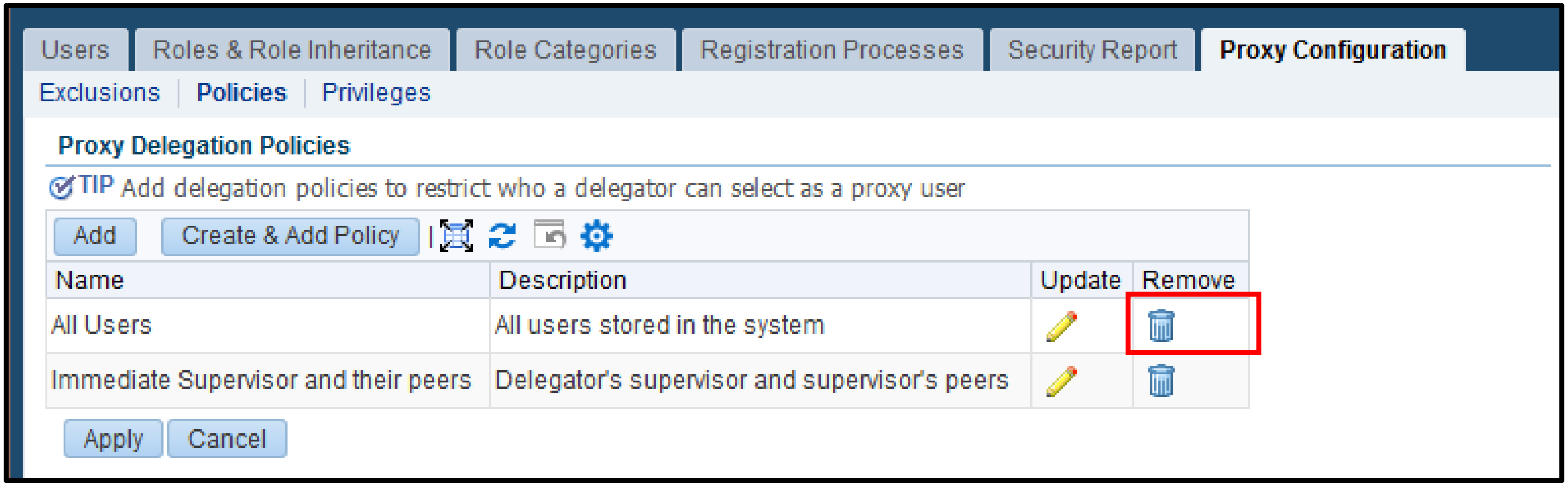
Select All | Select None

Select	Name	Description	Code
□	All Employees	All employees with user accounts stored in the system	UMX_ALL_EMPLOYEES
□	Direct Line of Command	Delegator's direct reports	UMX_REPORTEE_DIRECT_LINE
□	Second line of Command	Delegator's direct reports and their subsequent direct reports.	UMX_REPORTEE_TILL_SECOND_LINE
□	Third line of Command	Delegator's direct reports, plus their direct reports and their subsequent reports	UMX_REPORTEE_TILL_THIRD_LINE
☑	Immediate Supervisor and their peers	Delegator's supervisor and supervisor's peers	UMX_IMMEDIATE_SUPERVISOR
□	Supervisor's Supervisor and his peers	Delegator's supervisor's supervisor and peers of that supervisor	UMX_SUPERVISORS_SUPERVISOR

About this Page

Proxy Configuration – 12.2.4+ - Policies

- Click on the track can to remove the policy for All Users
  - Then click the Apply button
- Remember, you can also create a policy if the seeded policies do not meet your needs



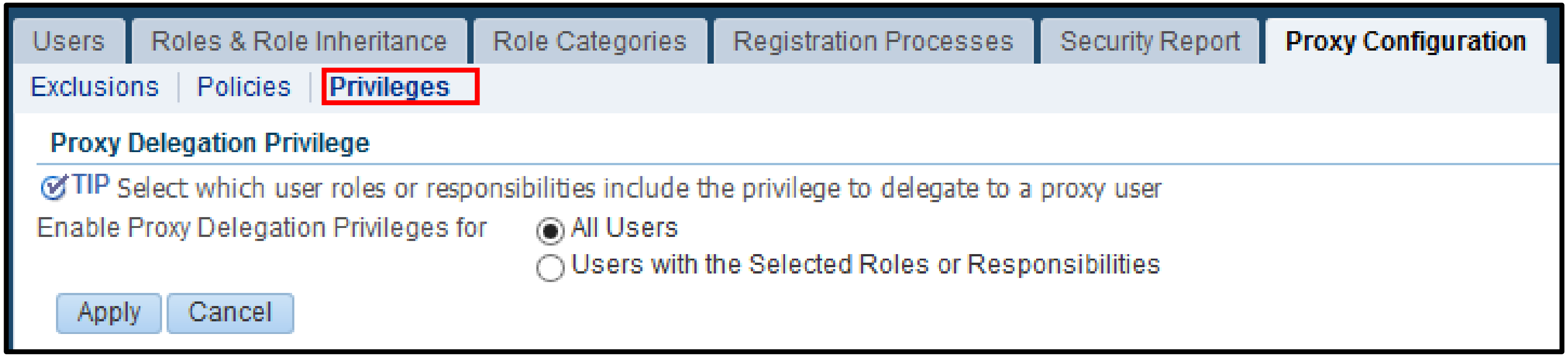
Proxy Delegation Policies

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

Name	Description	Update	Remove
All Users	All users stored in the system	✎	🗑
Immediate Supervisor and their peers	Delegator's supervisor and supervisor's peers	✎	🗑

Proxy Configuration – 12.2.4+ - Privileges

- User Management → Proxy Configuration → Privileges (Who can delegate)
  - Replace granting of "Manage Proxies" role through User Management
  - Grant proxy privileges to all users is the default in some releases
    - Not best practice!!! Please update!



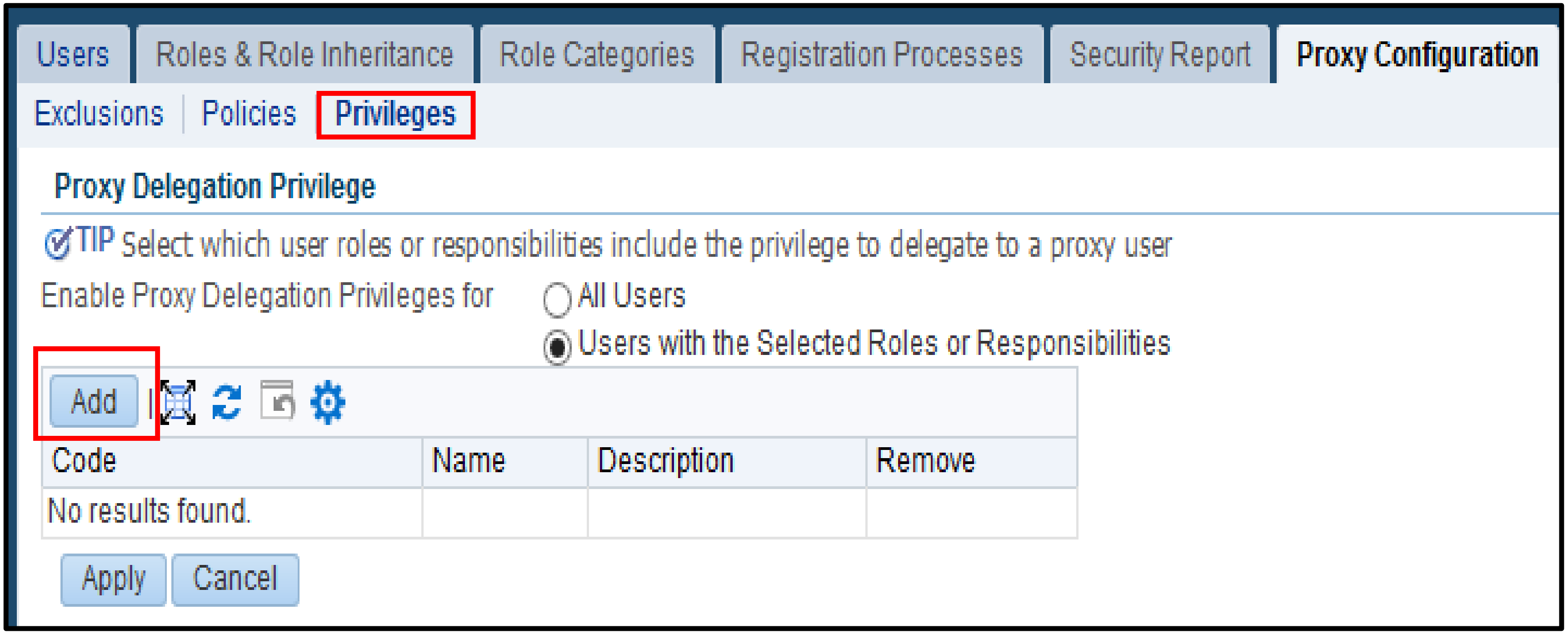
Proxy Delegation Privilege

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

Proxy Configuration – 12.2.4+ - Privileges

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



Proxy Delegation Privilege

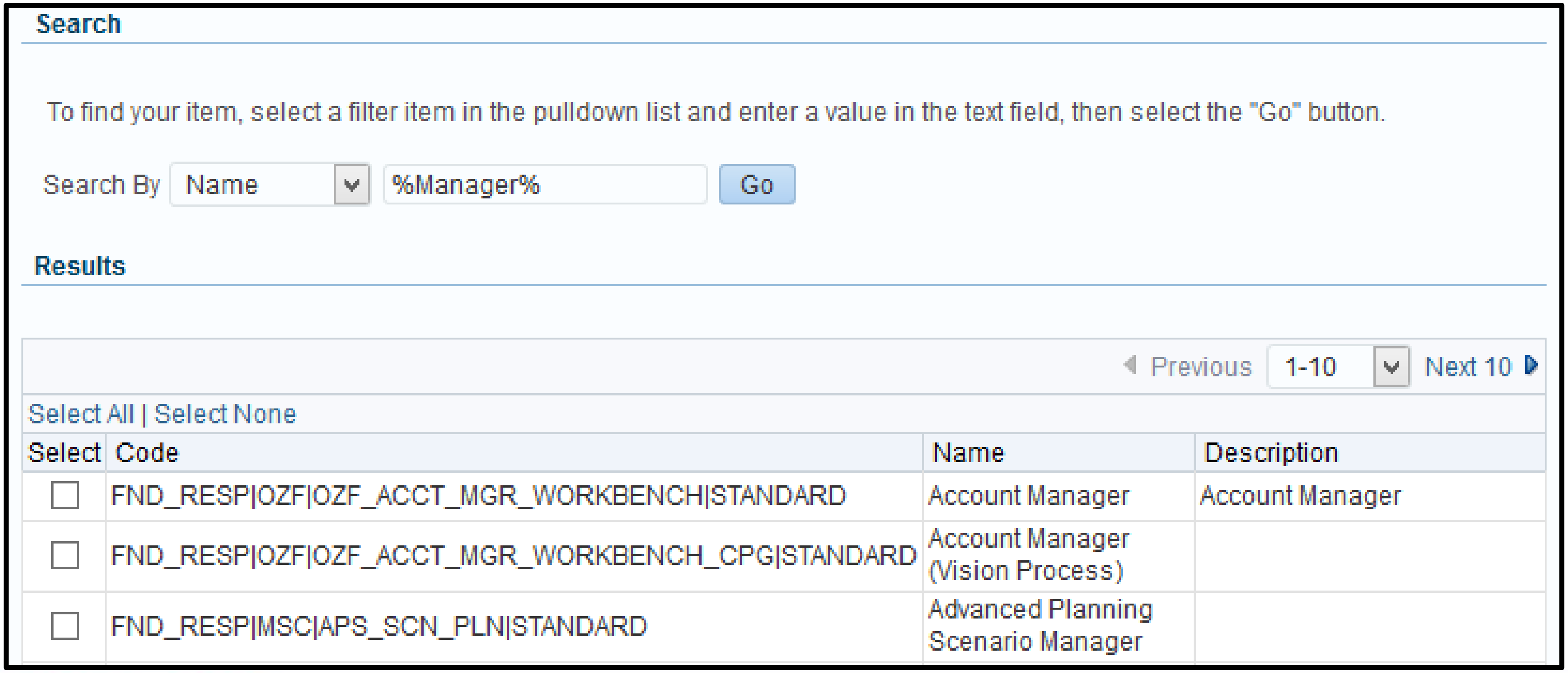
TIP Select which user roles or responsibilities include the privilege to delegate to a proxy user

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

Code	Name	Description	Remove
No results found.			

Proxy Configuration – 12.2.4+ - Privileges

- User Management → Proxy Configuration → Privileges
  - Search and choose the responsibility or role
    - Note the code for responsibilities start with FND_Resp; Roles start with UMX



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.

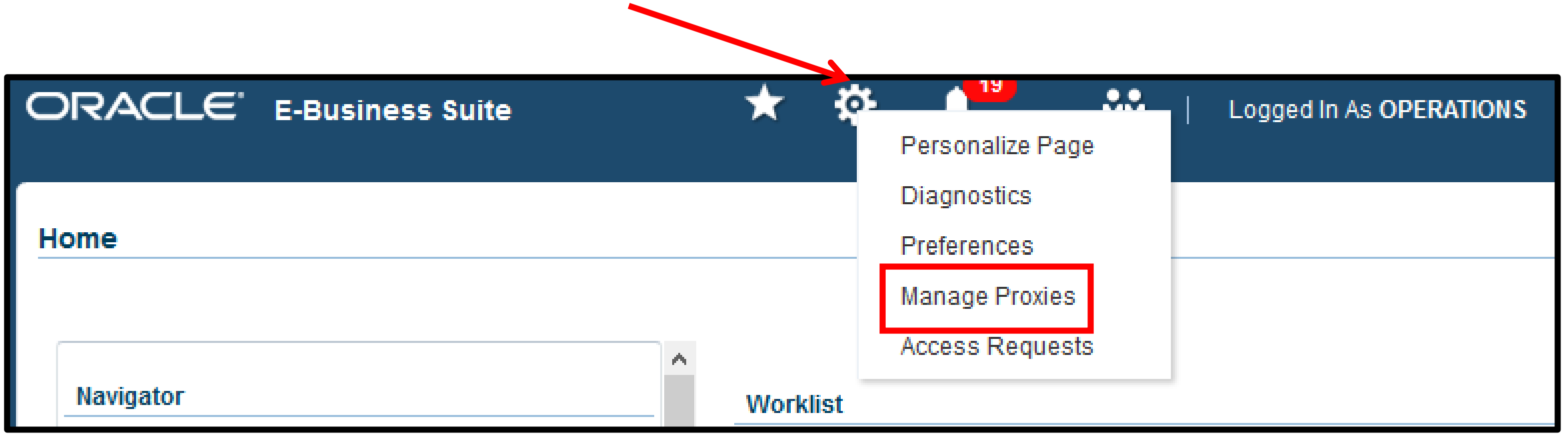
Search By: Name, %Manager%

Results

Select	Code	Name	Description
□	FND_RESP|OZF|OZF_ACCT_MGR_WORKBENCH|STANDARD	Account Manager	Account Manager
□	FND_RESP|OZF|OZF_ACCT_MGR_WORKBENCH_CPG|STANDARD	Account Manager (Vision Process)	
□	FND_RESP|MSC|APS_SCN_PLN|STANDARD	Advanced Planning Scenario Manager	

Proxies – 12.2.4+ - Granting proxy access

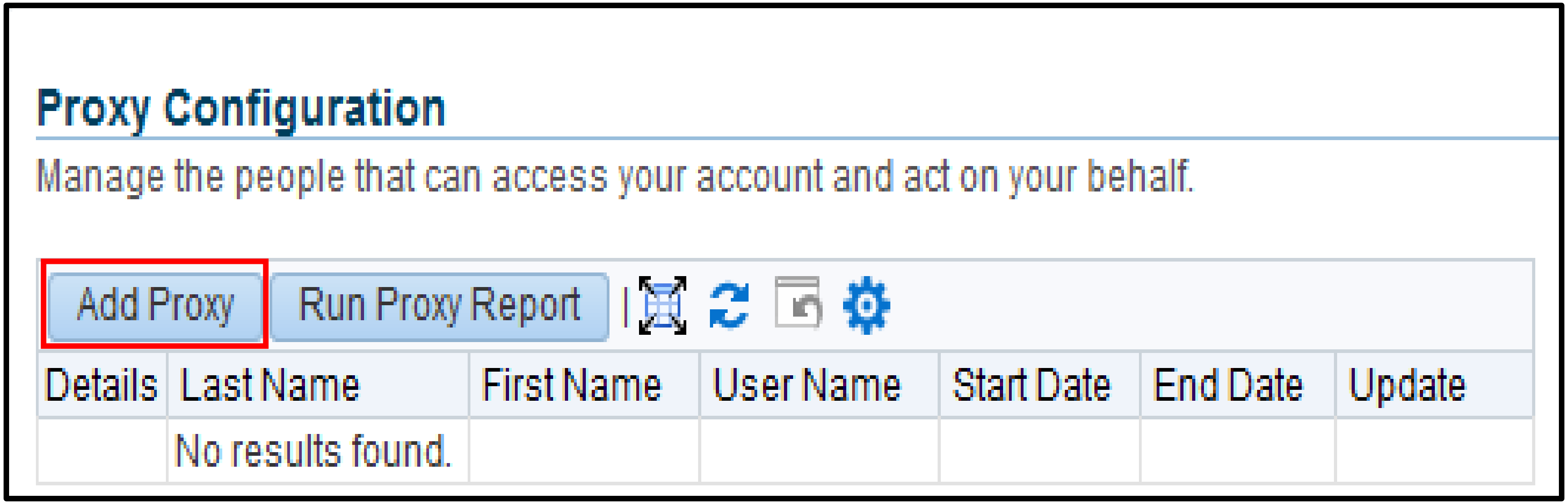
- Click the settings gear, then Manage Proxies



- Note: Clicking the settings gear, then Preferences will show the Manage Proxies option on the left similar to earlier releases

Proxies – 12.2.4+

- The Manage Proxies page looks only slightly different in 12.2.4
- Click the Add Proxy button
  - In early releases, this button is “Add People”



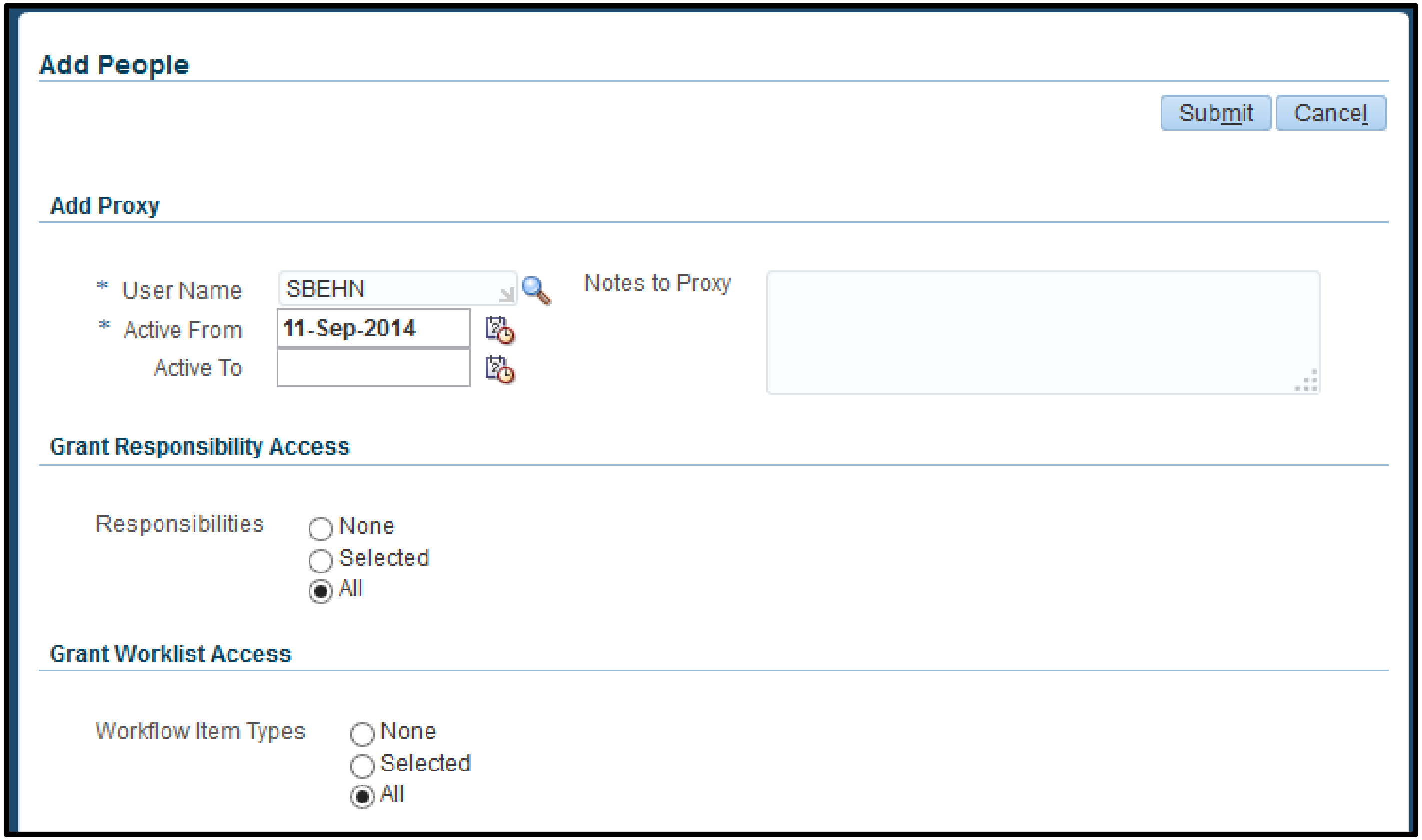
Proxy Configuration

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

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

Proxies – 12.2.4+

- Choose the user name, then choose the appropriate options for responsibility and workflow access



Add People

Add Proxy

* User Name: SBEHN

* Active From: 11-Sep-2014

Active To:

Notes to Proxy:

Grant Responsibility Access

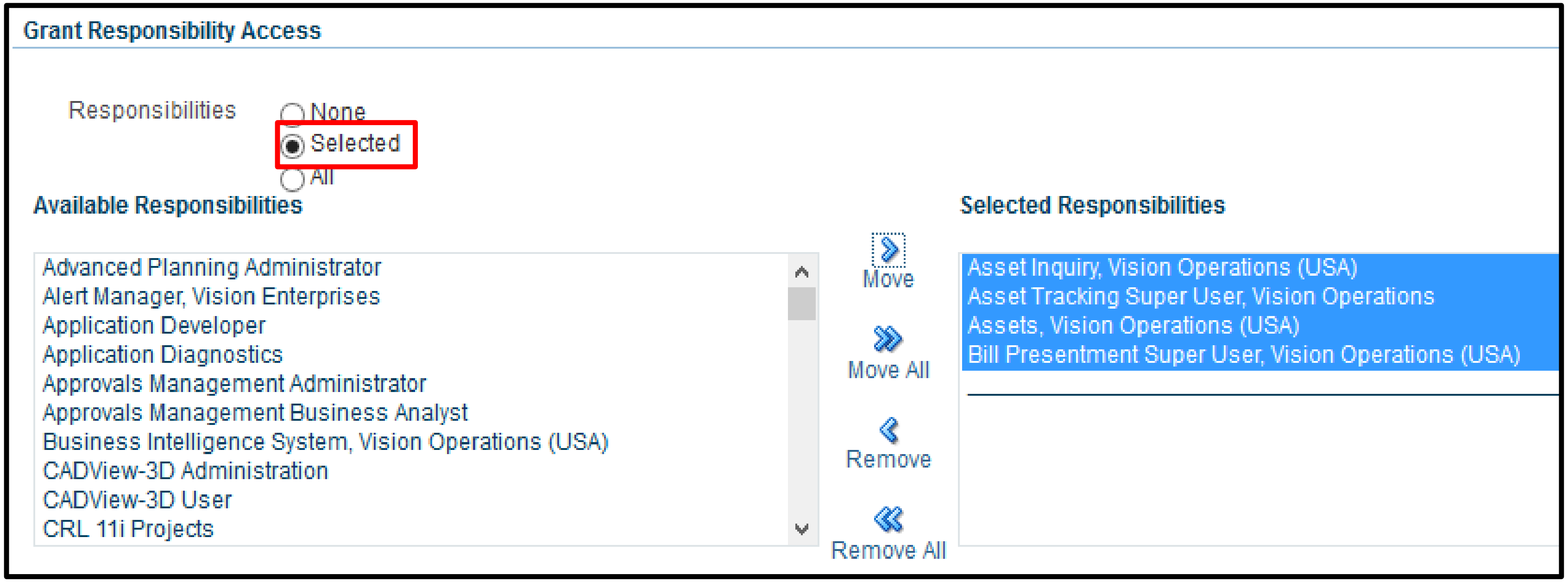
Responsibilities
○ None
○ Selected
● All

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 except those listed as exclusions earlier
  - Move the desired responsibilities from the available column to the selected column



Grant Responsibility Access

Responsibilities ○ None ● Selected ○ All

Available Responsibilities

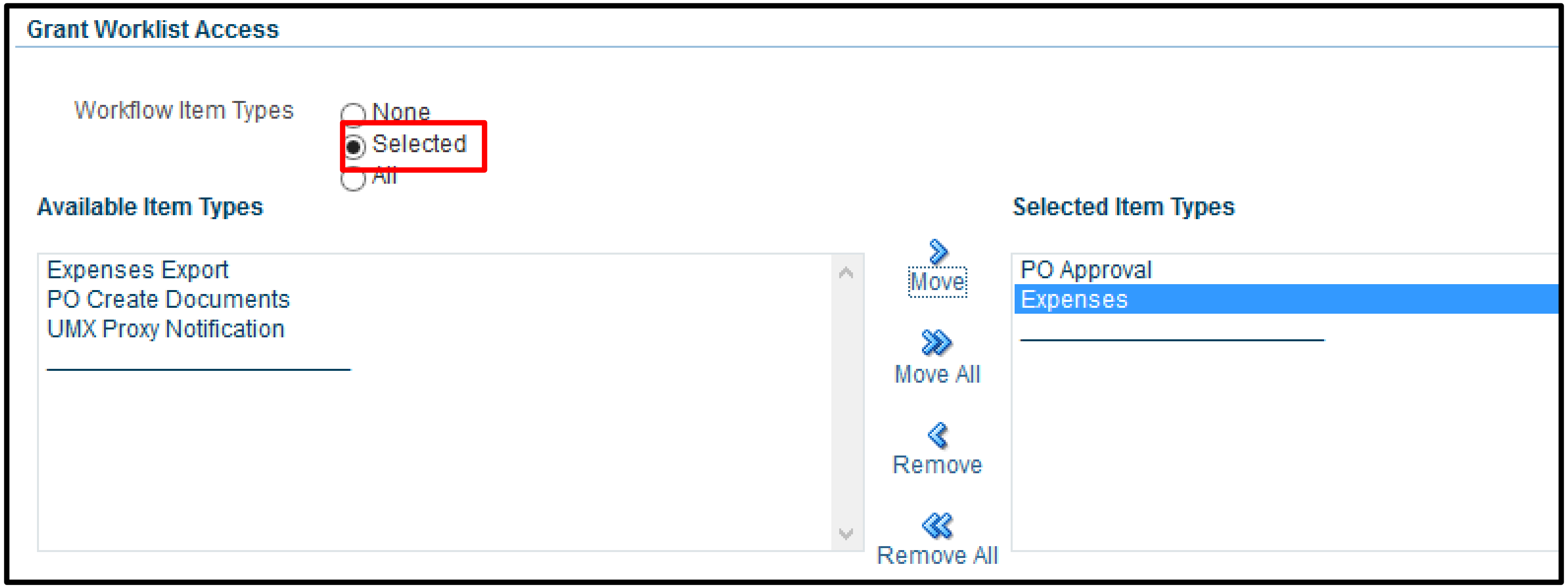
Advanced Planning Administrator
Alert Manager, Vision Enterprises
Application Developer
Application Diagnostics
Approvals Management Administrator
Approvals Management Business Analyst
Business Intelligence System, Vision Operations (USA)
CADView-3D Administration
CADView-3D User
CRL 11i Projects

Selected Responsibilities

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

Proxies – 12.2.4+

- To grant selected worklist access, click the Selected radio button and all current workflow item types will appear except those in the exclusion list
  - Move the desired item types from the available column to the selected column
    - Note: Add valid workflow item types to Lookup Type WF: Vacation Rule Item Types



Grant Worklist Access

Workflow Item Types ○ None ● Selected ○ All

Available Item Types

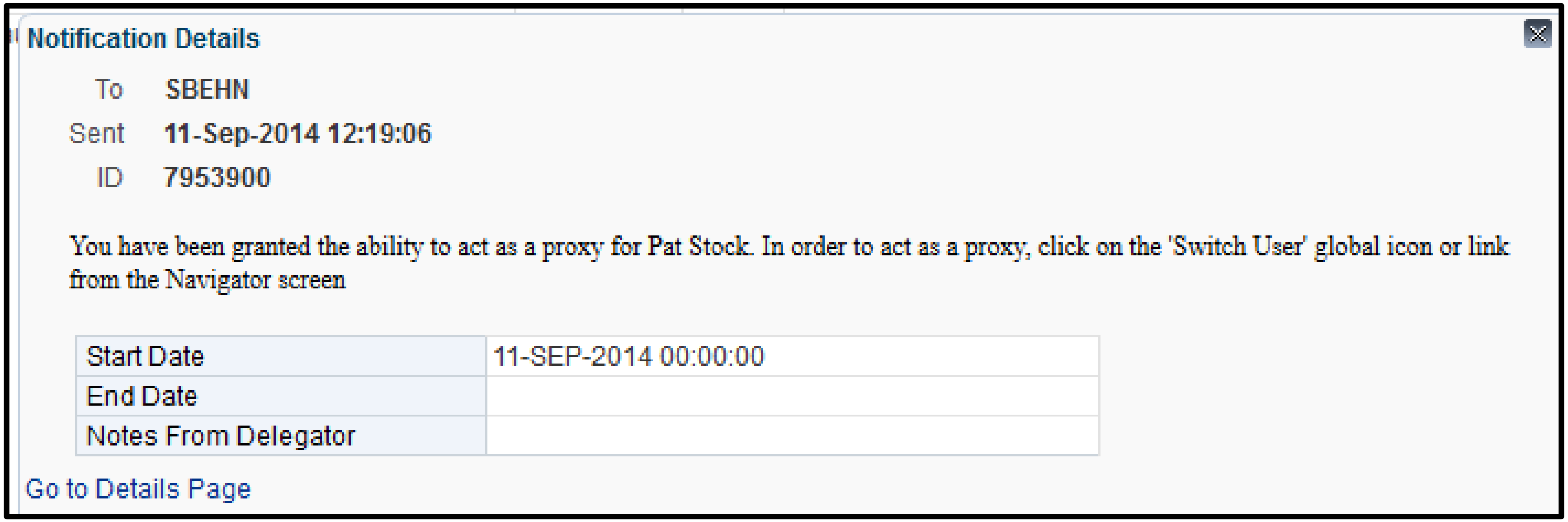
Expenses Export
PO Create Documents
UMX Proxy Notification

Selected Item Types

PO Approval
Expenses

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

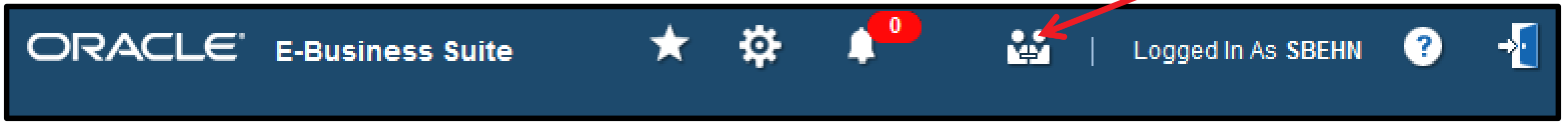
You have been granted the ability to act as a proxy for Pat Stock. In order to act as a proxy, click on the 'Switch User' global icon or link from the Navigator screen

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

Go to Details Page

Proxies – 12.2.4+

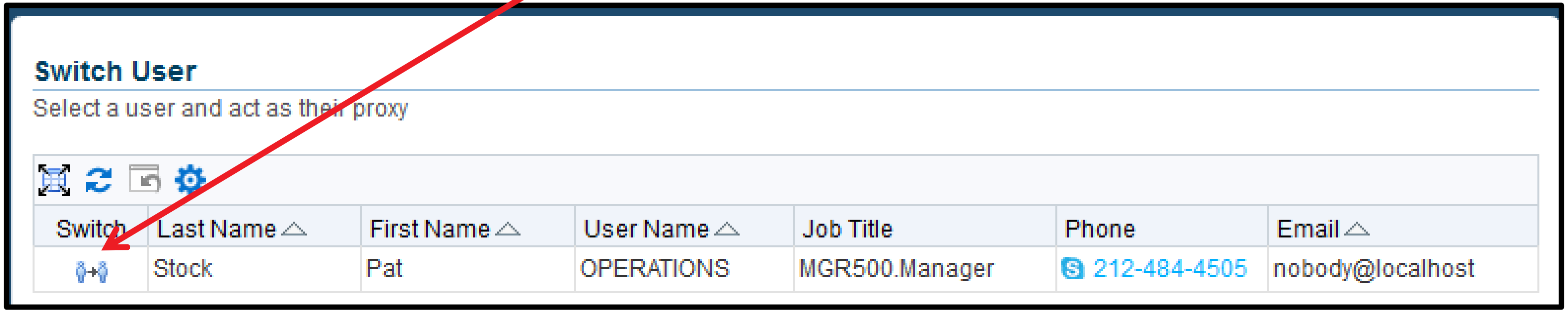
- As the SBEHN user, click the switch user icon



ORACLE E-Business Suite

Logged In As SBEHN

- Then click the switch icon



Switch User

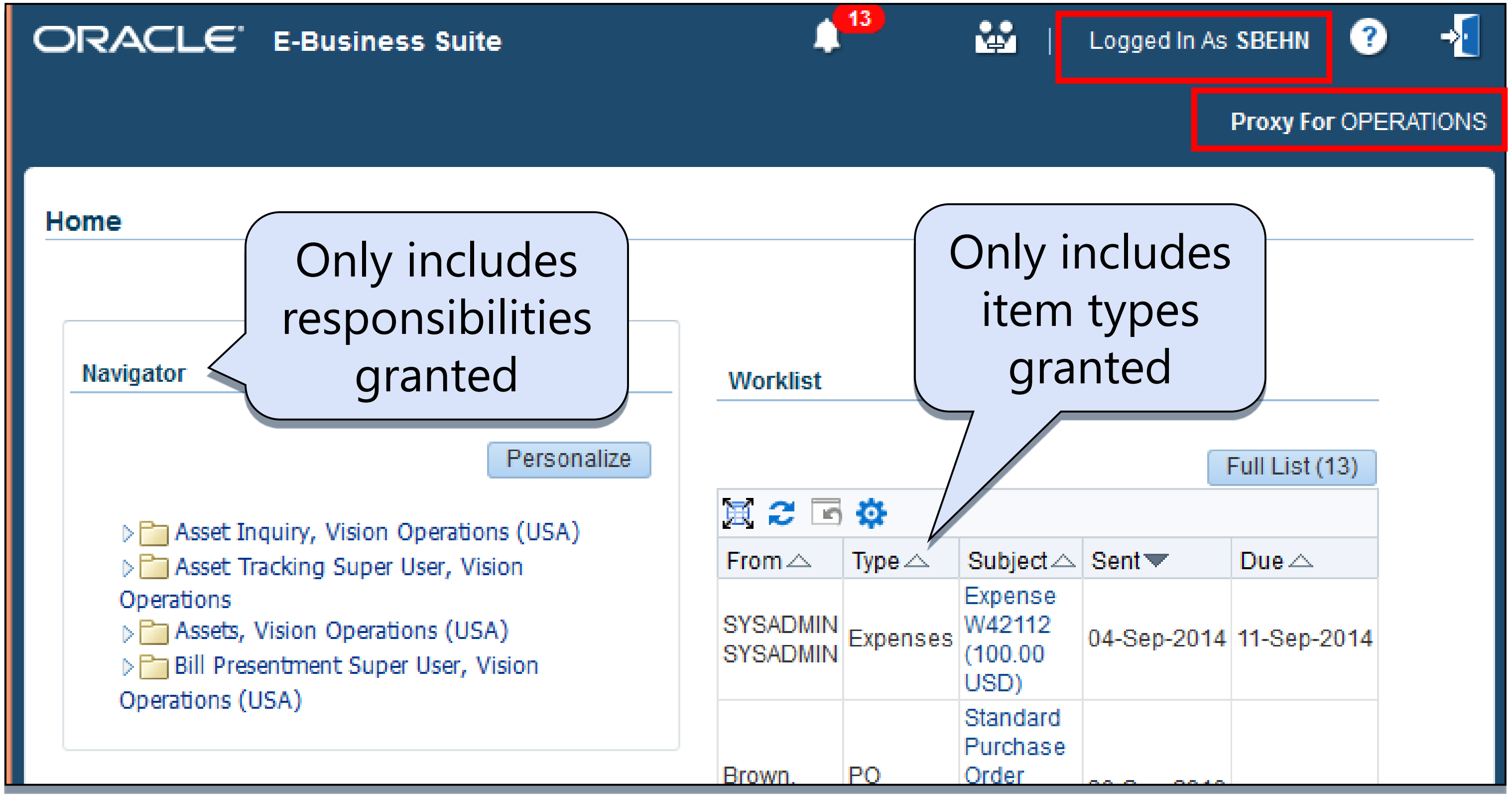
Select a user and act as their proxy

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

- Note: Apply patch 20771787 to fix bug if “switch user” icon is missing
  - Switch User Button Missing on Notification after Worklist Access Proxy Setup In 12.2.4 (Doc ID 2039781.1)

Proxies – 12.2.4+

- Now logged in as SBEHN as Proxy for Operations



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

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

References

- Oracle Applications System Administrator's Guide - Security
- See Oracle User Management Developer Guide
- My Oracle Support ID: 553547.1 – Data Security Terminology
- My Oracle Support ID: 553290.1 – Introduction to the Grants Security System and Data Security
- E-Business Suite User Management SIG
  - http://ebsumx.oaug.org/
- Proxy User Training
  http://ilearning.oracle.com/ilearn/en/learner/jsp/offering_details_find.jsp?classid=1524577857
- Release 12.2.3 "Oracle® E-Business Suite Flexfields Guide, Release 12.2" Part No. E22963-07
- Flexfield Value Set Security Training
  http://oukc.oracle.com/static12/opn/login/?t=checkusercookies%7Cr=-1%7Cc=1362916480

Contact

Susan Behn
Vice President
susan.behn@infosemantics.com

Infosemantics, Inc.
www.infosemantics.com

Join our conversation with #EBSVC16

Thank you for attending the EBS Answers Virtual Conference.

Please be sure to visit the exhibitor showcase to meet with EBS solution providers, and enter for a chance to win giveaways!

EBS Answers
Virtual Conference