Wizarding with EBS Security Wizards and Proxy Users

User Management Training Part II

January, 2020

Susan Behn

ORACLE ACE Director

Infosemantics℠
People first. Driving solutions together.

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

Inc. 5000

siTech20 2017
20 Most Promising Technology Companies

SR 2017 50 Fastest Growing Companies Of The Year

CIO 20 Most Promising Oracle Review Solution Providers - 2018

Best and Brightest Companies to Work For in the Nation WINNER 2018 & 2017

Dallas/Fort Worth's Best and Brightest Companies to Work For WINNER 2019 & 2018

Infosemantics℠

ORACLE Gold Partner

snowflake Certified Partner

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

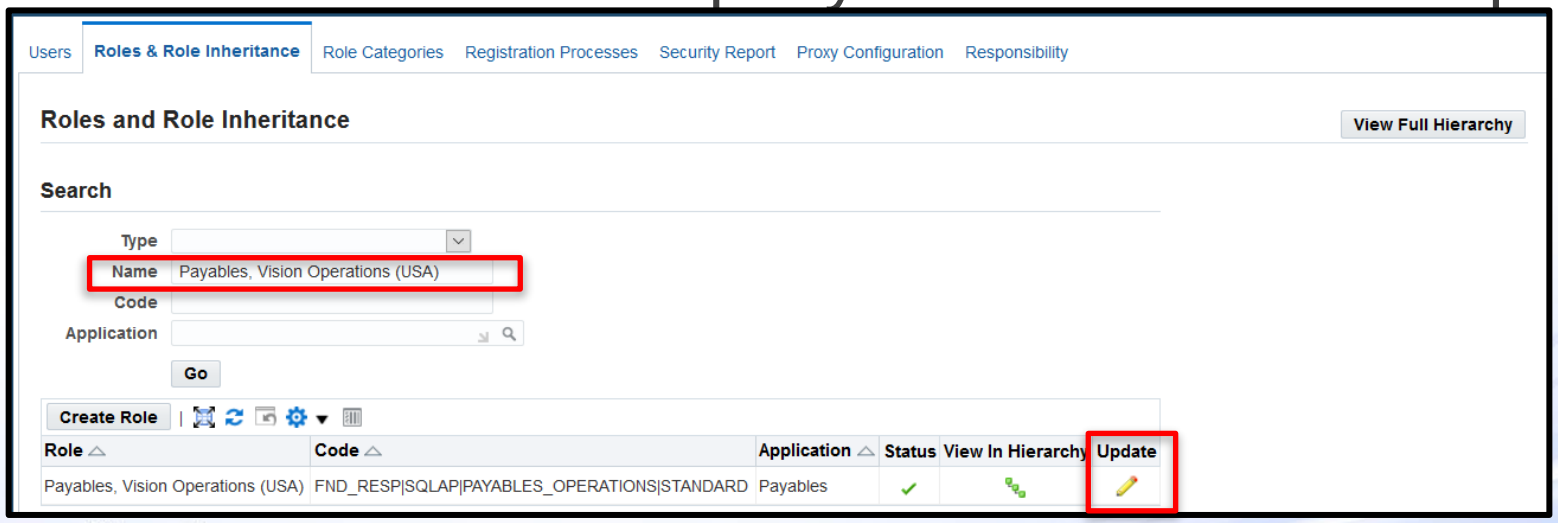
      Select * from wf_local_roles
      where partition_id = 13;

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

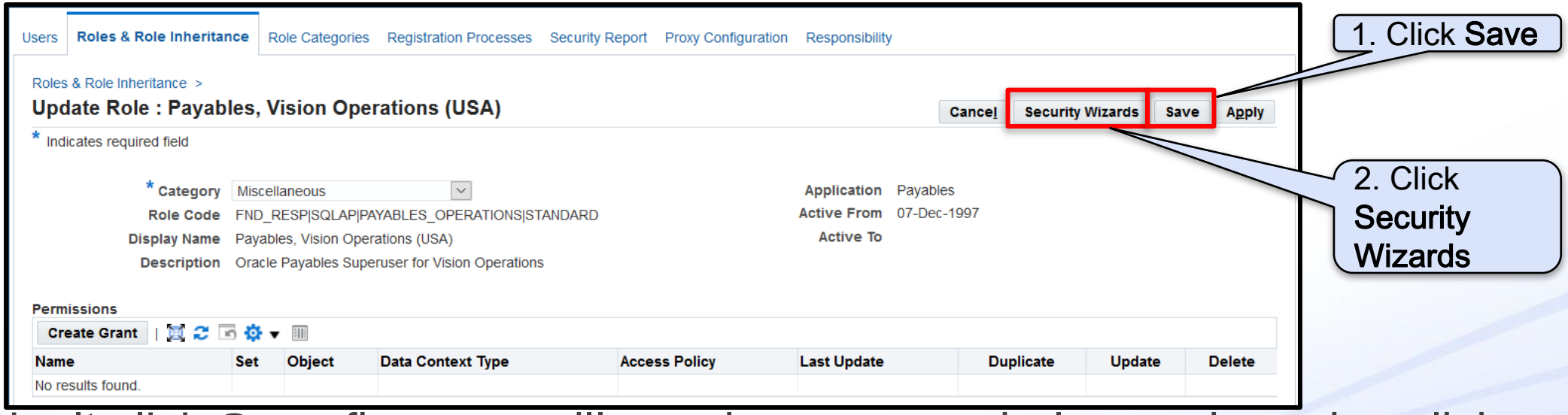
How to Access Wizards

- 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



How to Access Wizards

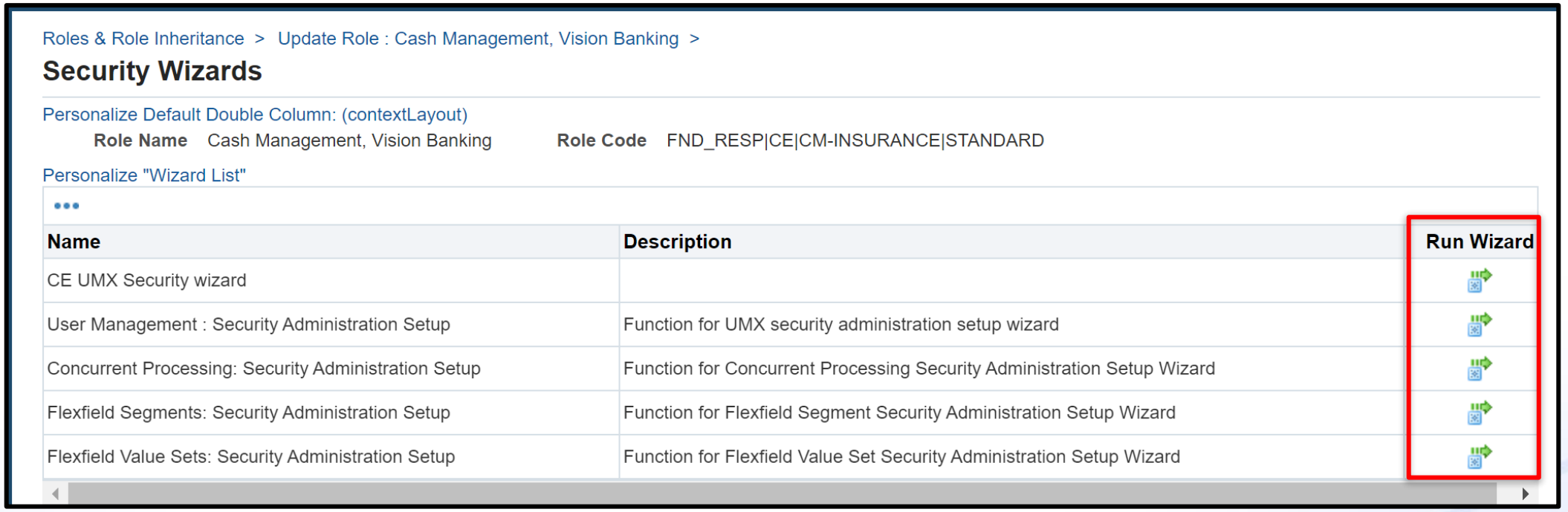
- If any grants exist for the role, they will display under Permissions
- To run a wizard, click **Save**, then click **Security Wizards**
  - When you click **Save**, you will get a warning that updates require Background Engine to run



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

How to Access the Wizards

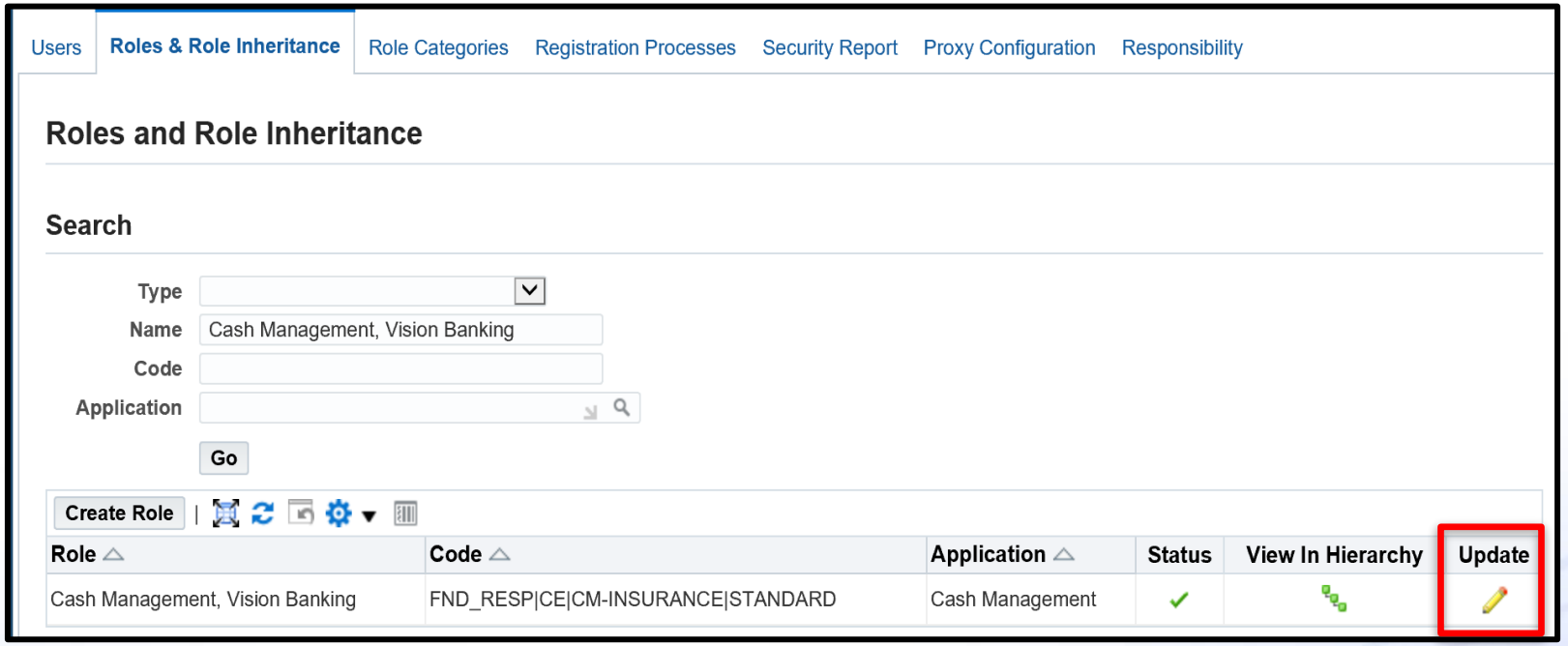
- Click the icon in the **Run Wizard** column



Cash Management Security Wizard

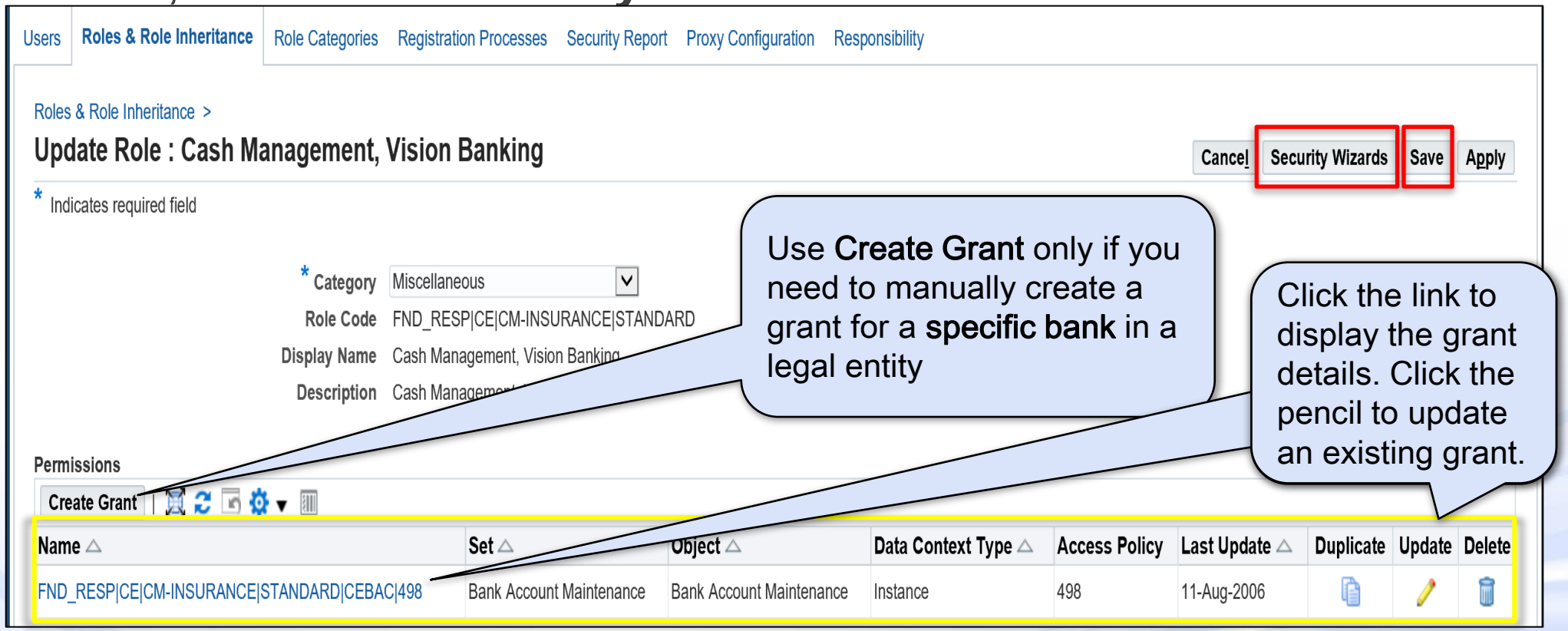
Cash Management Security Wizard

- 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



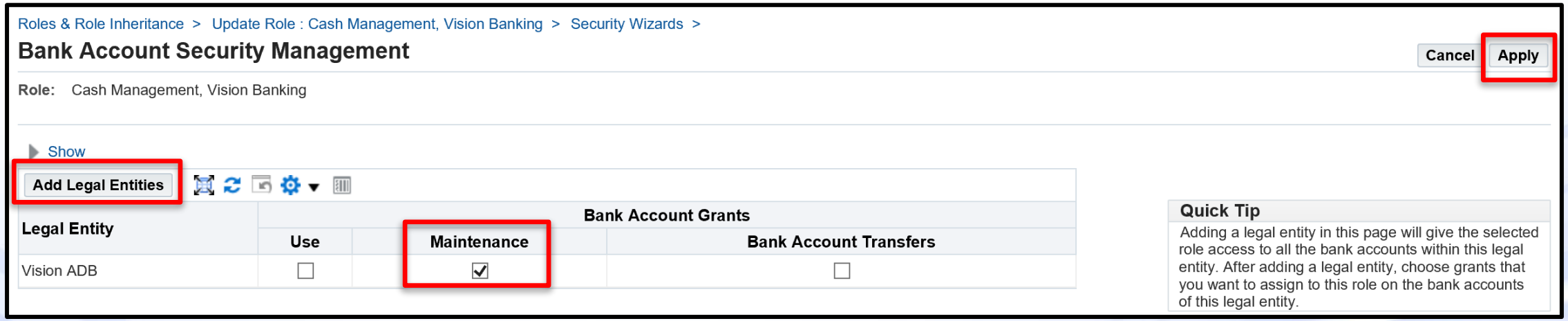
Cash Management Security Wizard

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



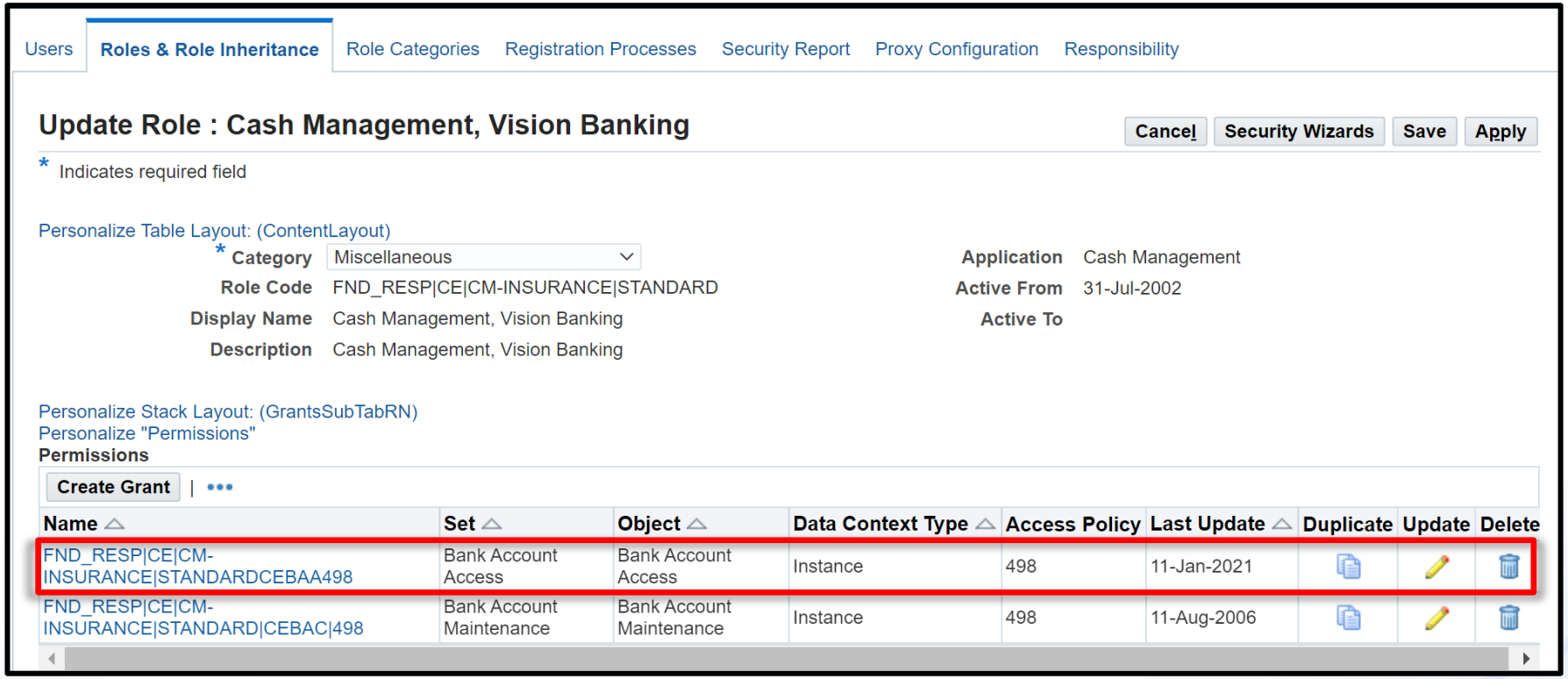
Cash Management Security Wizard

- 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



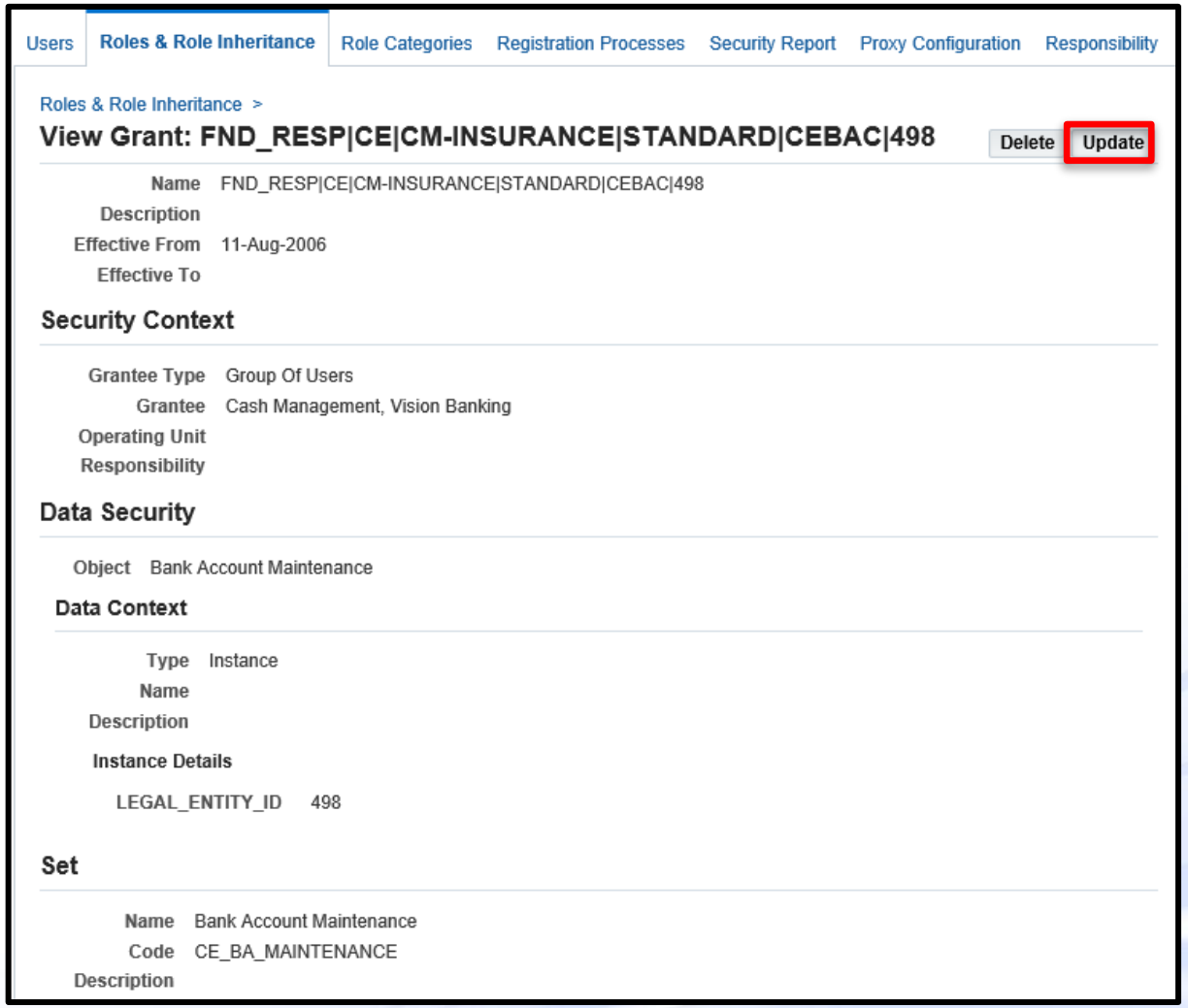
Cash Management Security Wizard

- New grant now appears



CE UMX Security Wizard

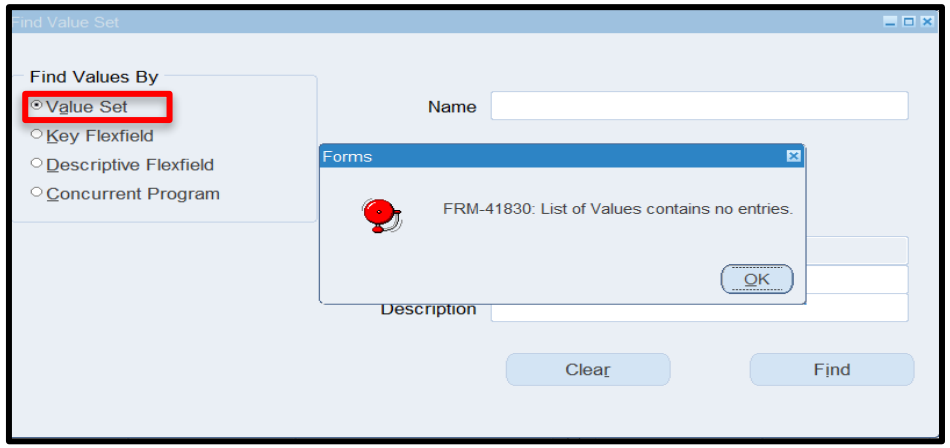
- This is an example of the grant displayed when you click a link for the name
- Click **Update** here if needed rather than going back to the list to click the update pencil
- Note: update does not allow changes to the Object or the Data Context

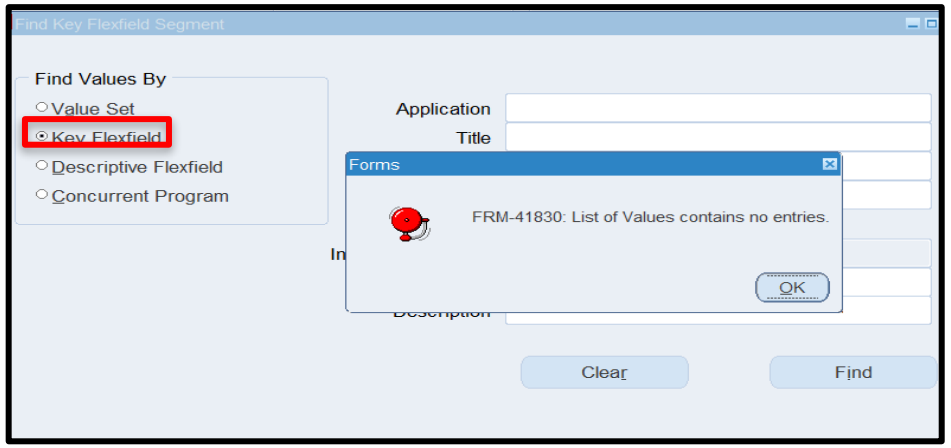


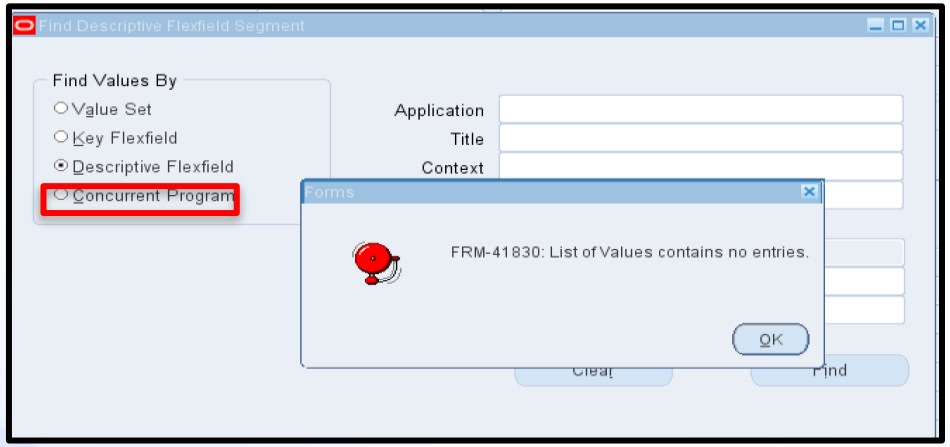
Flexfield Value Set Security **Required** in 12.2

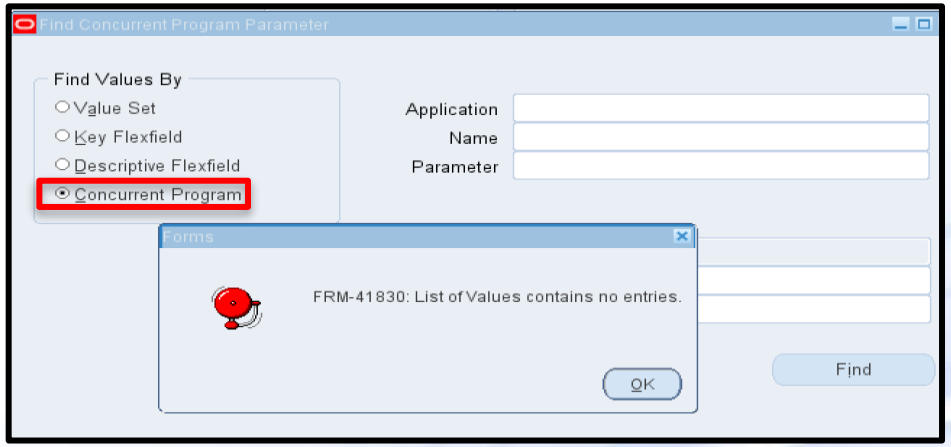
Flexfields | Validation | Values

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



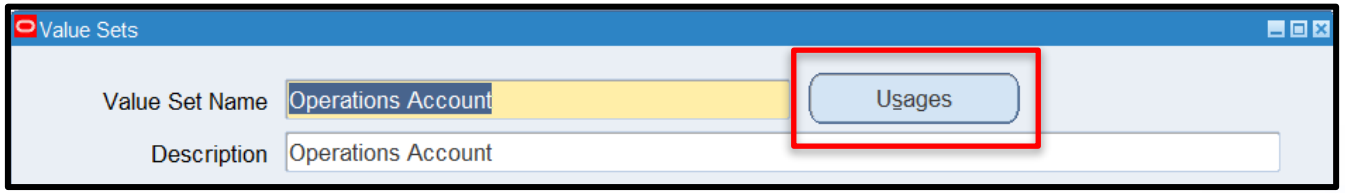


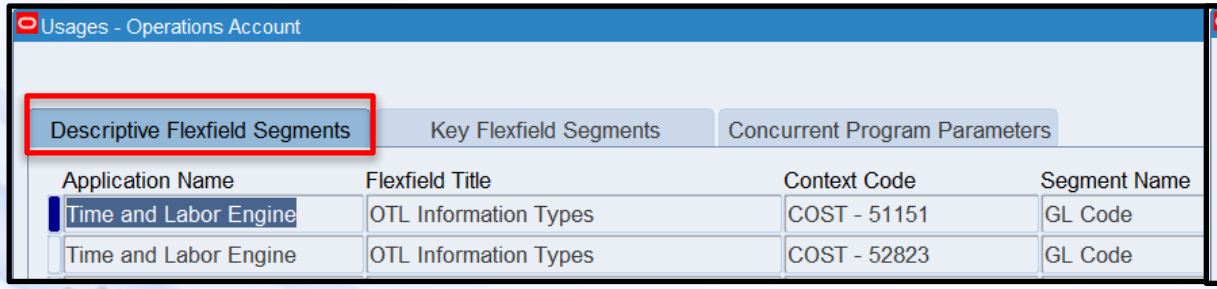


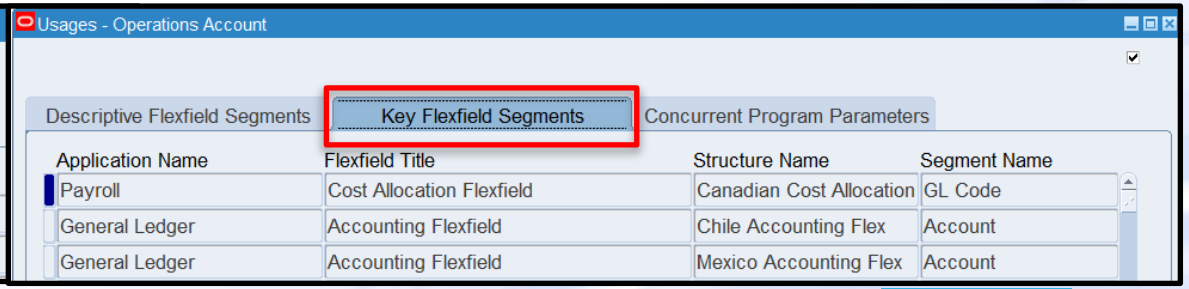


Flexfield Value Sets

- 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 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

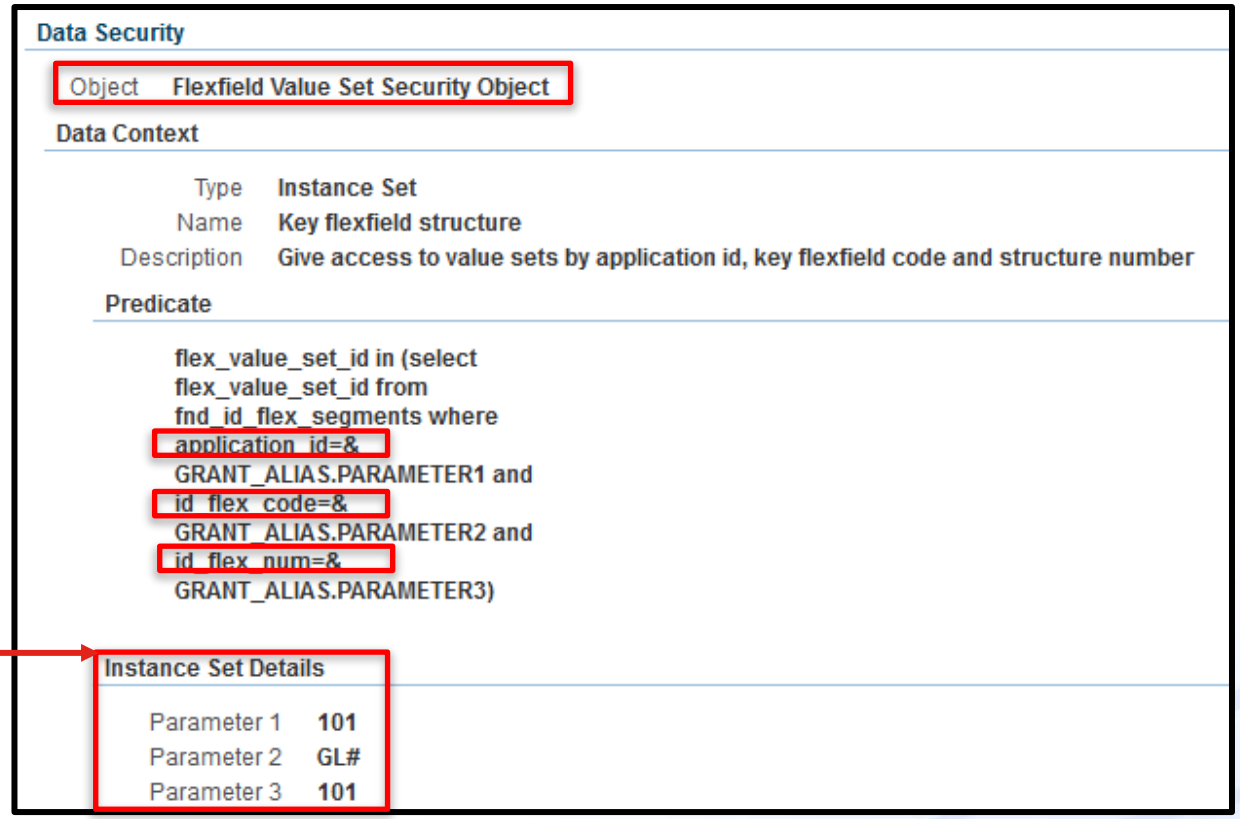
Name	GL Grant for Value Sets for General Ledger, Vision Operations (USA)
Description	GL Grant for Value Sets
Effective From	11-Jul-2014
Effective To	

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

- 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



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

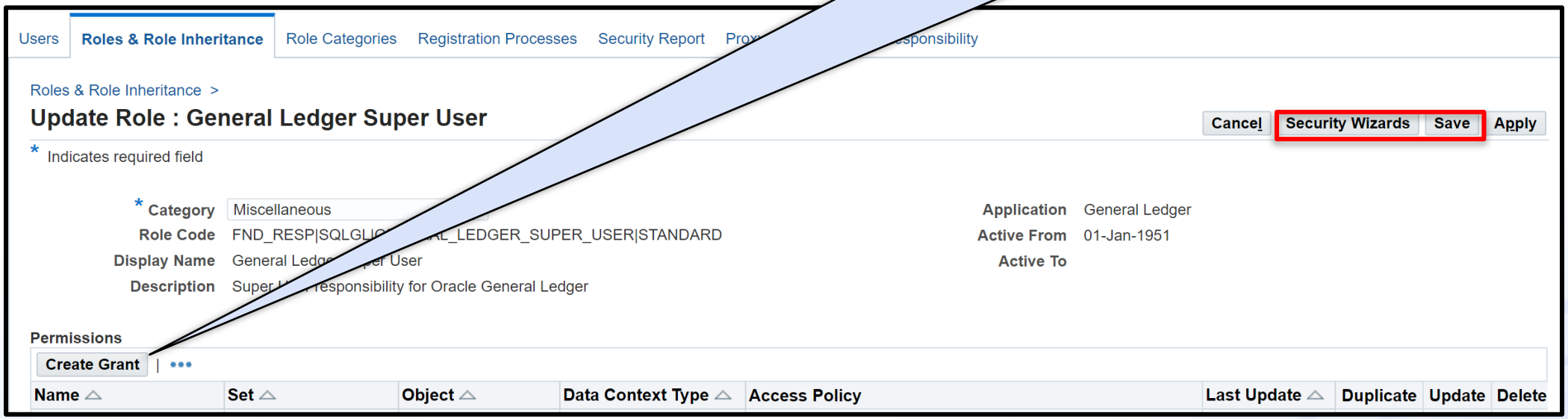
Select	Quick Select	Name	Code	Type	Description
○		Flexfield Value Set Security Insert Set	FND_FLEX_VSET_INSERT_PS	Permission Set	Allow insert of values into a value set
○		Flexfield Value Set Security Insert/Update Set	FND_FLEX_VSET_INSERT_UPDATE_PS	Permission Set	Allow insert and update of values in 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

Flexfield Value Sets:
Using Security Wizard 12.2.6+

Flexfield Value Sets: Security Administration Setup

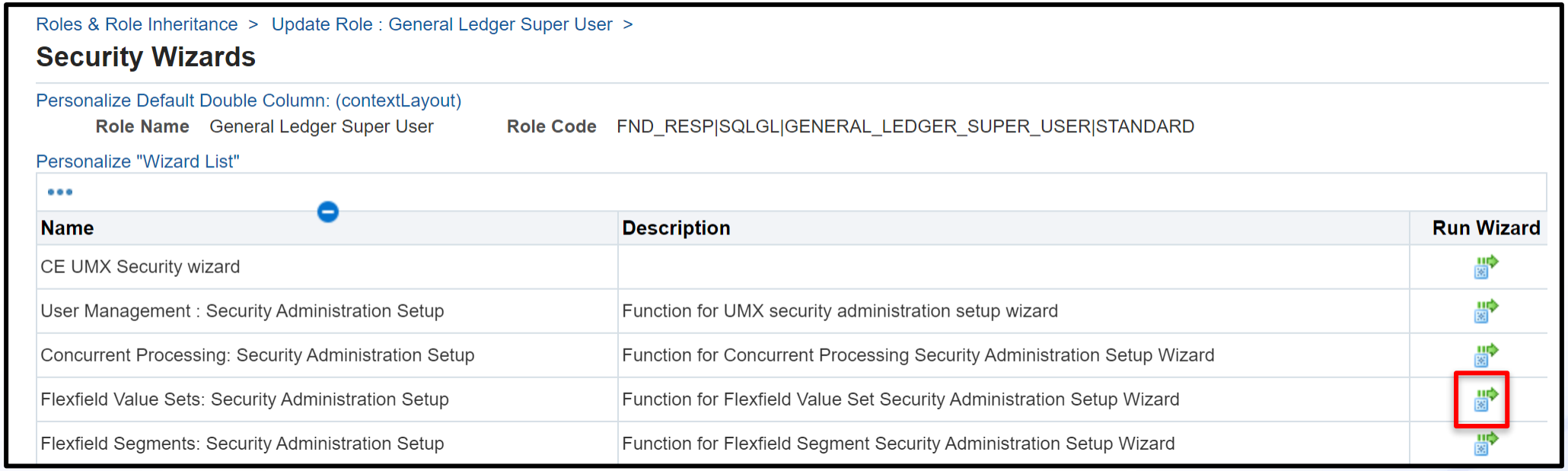
- Example
  - Query General Ledger Super User
  - Click **Save**, then **Security Wizards**

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



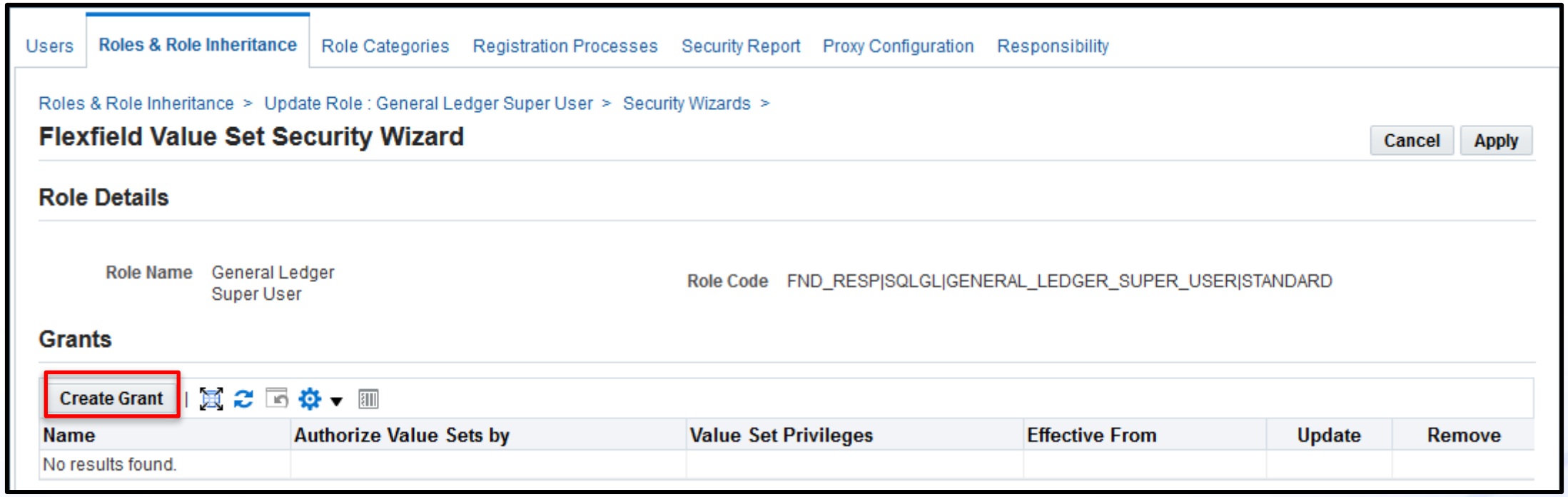
Flexfield Value Sets: Security Administration Setup

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



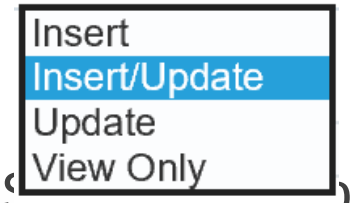
Flexfield Value Sets: Security Administration Setup

- Now click **Create Grant**

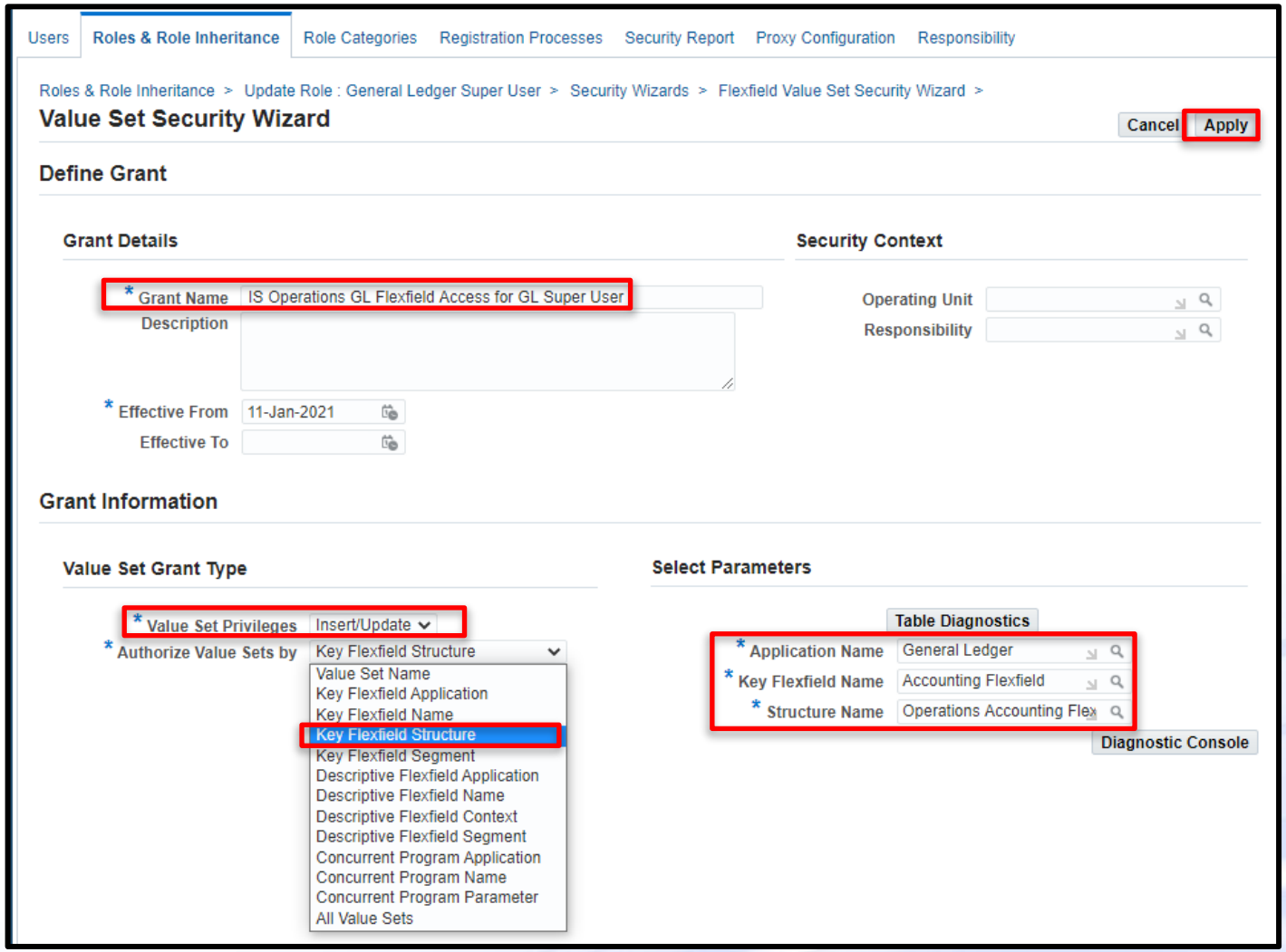


Flexfield Value Sets: Security Administration Setup

- Screen displayed is pared down version of full Create Grant screen
- Name Required
- Choose Value Set Privileges (permission set)

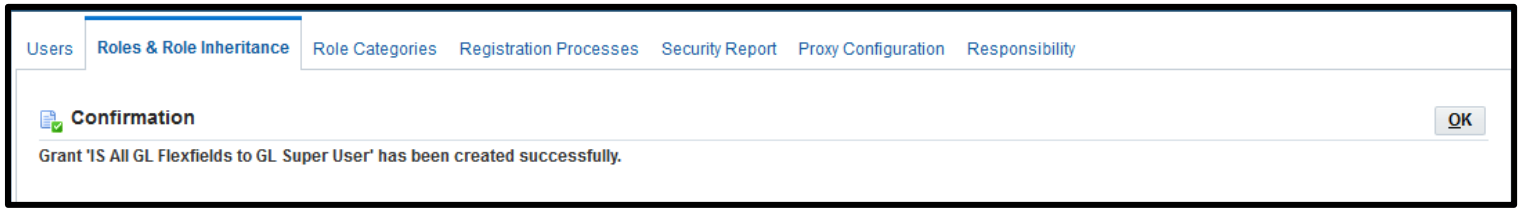


- Select how to authorize (instance set)
- Select Parameters (instance set details)
  - Parameters display based on authorization selection
- Click **Apply**

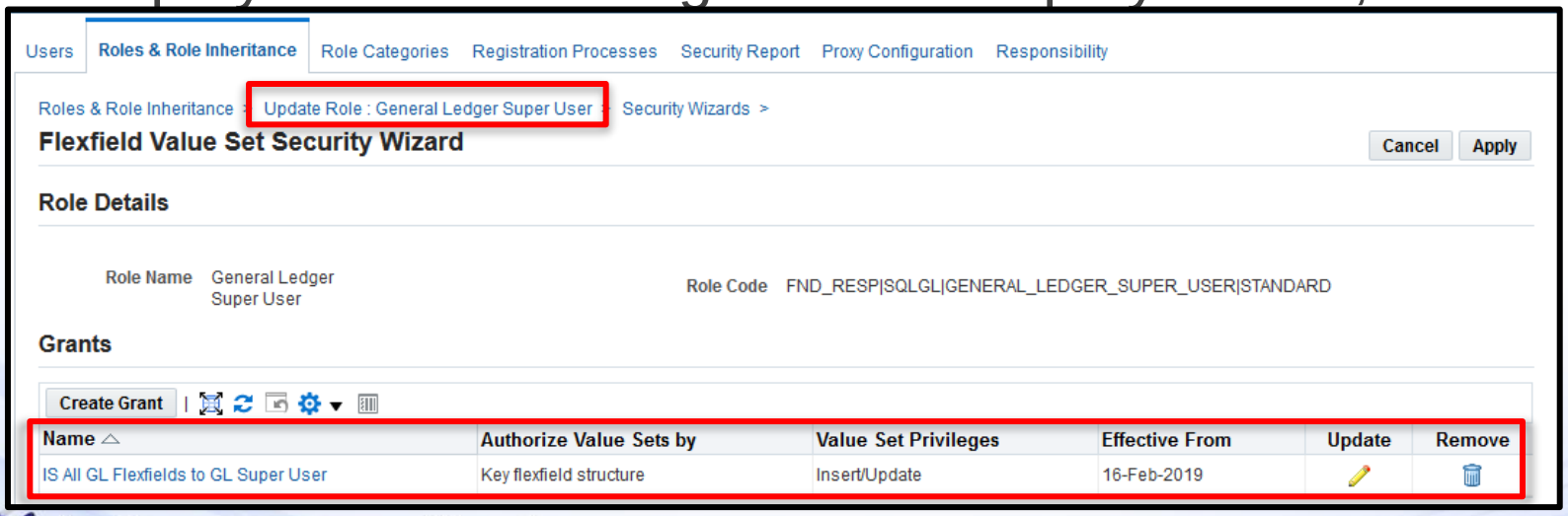


Flexfield Value Sets: Security Administration Setup

- Click **OK** on the Confirmation Screen

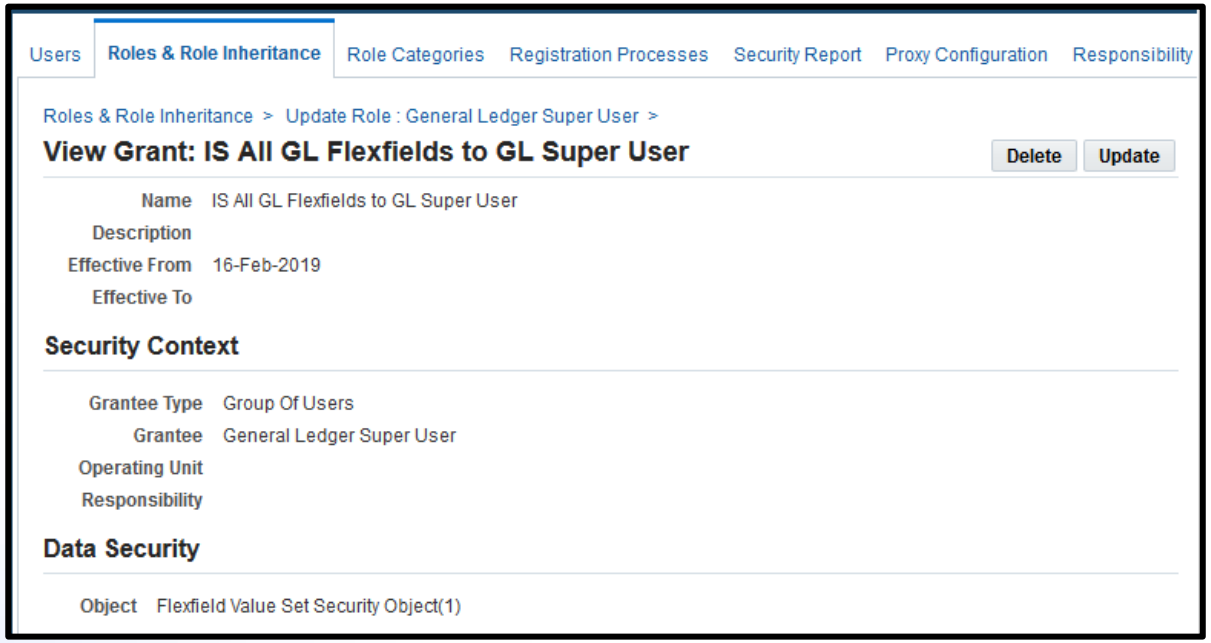


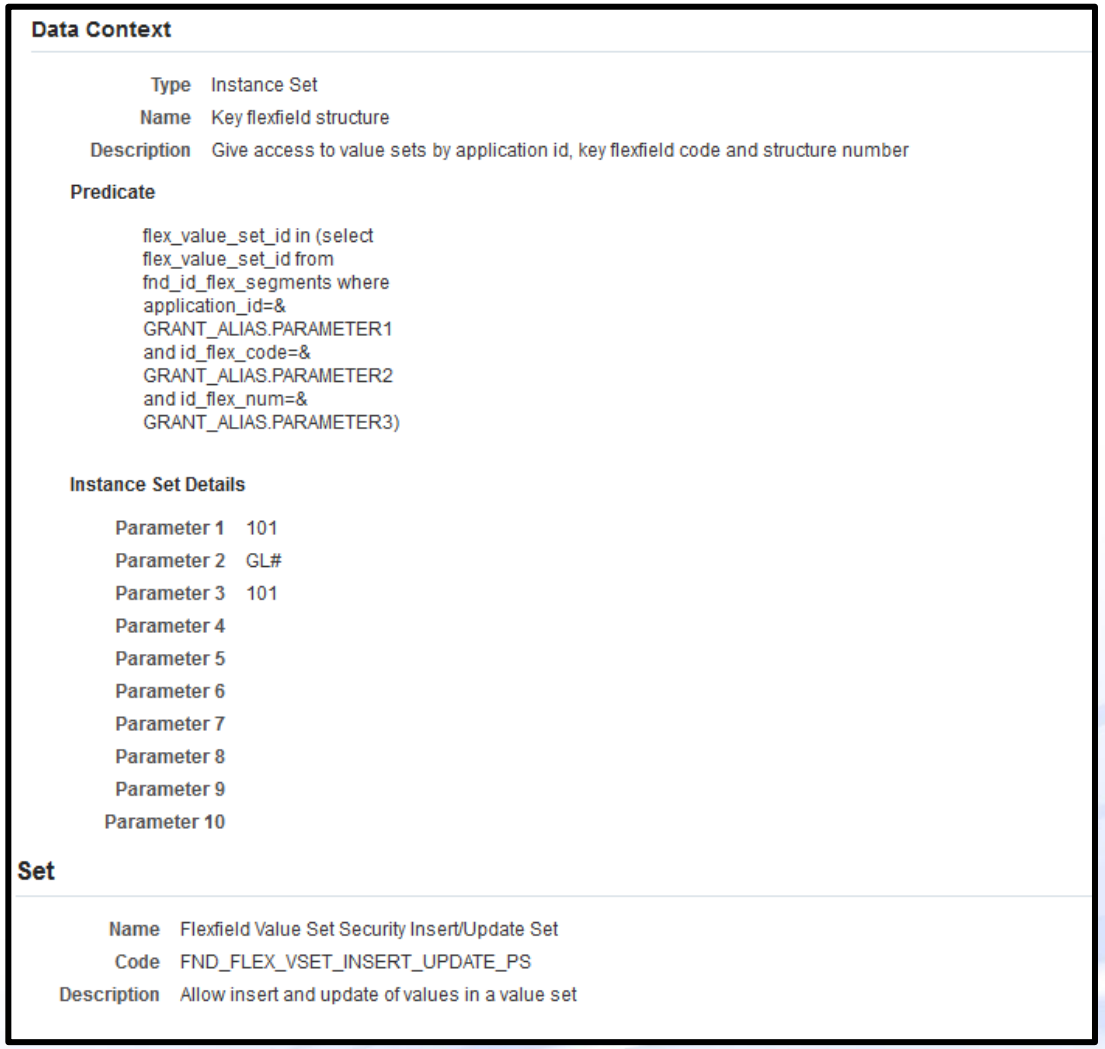
- New grant is displayed
  - Since you are still in the Security Wizard, only grants for Value Sets are displayed – to see all grants for displayed role, click Update Role: <role name>



Flexfield Value Sets: Security Administration Setup

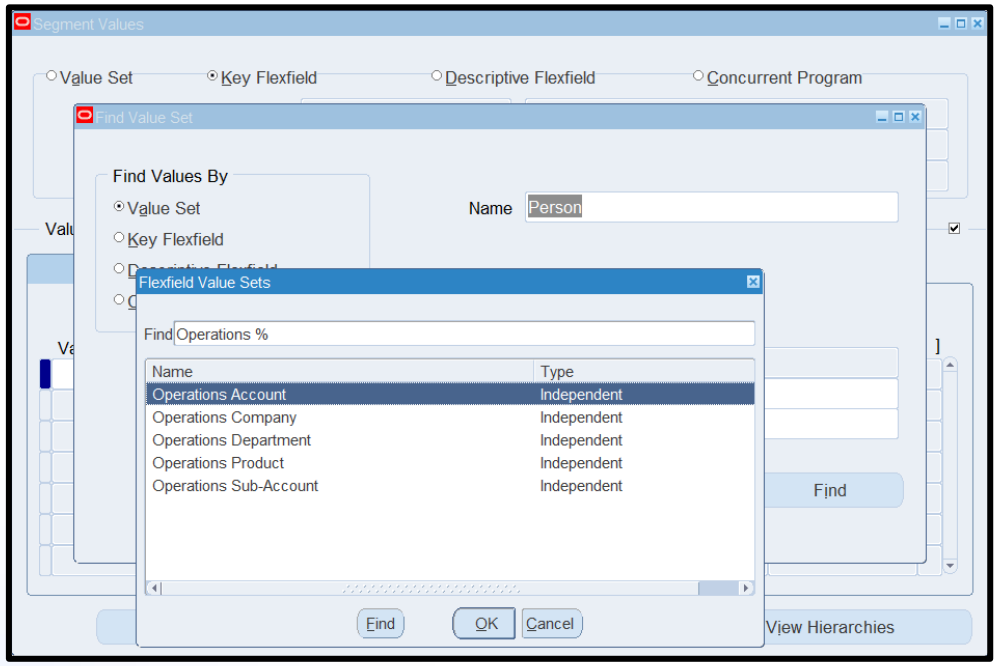
- Clicking Grant name shows definition of grant

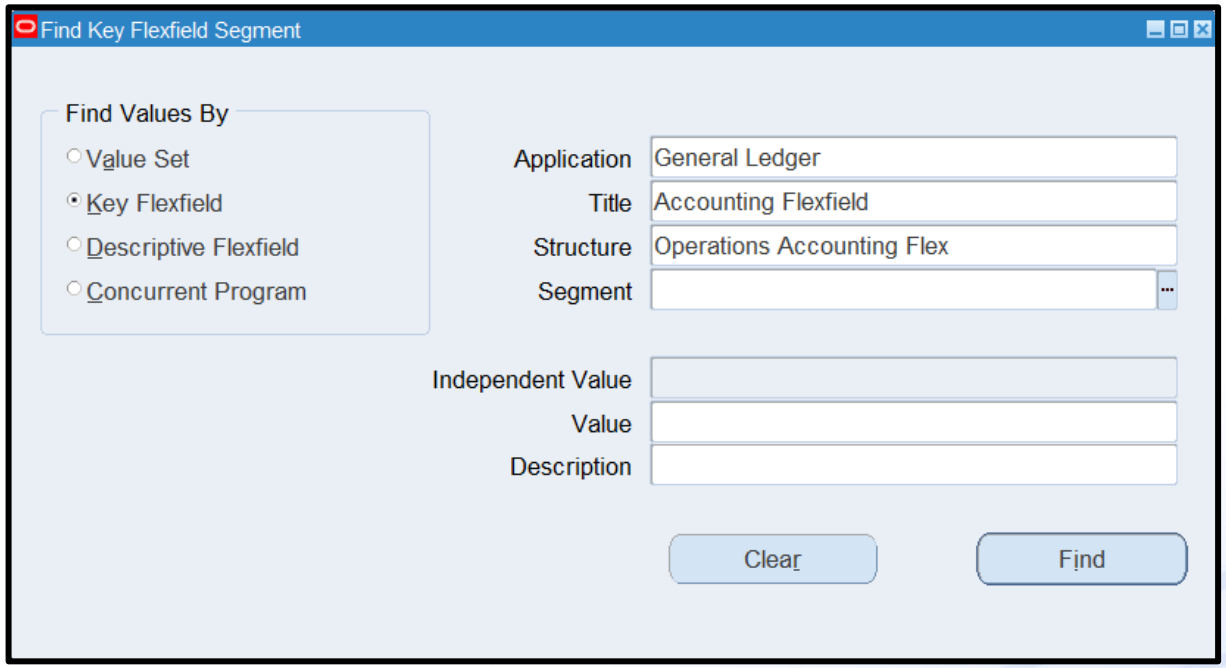




Flexfield Value Sets: Security Administration Setup – Results

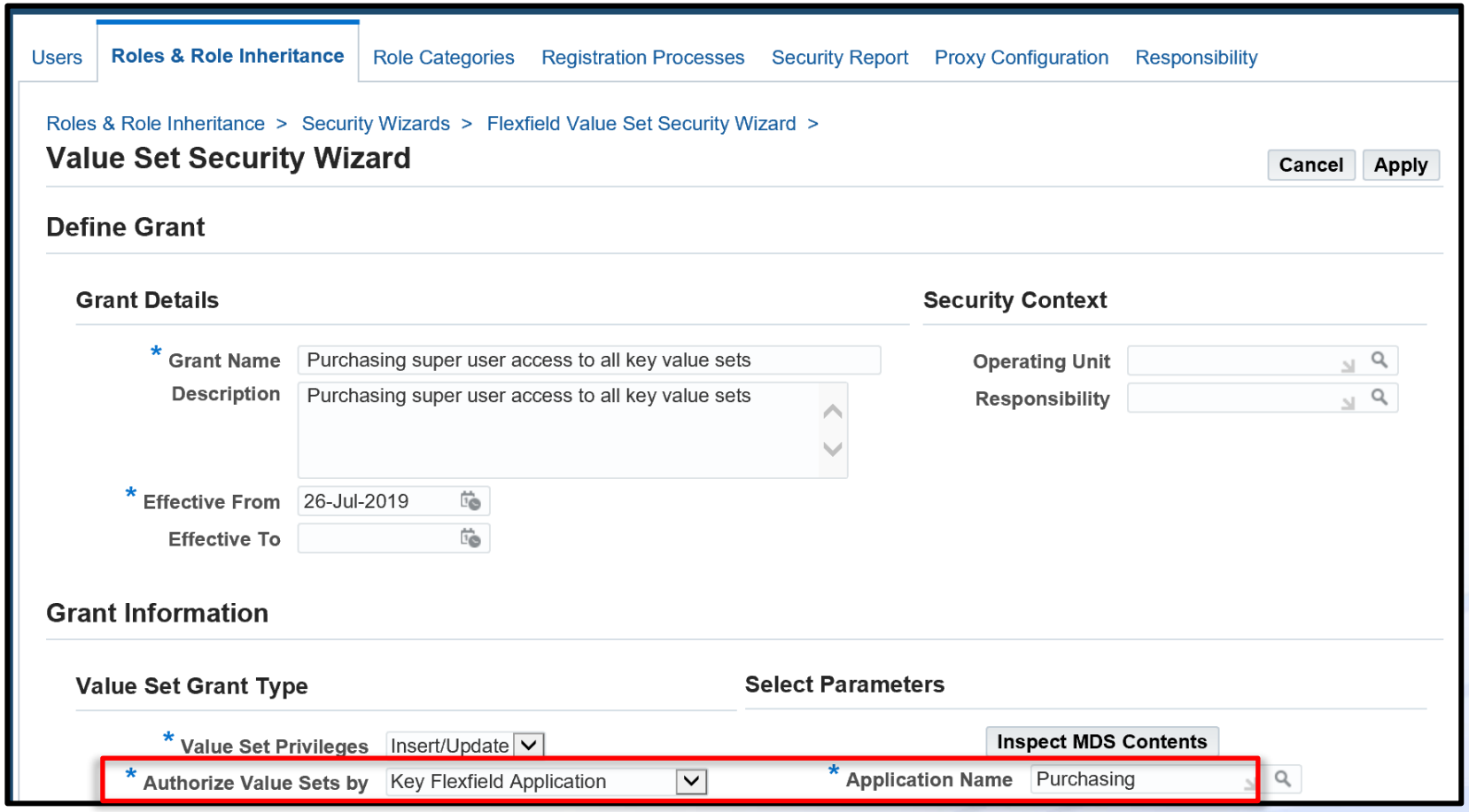
- LOV by Value Set limited to KFF Value Sets, to just the Operations Accounting Flexfield





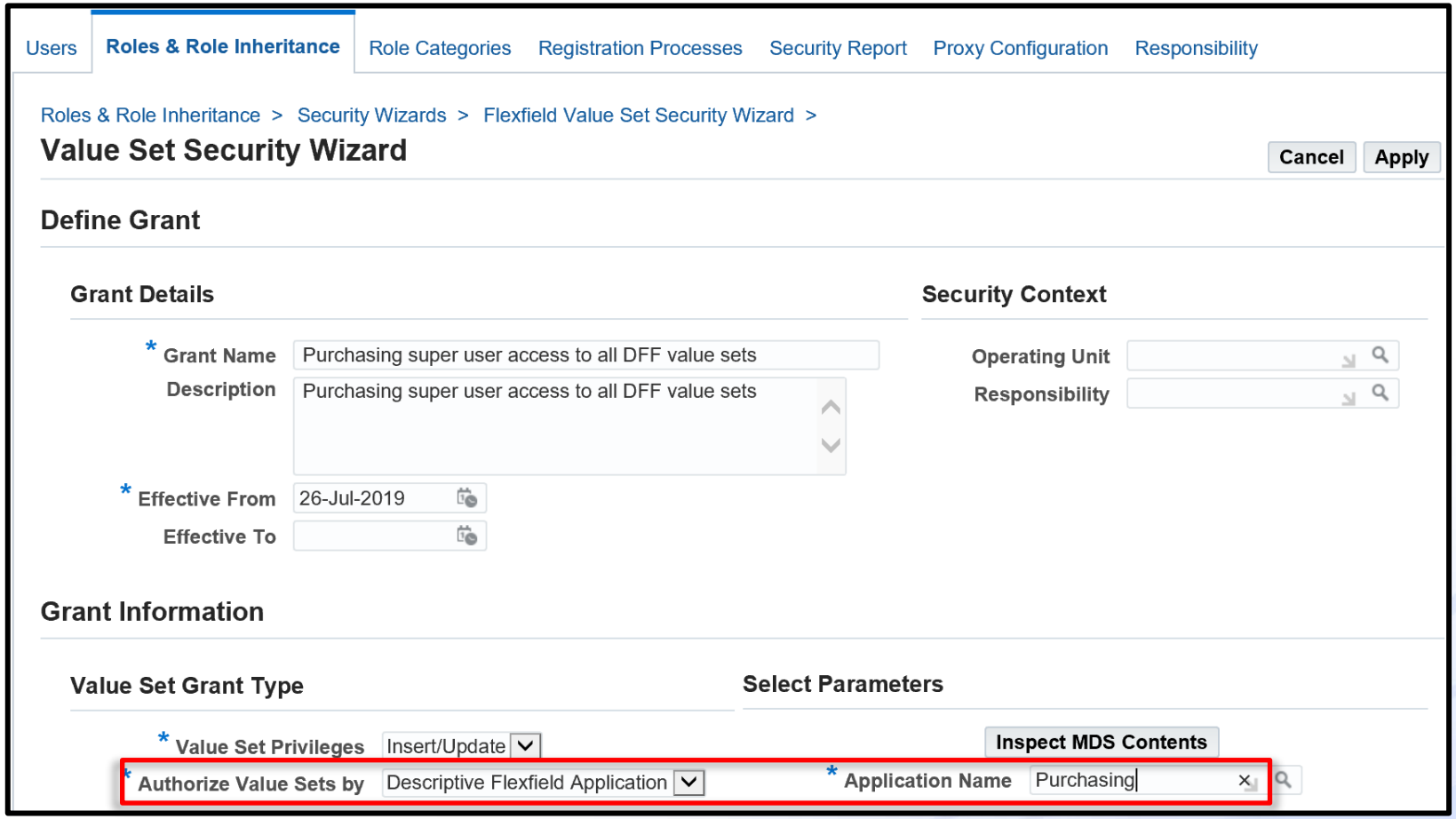
Flexfield Value Sets: Security Administration Setup

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



Flexfield Value Sets: Security Administration Setup

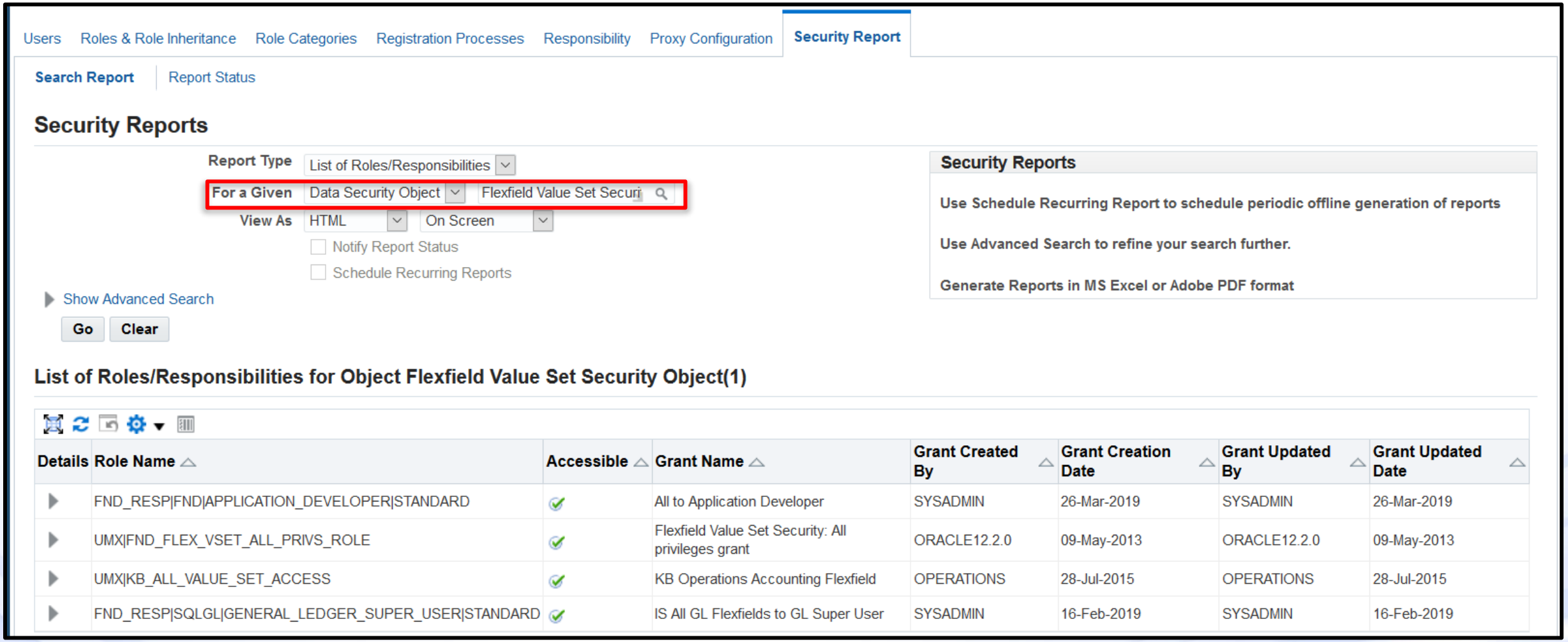
- Purchasing example 2
- Grant access to all value sets for Purchasing **descriptive** flexfields to Purchasing **Application**
- Responsibility/Role not applicable



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

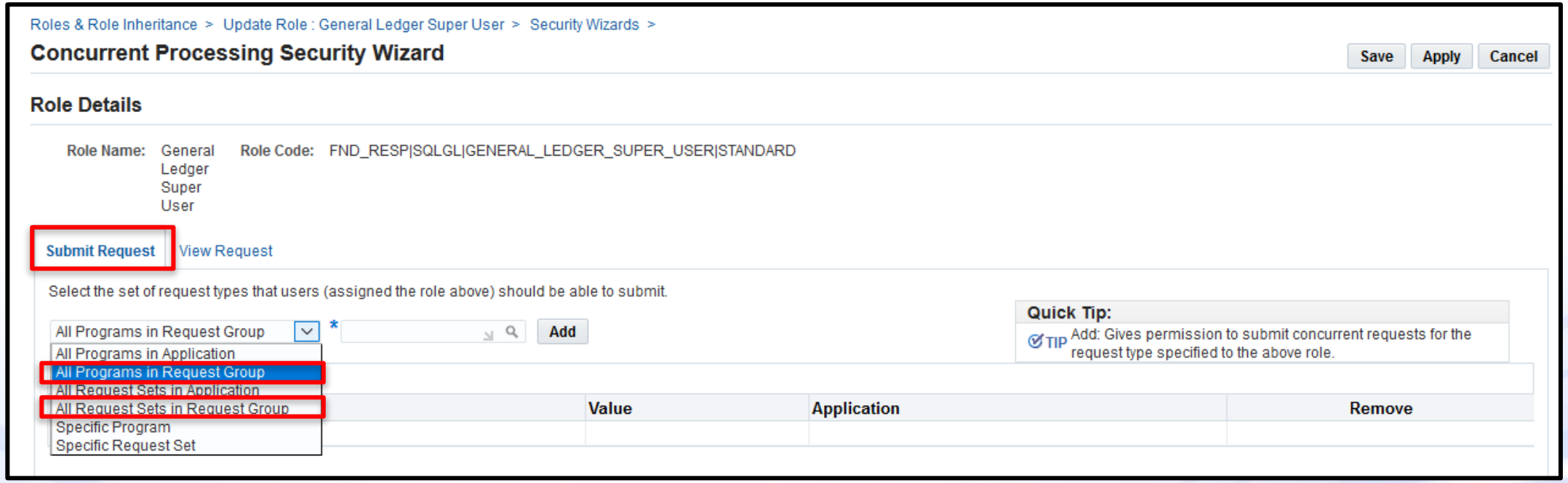


Details	Role Name	Accessible	Grant Name	Grant Created By	Grant Creation Date	Grant Updated By	Grant Updated Date
▶	FND_RESP|FND|APPLICATION_DEVELOPER|STANDARD	✓	All to Application Developer	SYSADMIN	26-Mar-2019	SYSADMIN	26-Mar-2019
▶	UMX|FND_FLEX_VSET_ALL_PRIVS_ROLE	✓	Flexfield Value Set Security: All 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

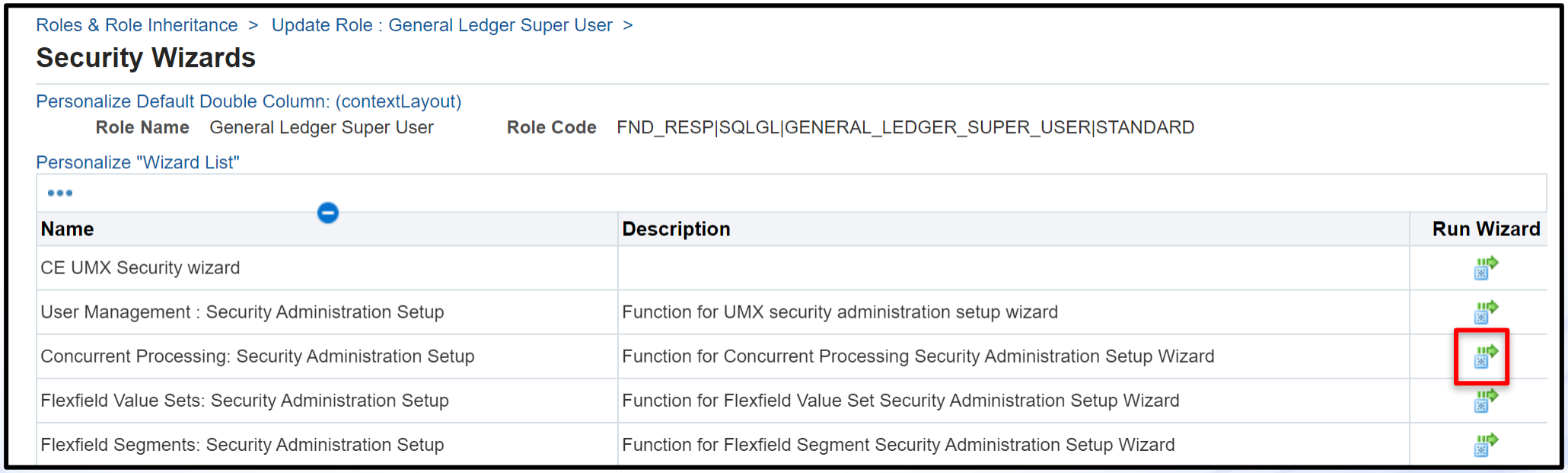
Concurrent Processing: Security Administration Setup

- 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



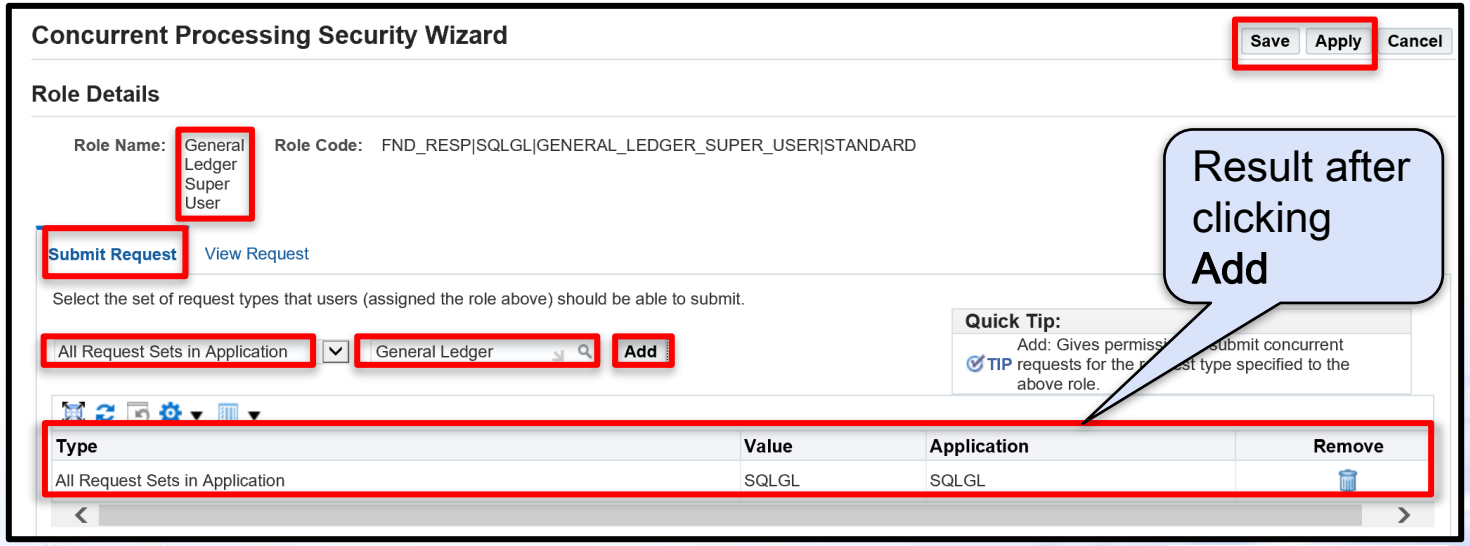
Concurrent Processing: Security Administration Setup

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



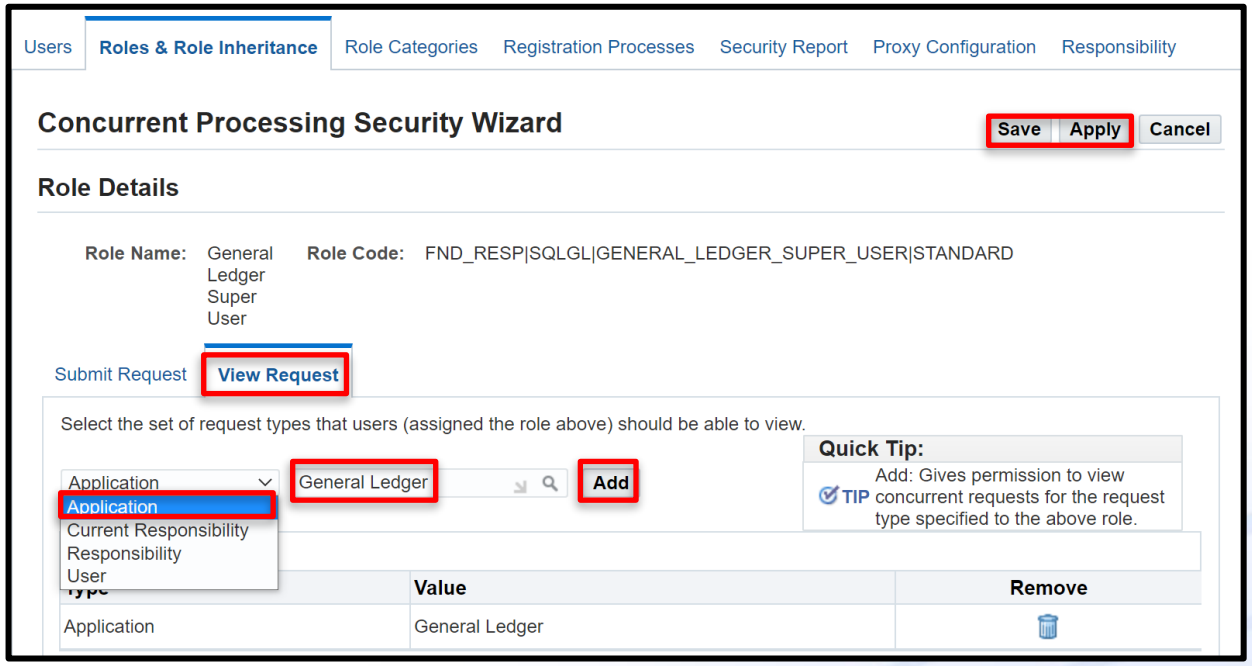
Concurrent Processing: Security Administration Setup

- 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



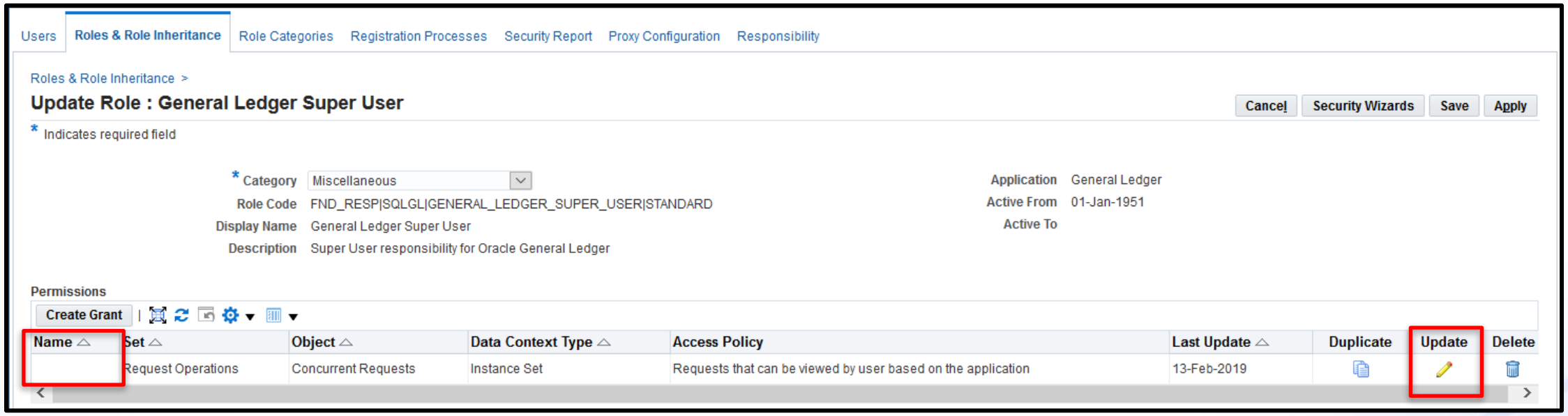
Concurrent Processing: Security Administration Setup

- 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



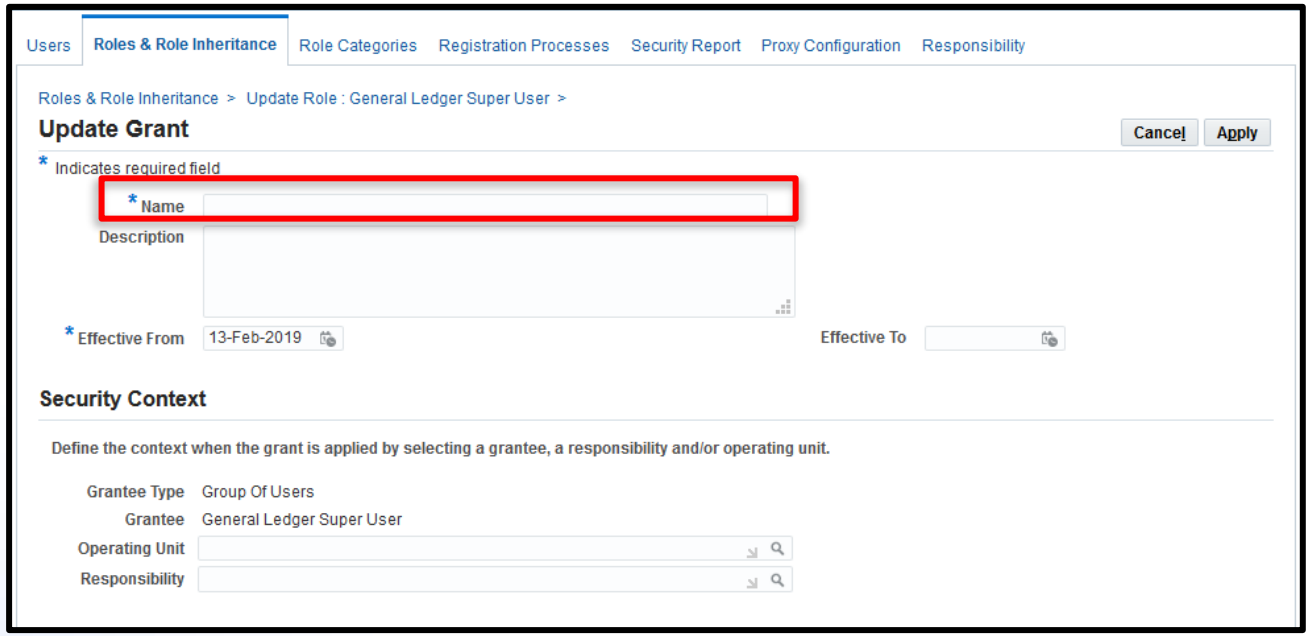
Concurrent Processing: Security Administration Setup

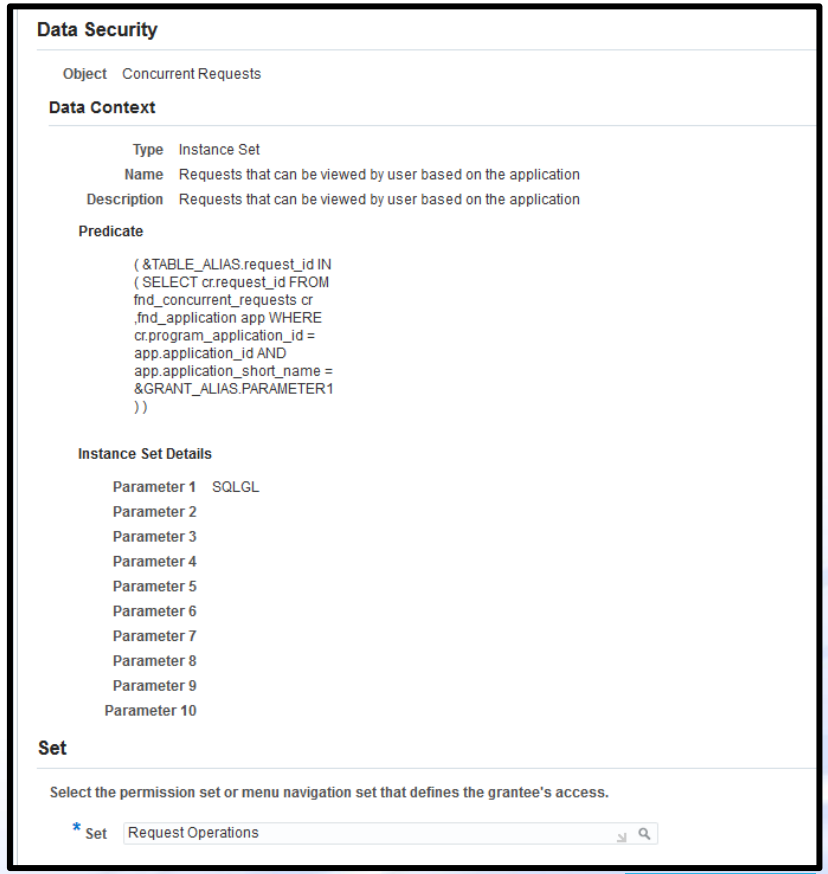
- Unlike the CE Wizard, resulting grants are not named
  - To see the grant, click **Update**



Concurrent Processing: Security Administration Setup

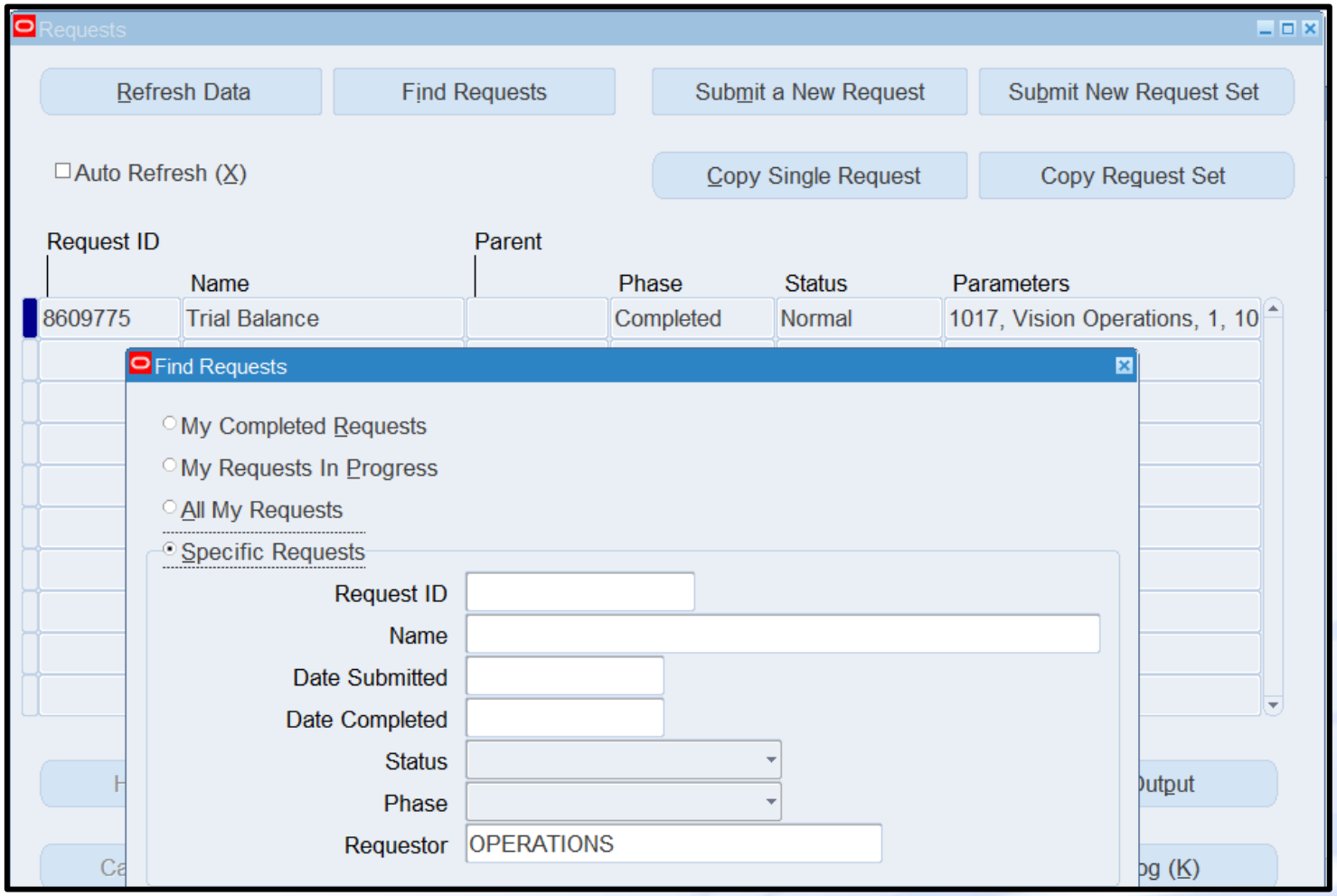
- If any updates are made on this page, adding a name will be required
  - Recommend just deleting and recreating the grant unless restricting by Operating Unit





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



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

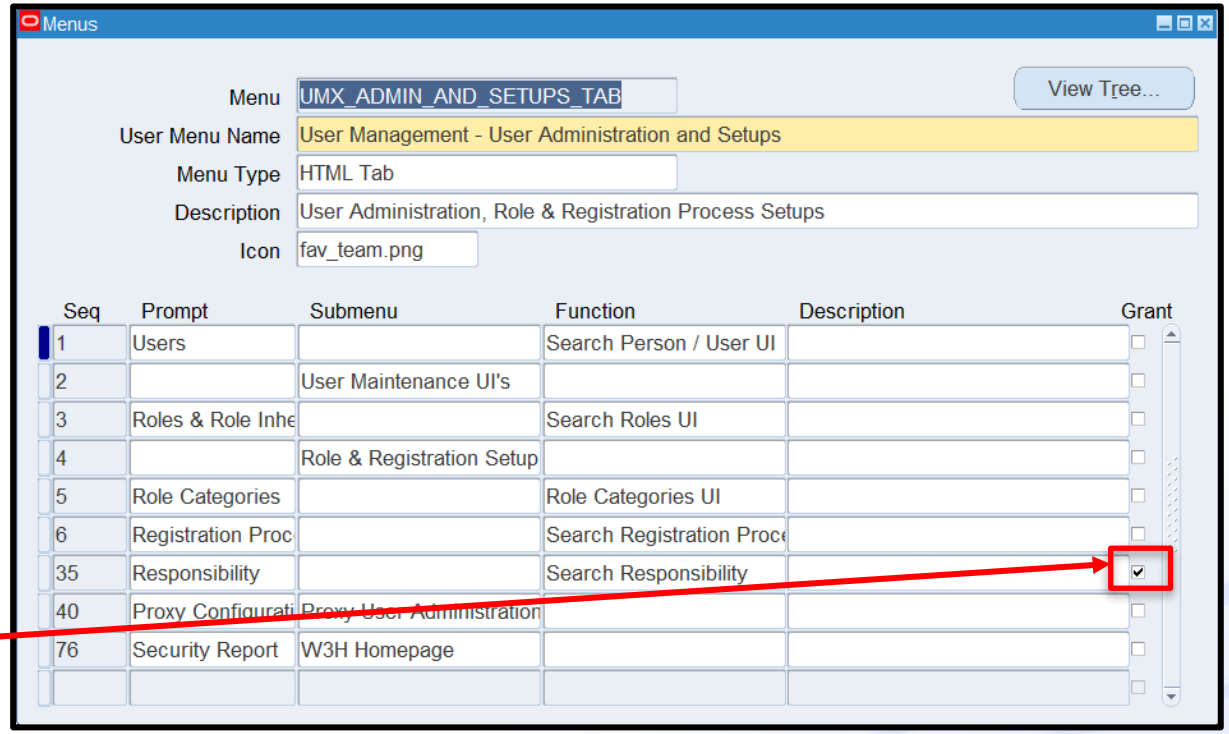
User Management:
Security Administration Setup

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

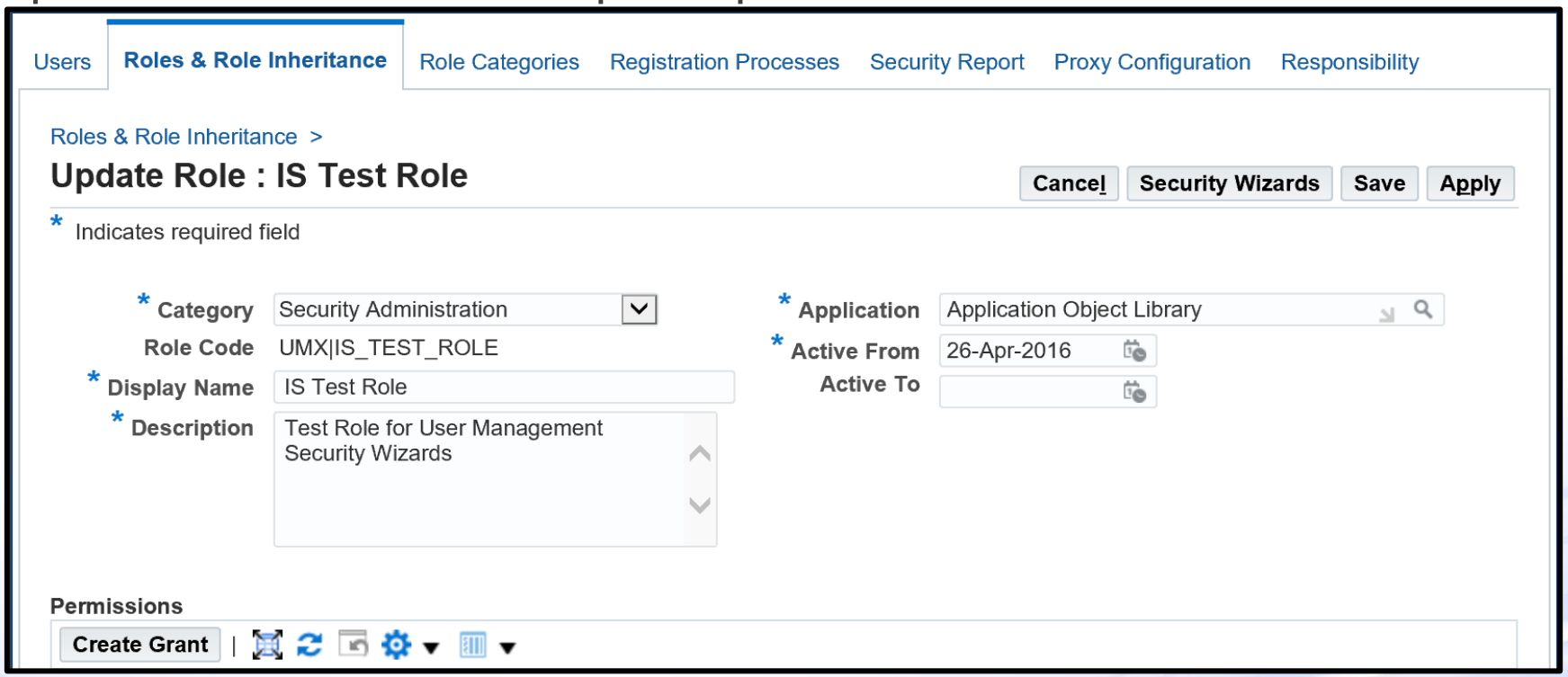
User Management : Security Administration Setup

- 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 though 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



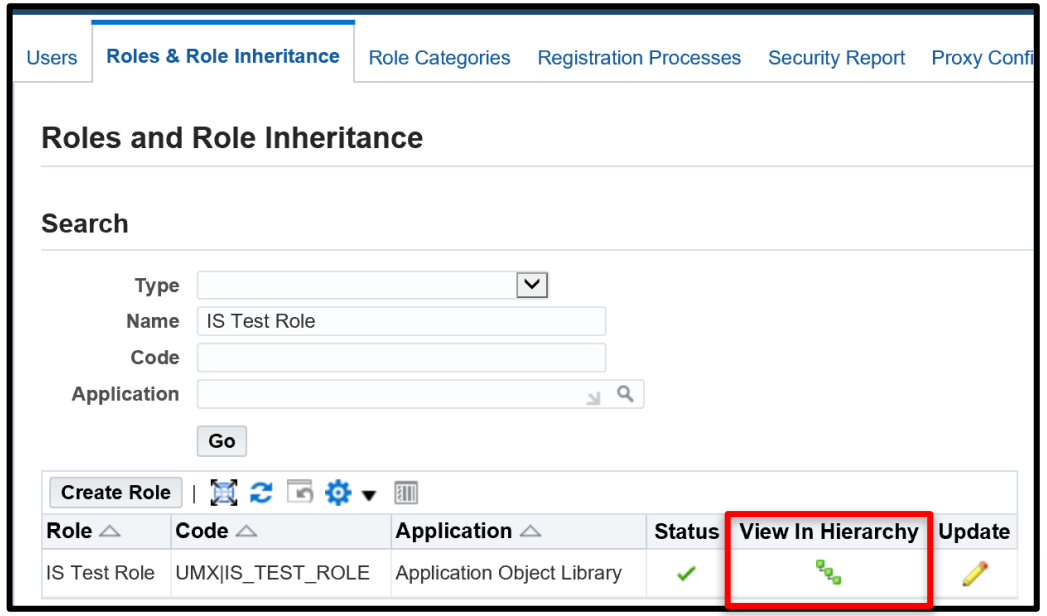
User Management : Security Administration Setup

- 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



User Management : Security Administration Setup

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

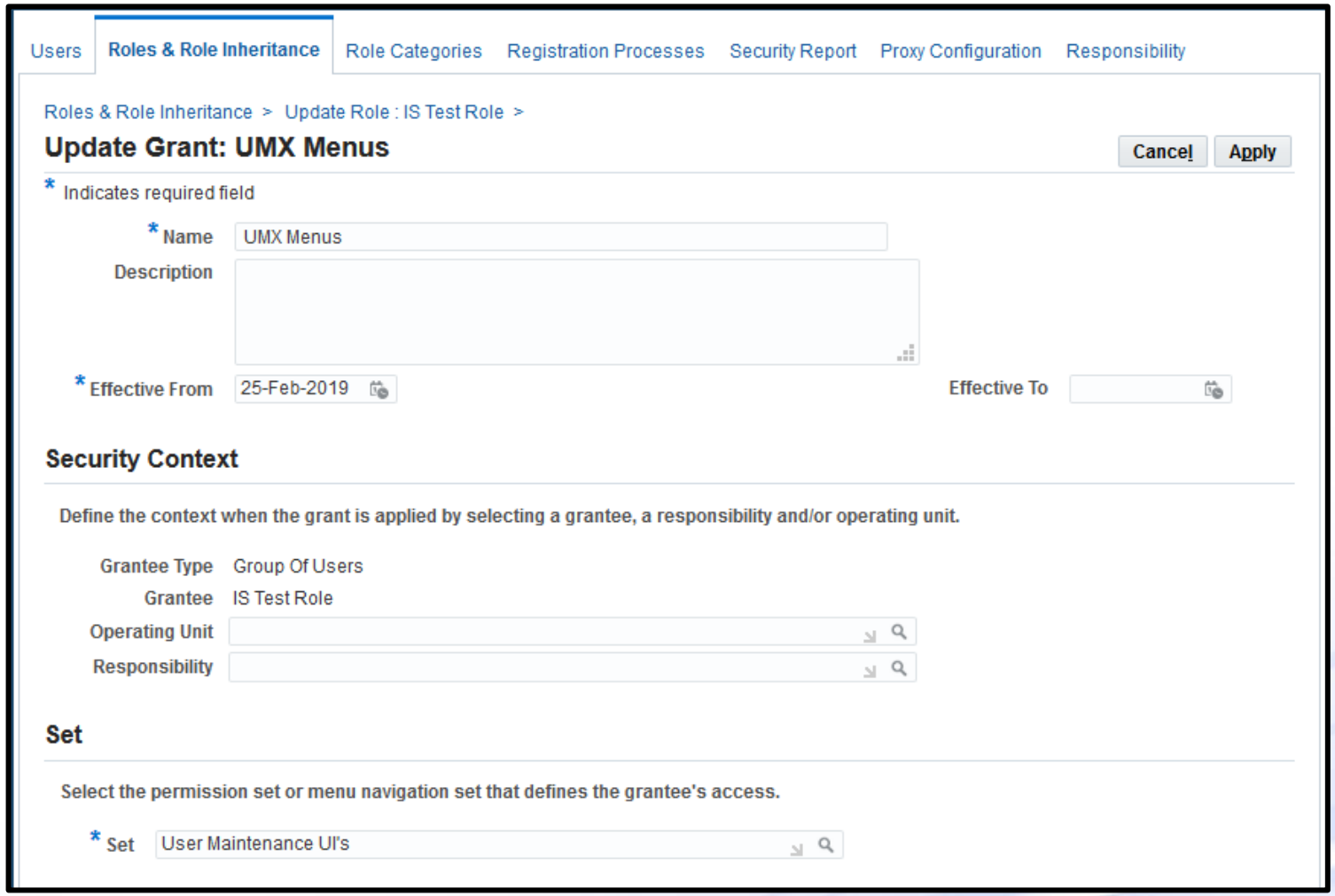


  - Click the Add Node icon to add the **User Management** responsibility to the Role Hierarchy for new role, resulting in hierarchy shown below

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	✓			

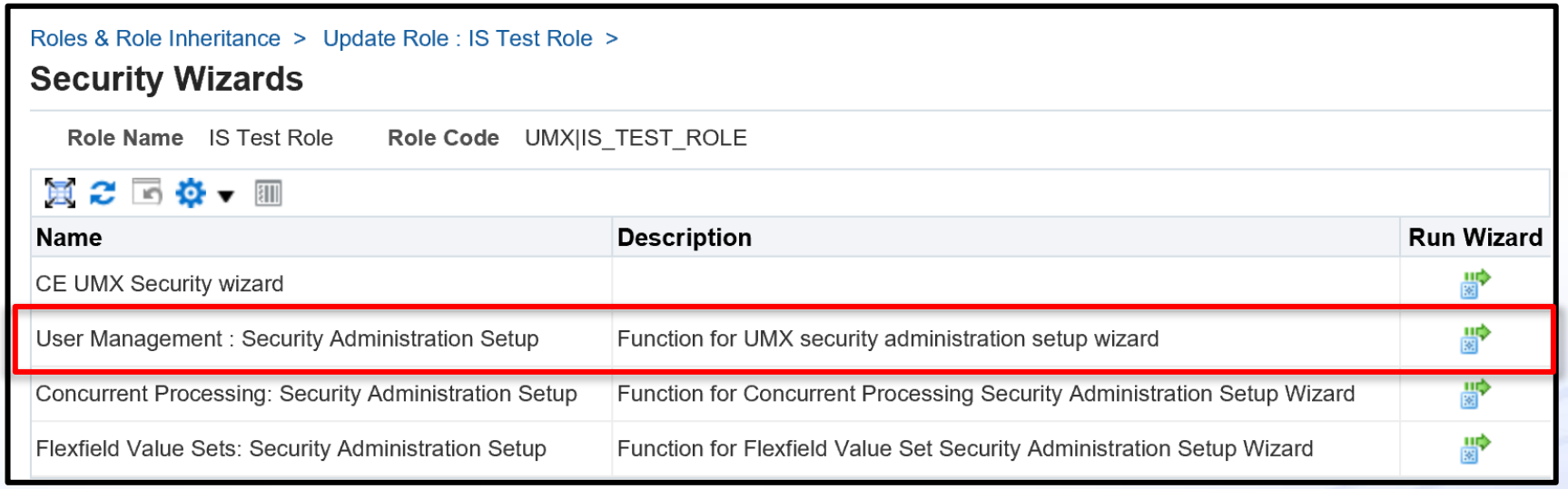
User Management : Security Administration Setup

- 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



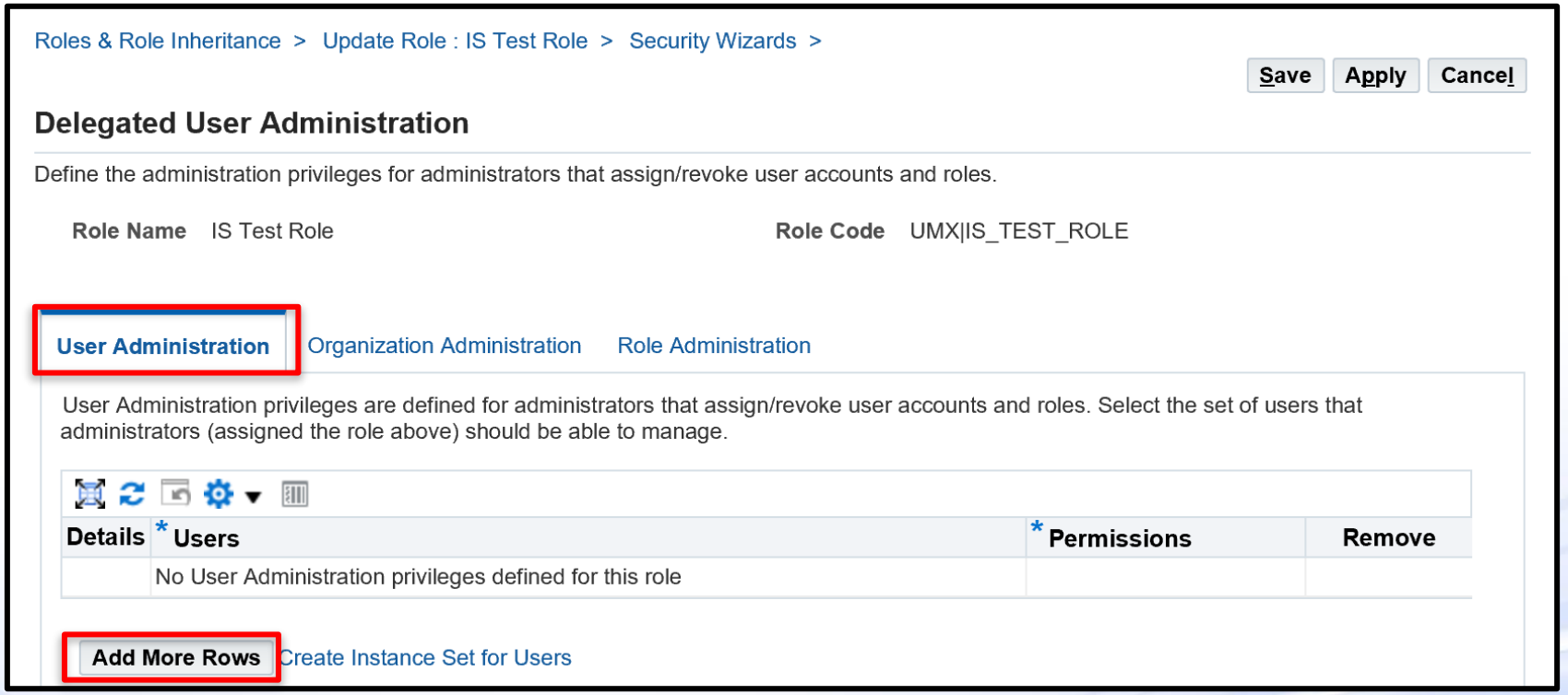
User Management : Security Administration Setup

- 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**”



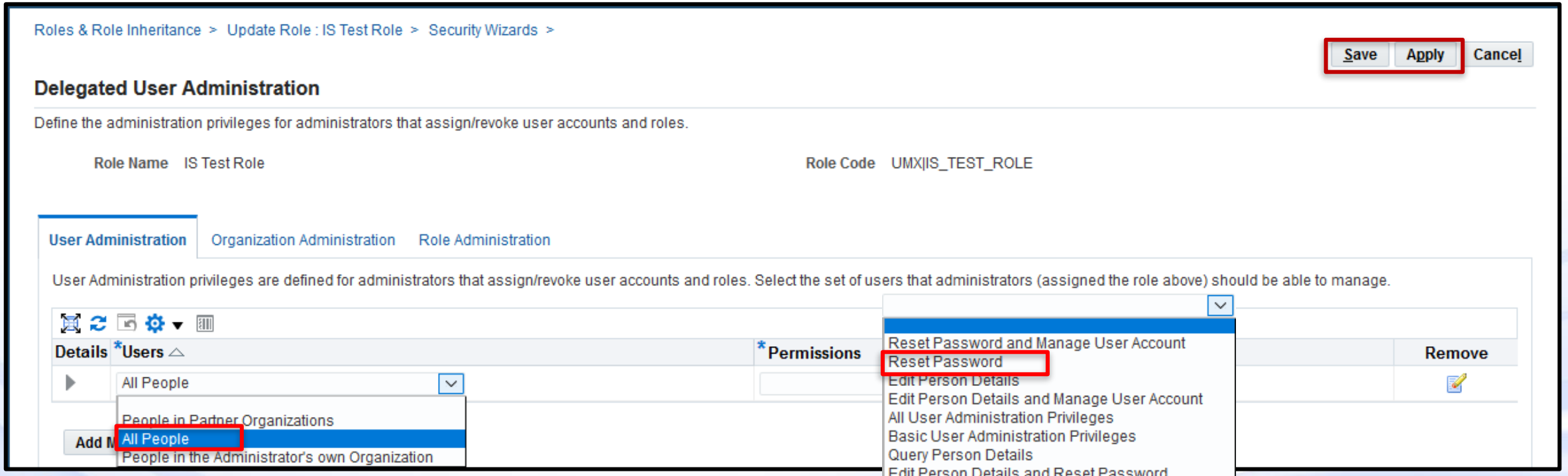
User Management : Security Administration Setup

- 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**

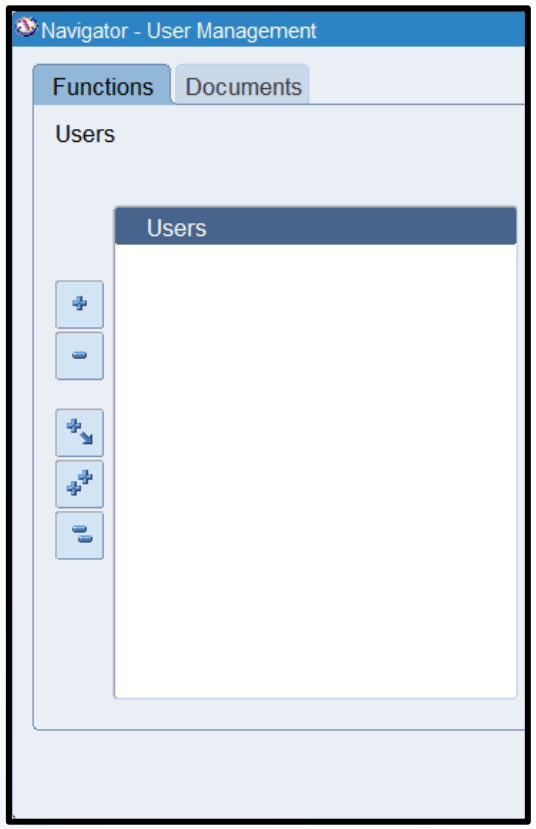


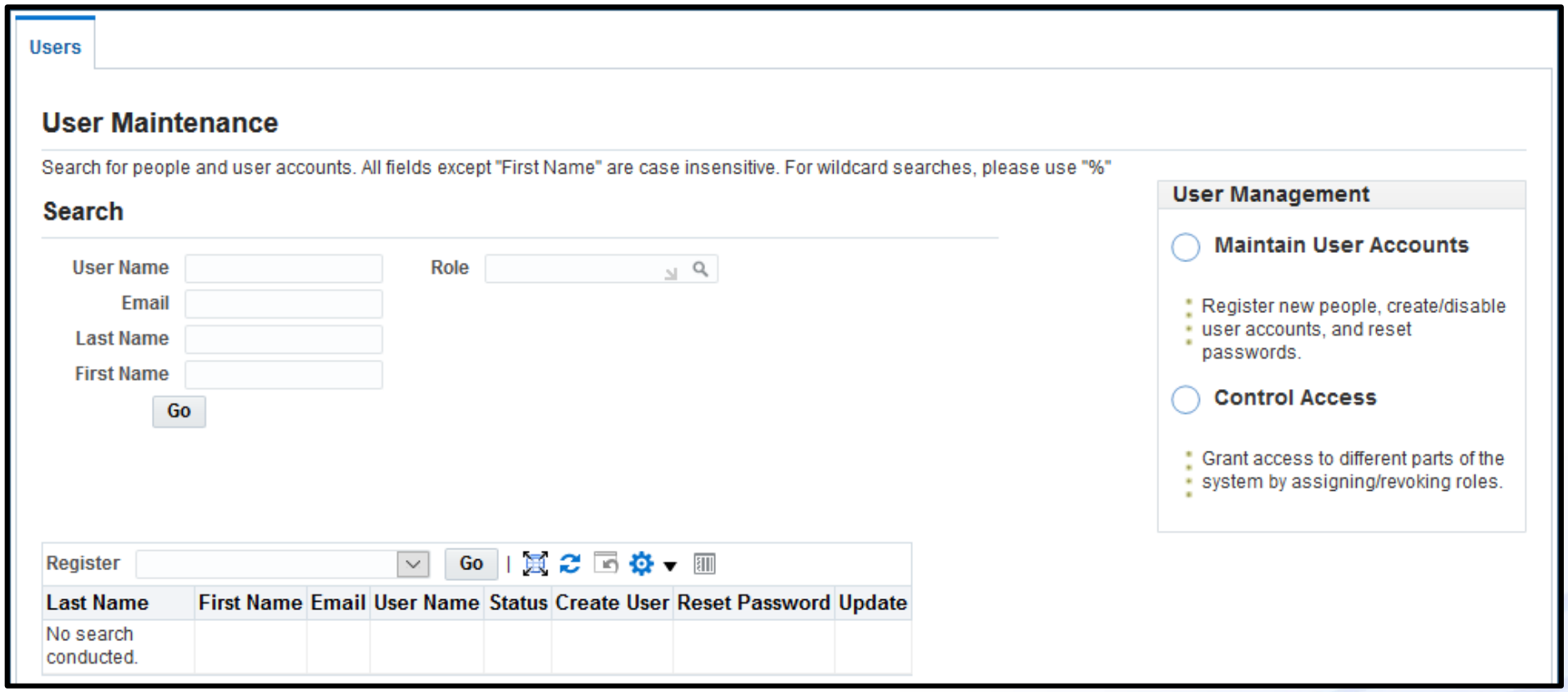
User Management : Security Administration Setup
User Administration

- 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**



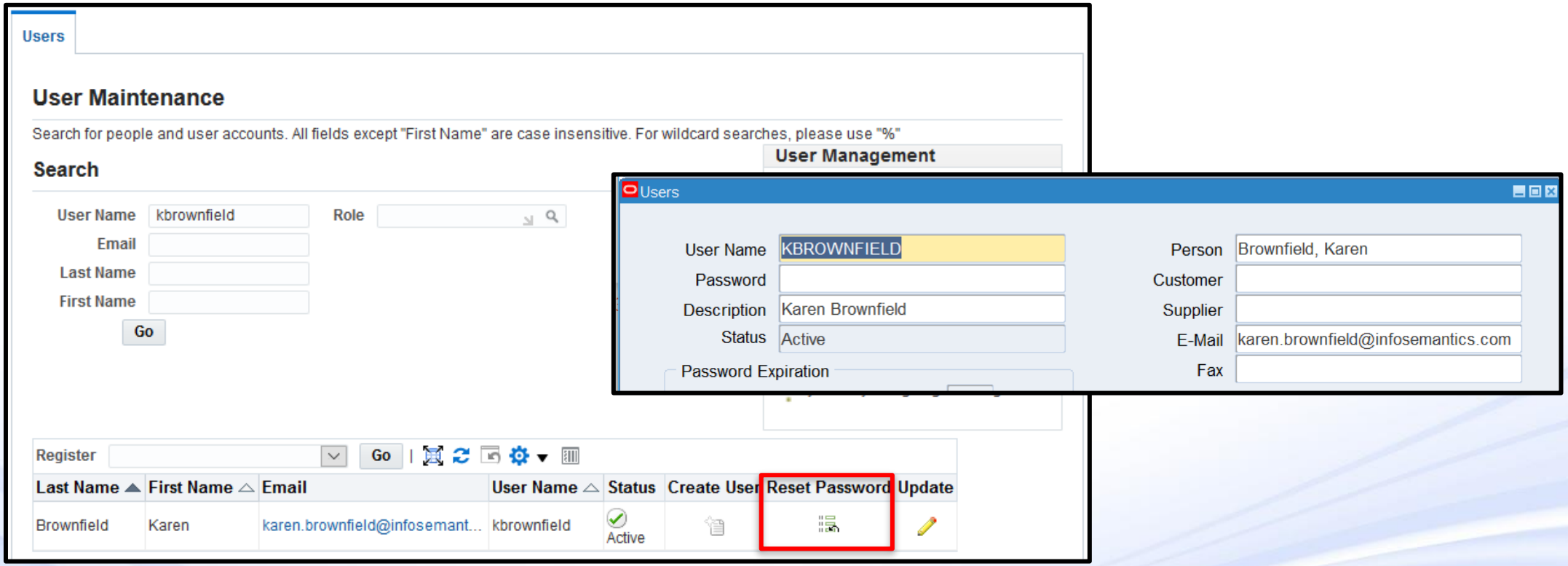
User Management : Security Administration Setup – Results
User Administration





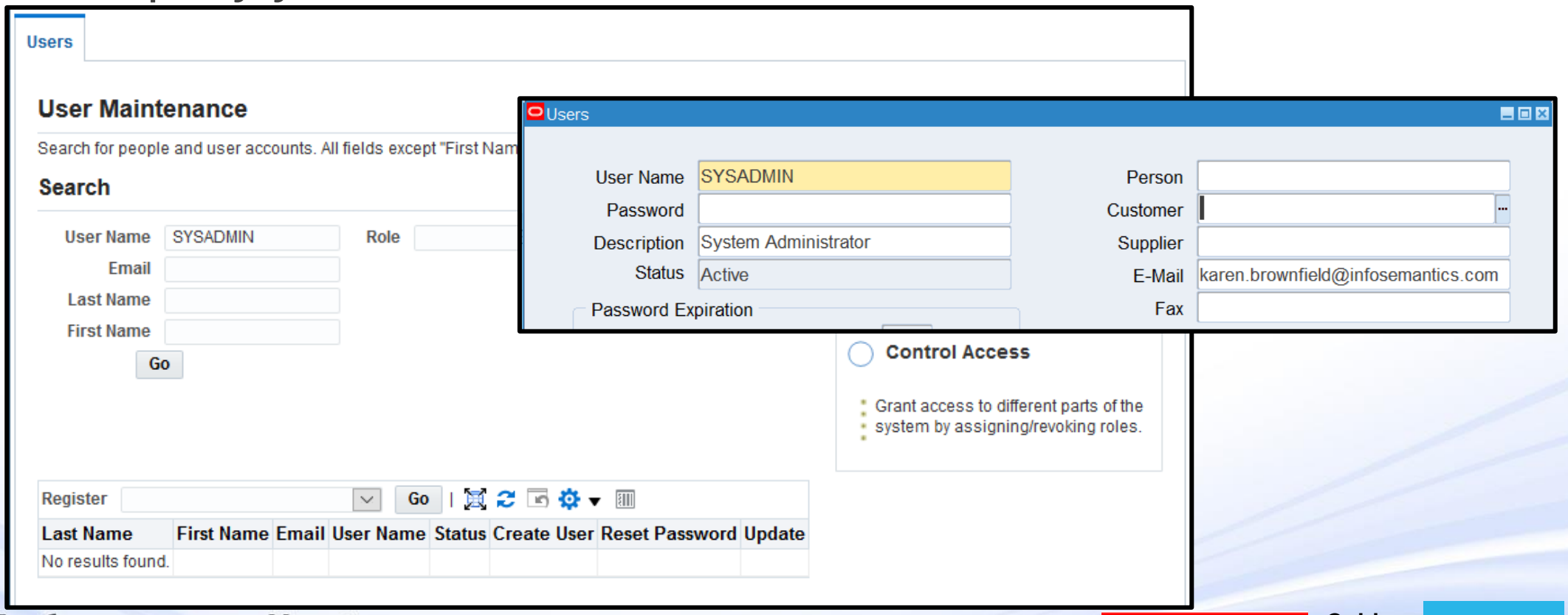
User Management : Security Administration Setup – Results
User Administration

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



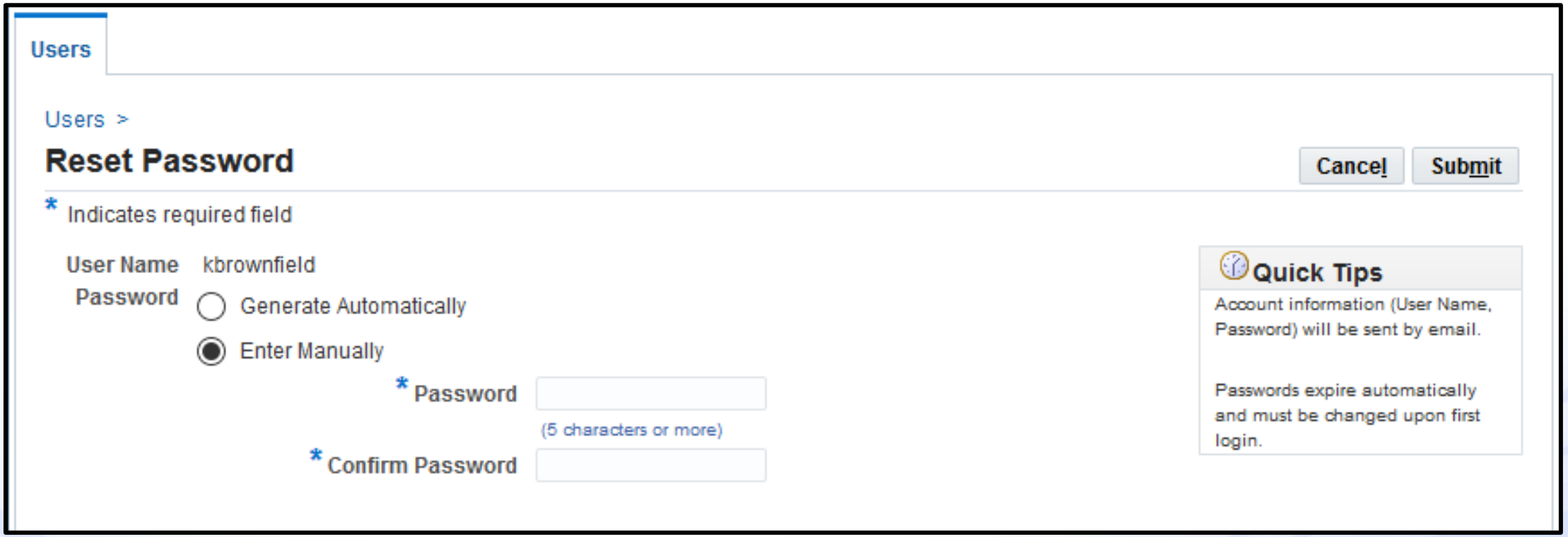
User Management : Security Administration Setup – Results
User Administration

- 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



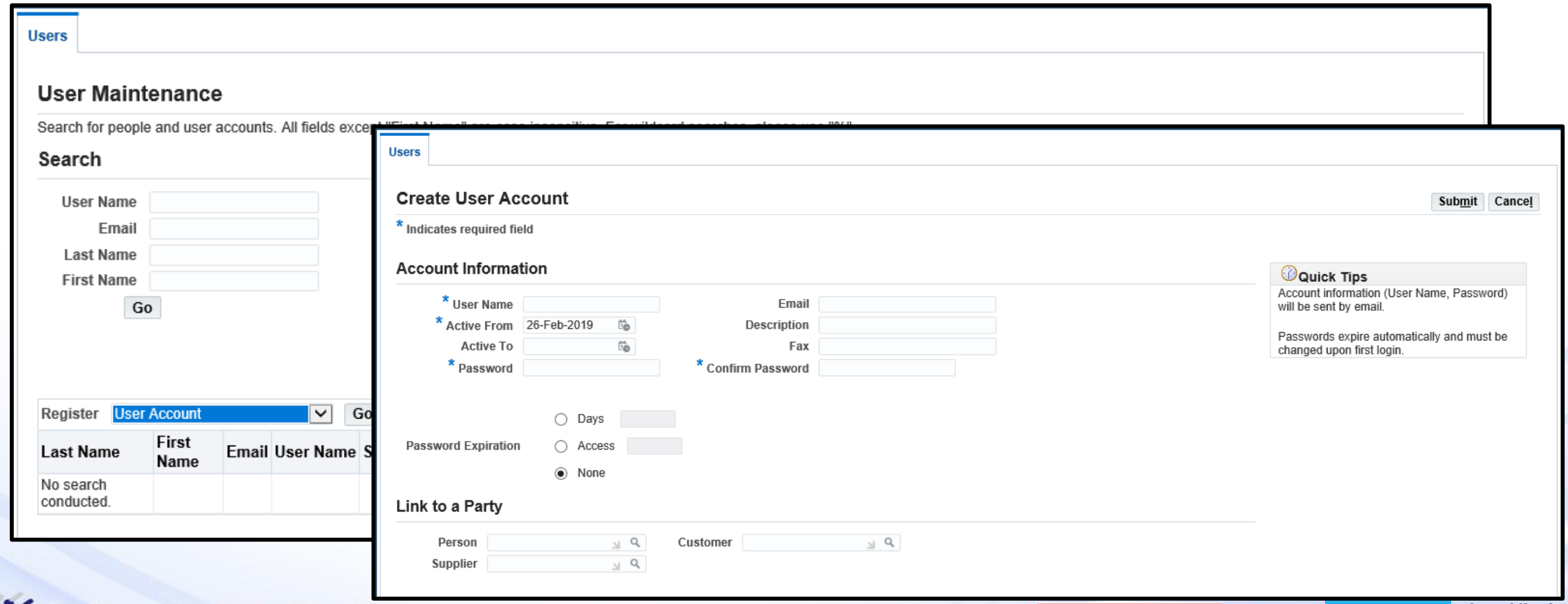
User Management : Security Administration Setup – Results
User Administration

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



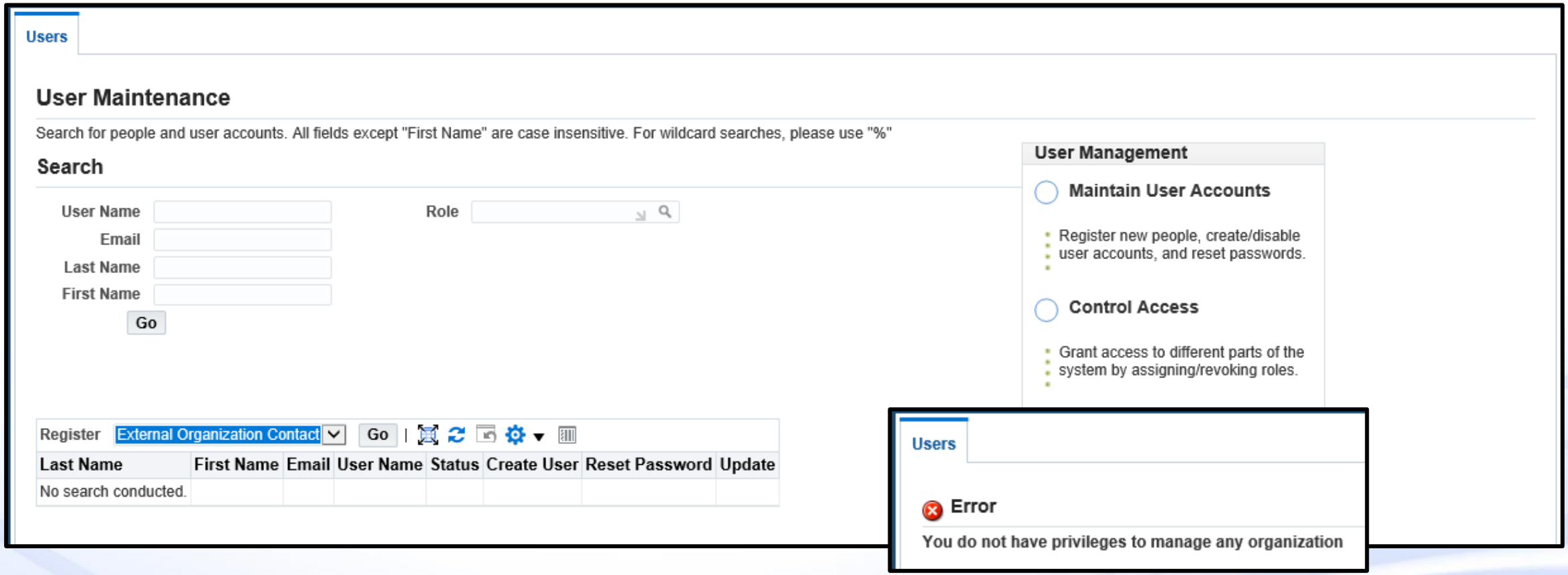
User Management : Security Administration Setup – Results
User Administration

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



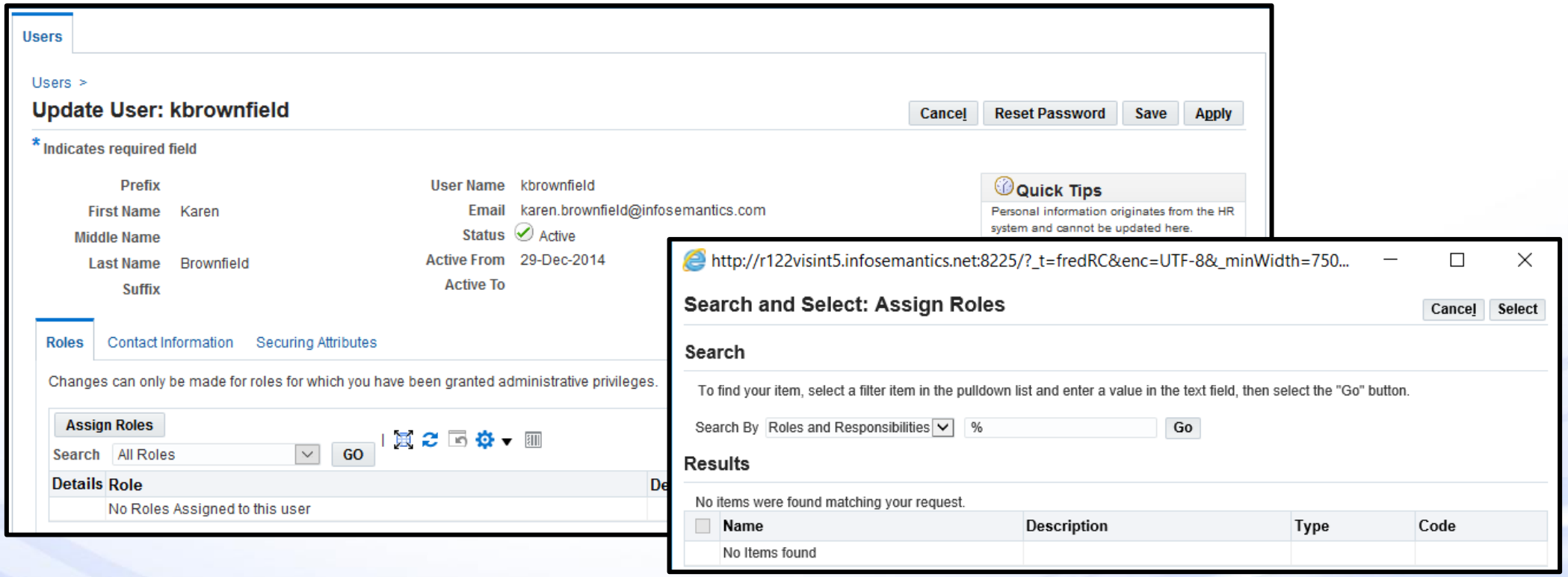
User Management : Security Administration Setup – Results
User Administration

- Does not allow creation of External Organization Contact



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

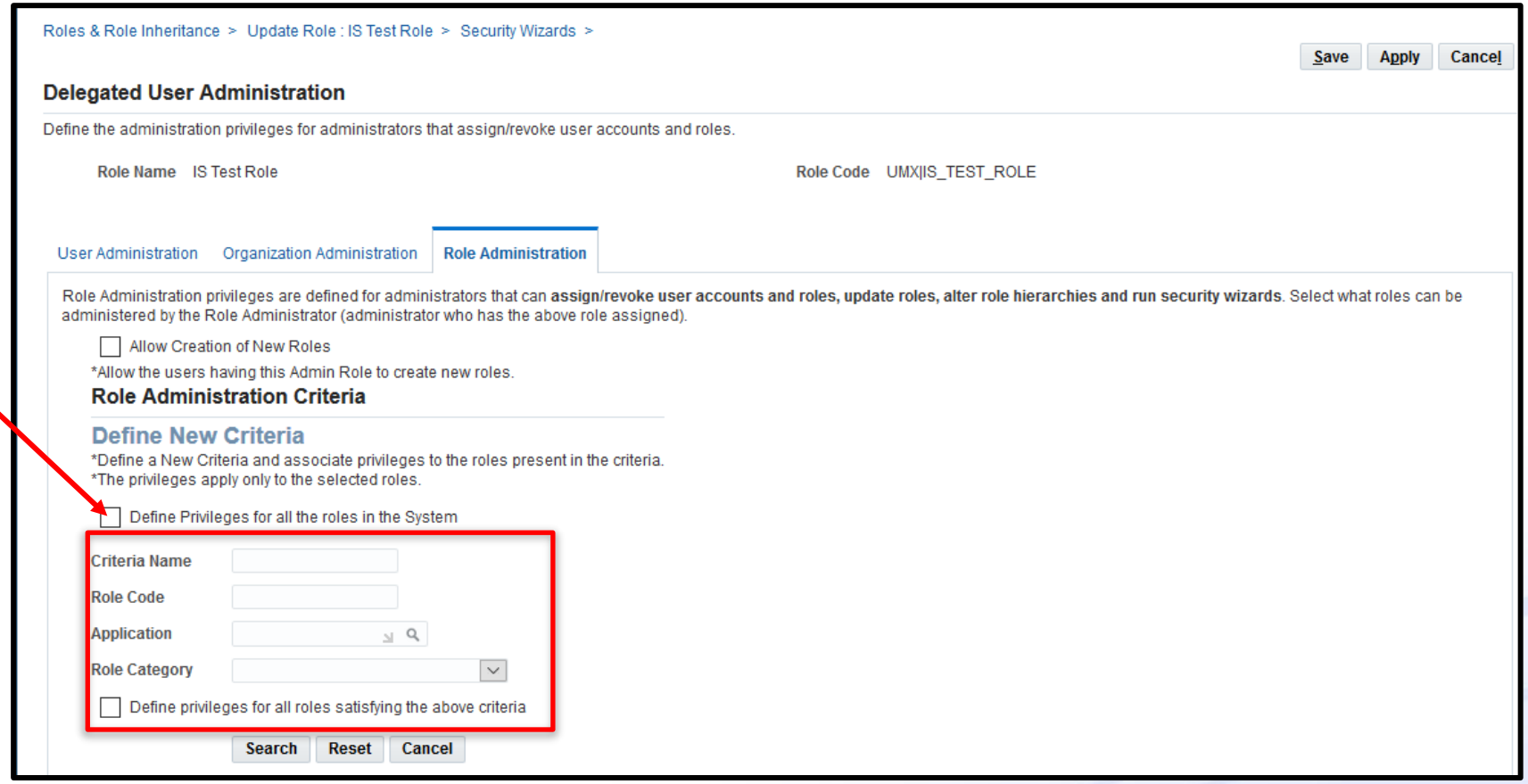


User Management : Security Administration Setup
Role Administration

- 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**

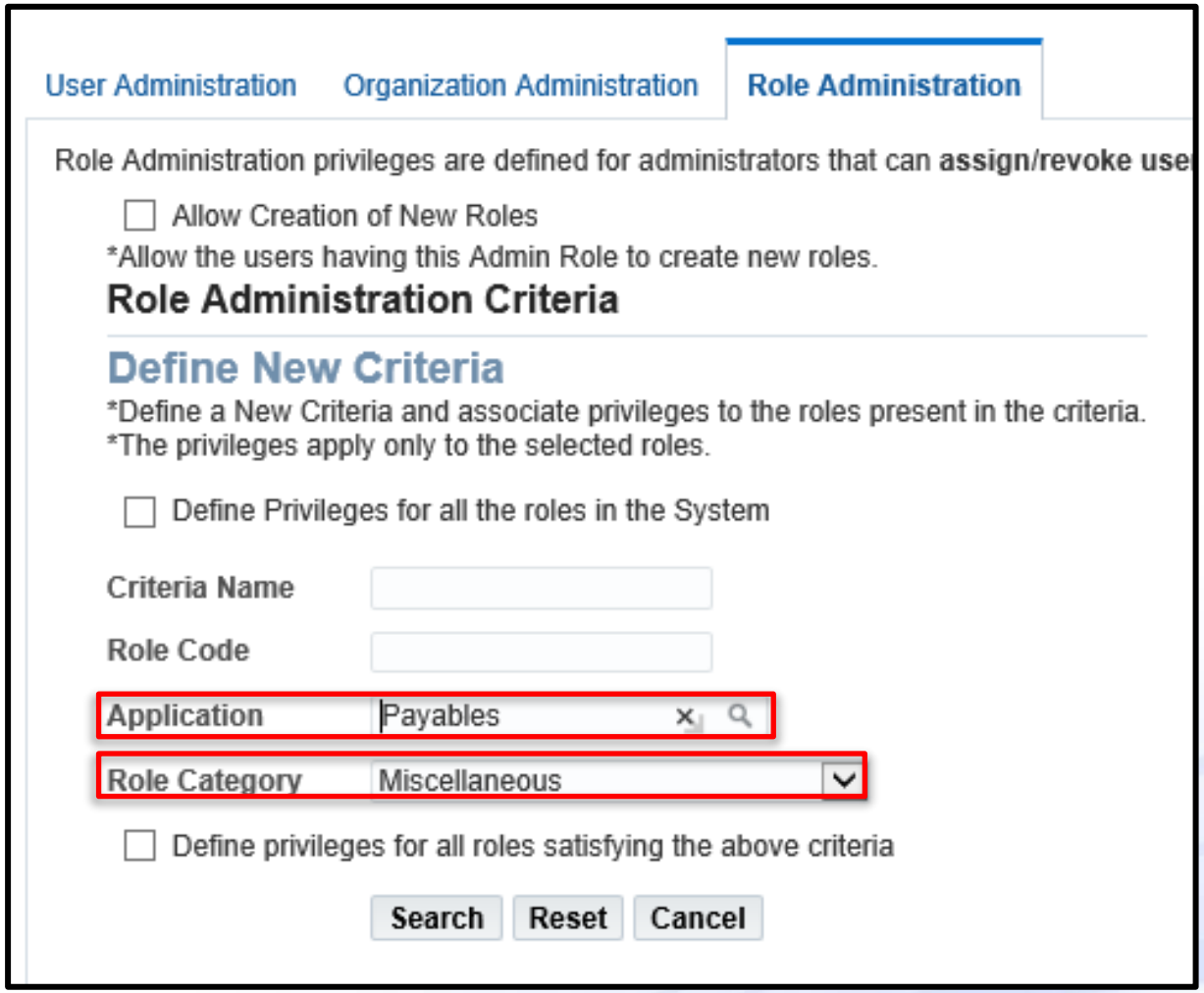
User Management : Security Administration Setup
Role Administration

- 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



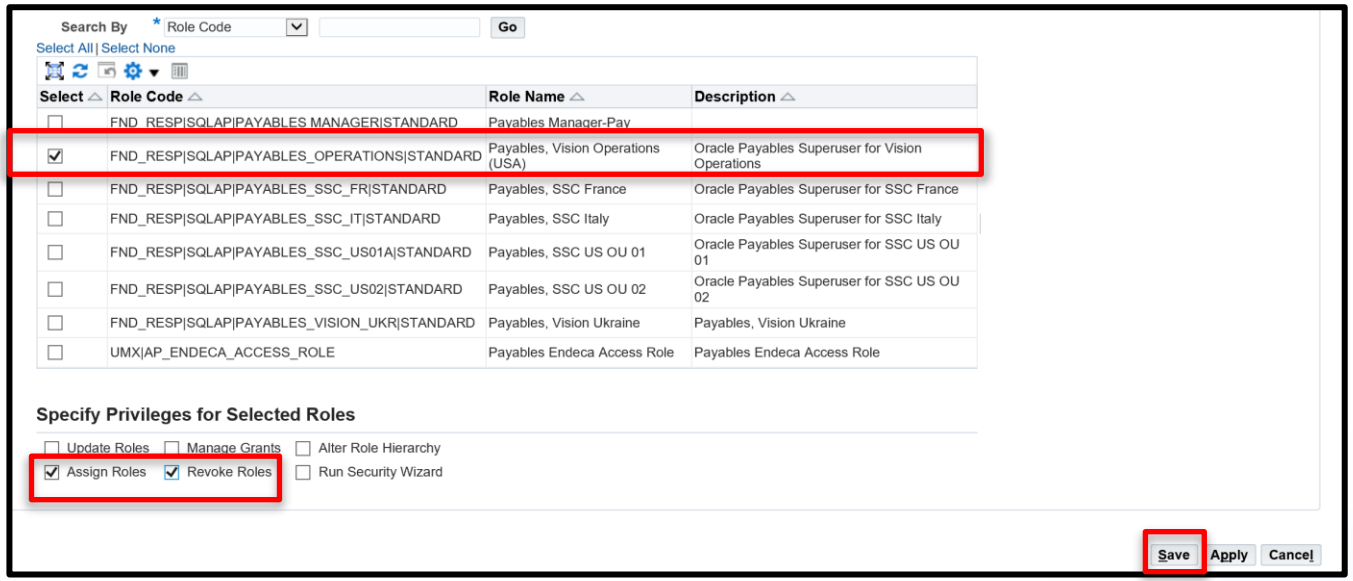
User Management : Security Administration Setup
Role Administration

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



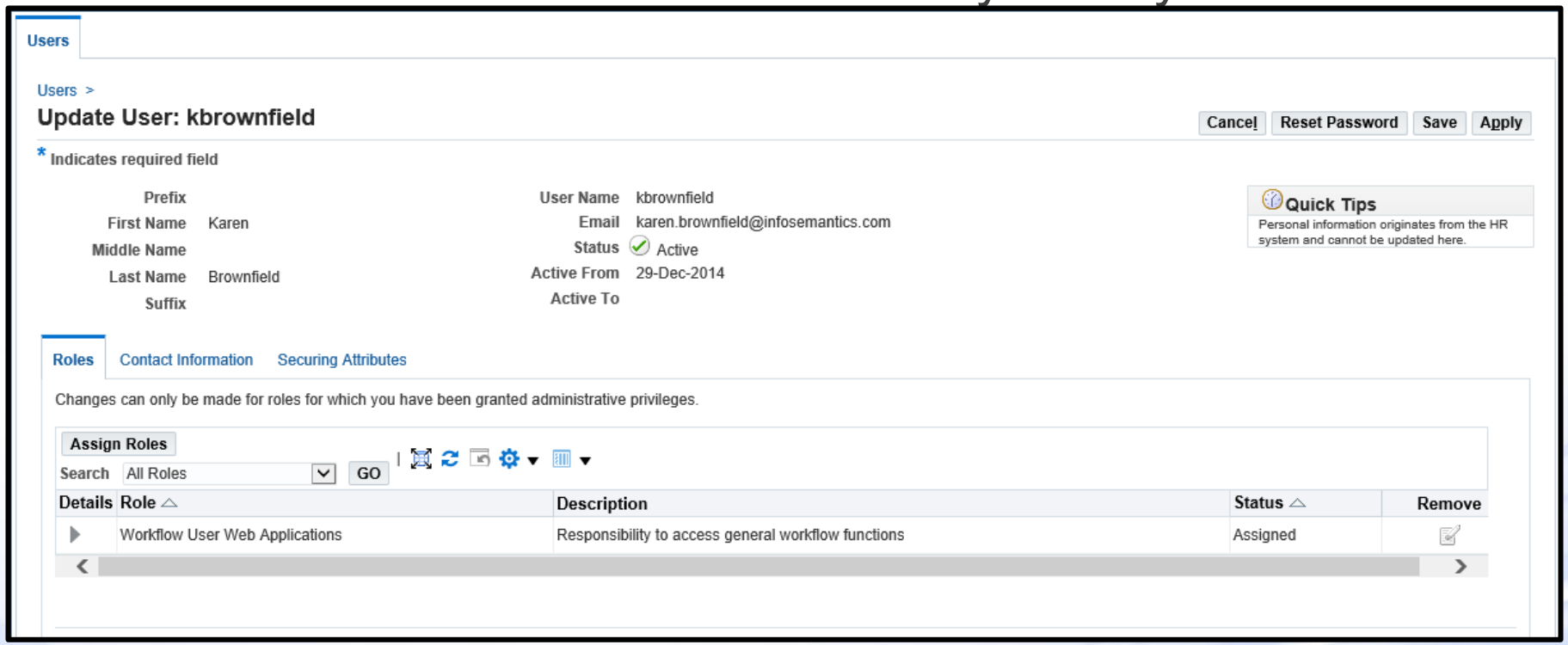
User Management : Security Administration Setup
Role Administration

- 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



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?

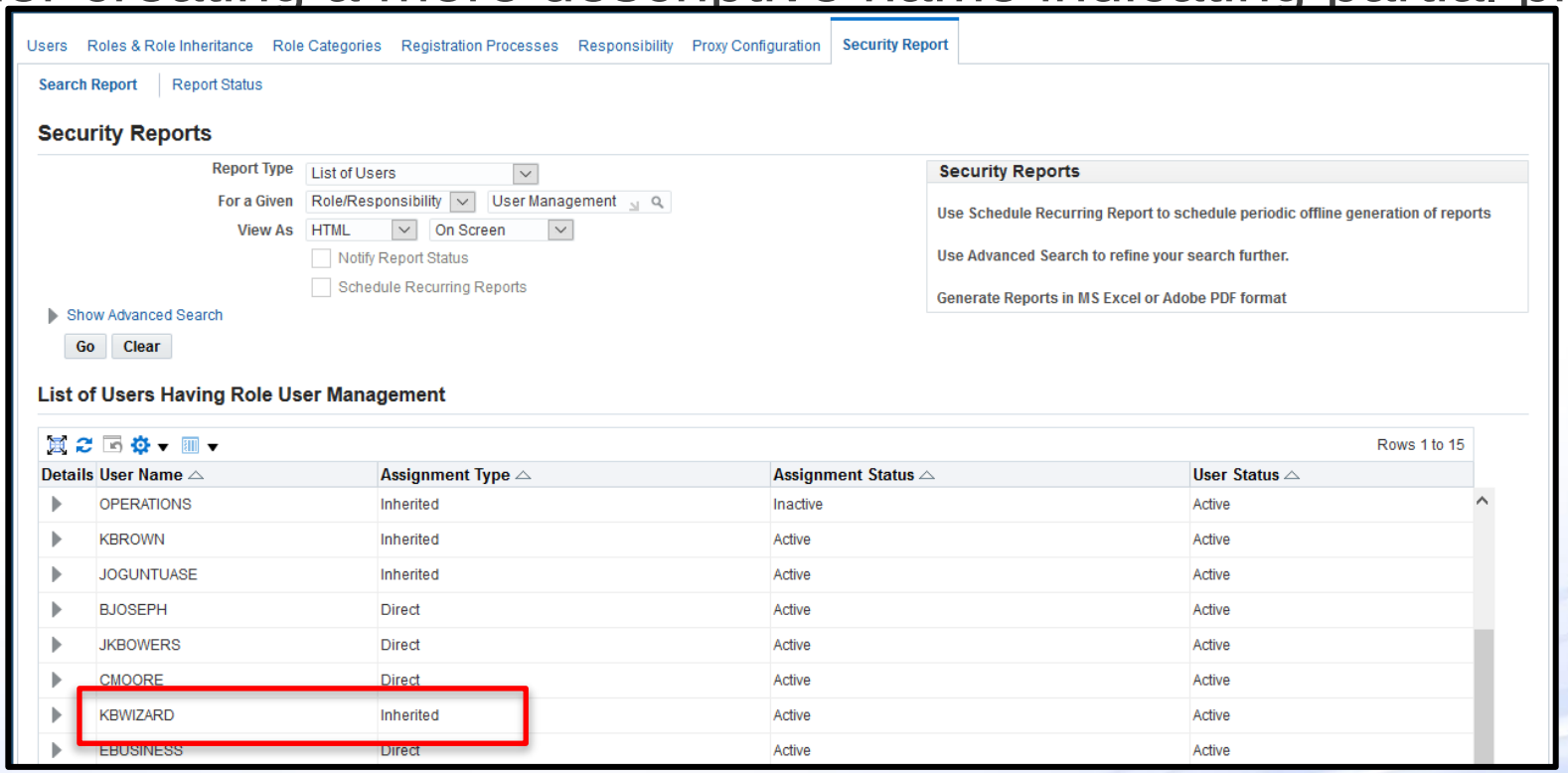


User Management : Security Administration Setup - Results Role Administration

- 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 accidently 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 priviledges



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**

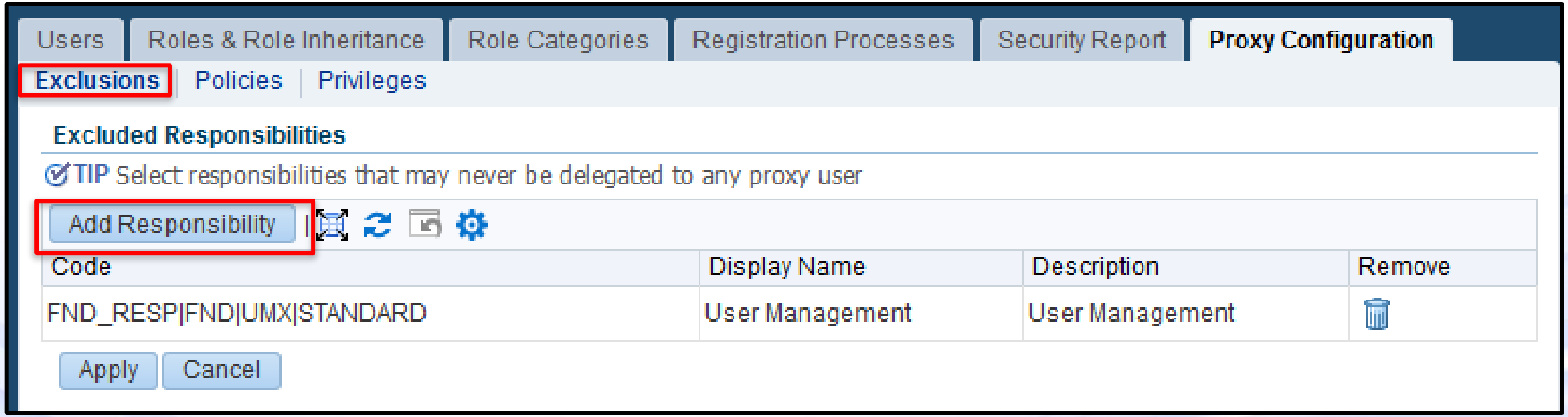
Proxy Users

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

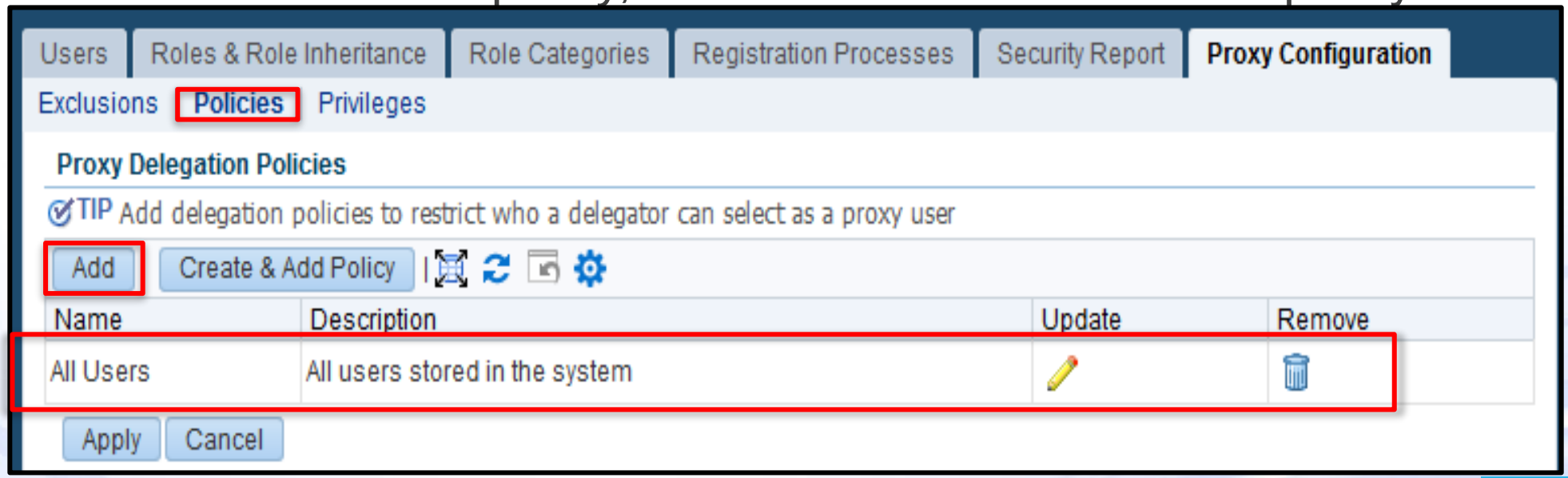
Proxy Configuration – 12.2.4+

- 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



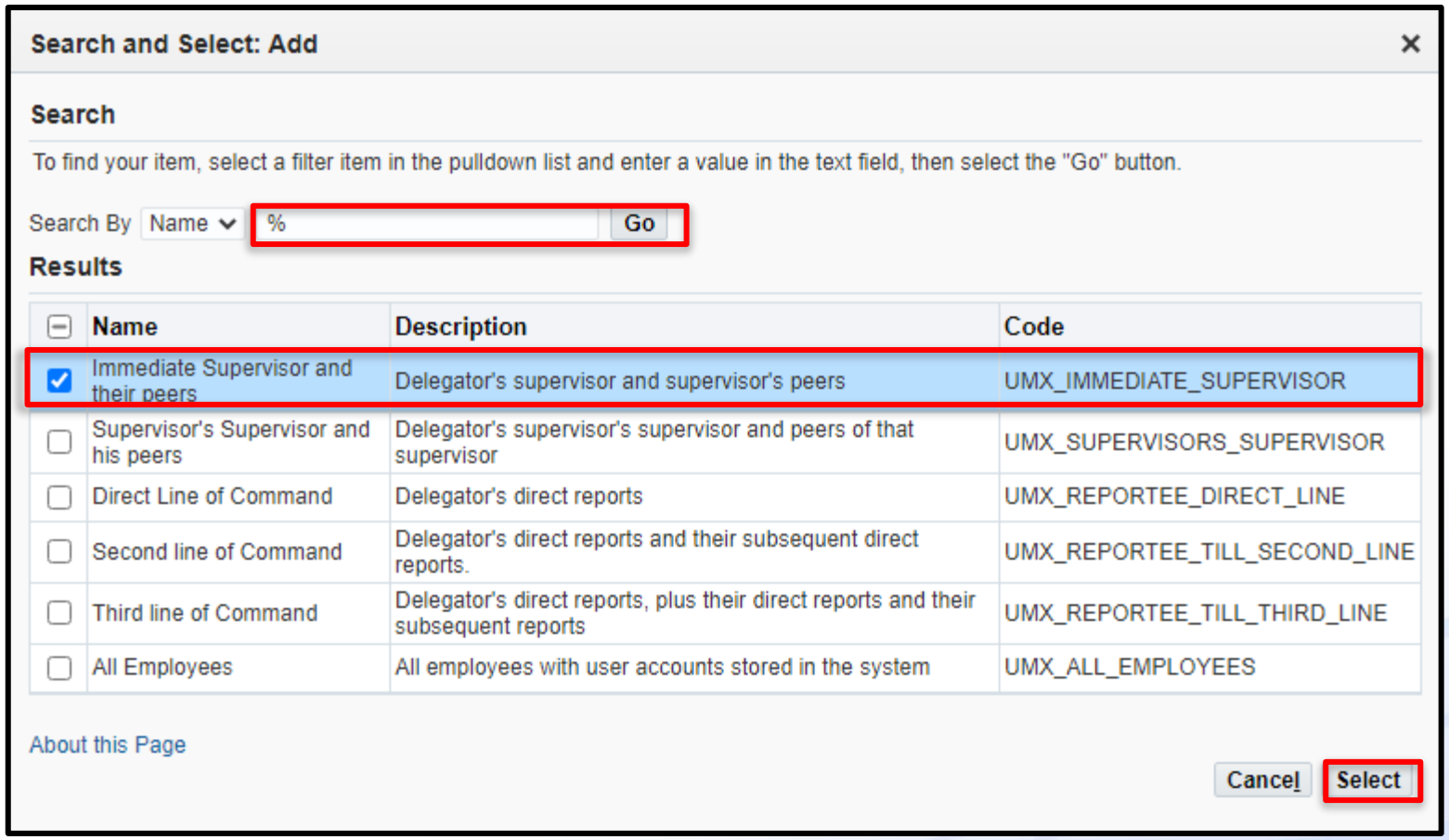
Proxy Configuration – 12.2.4+

- 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



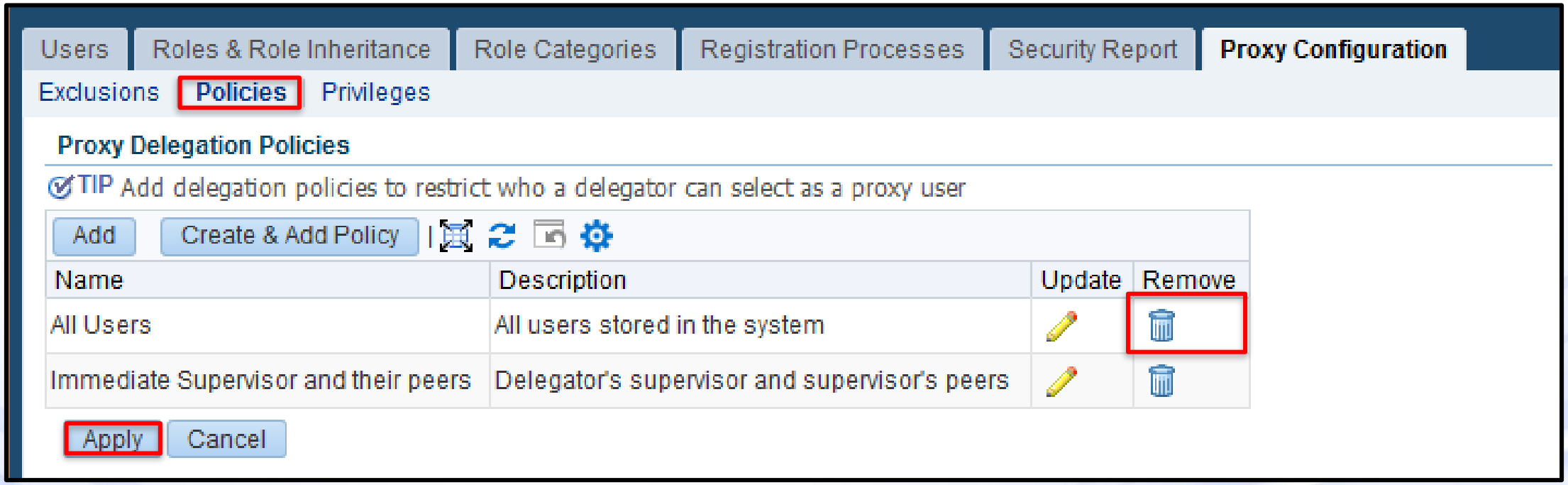
Proxy Configuration – 12.2.4+

- 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**



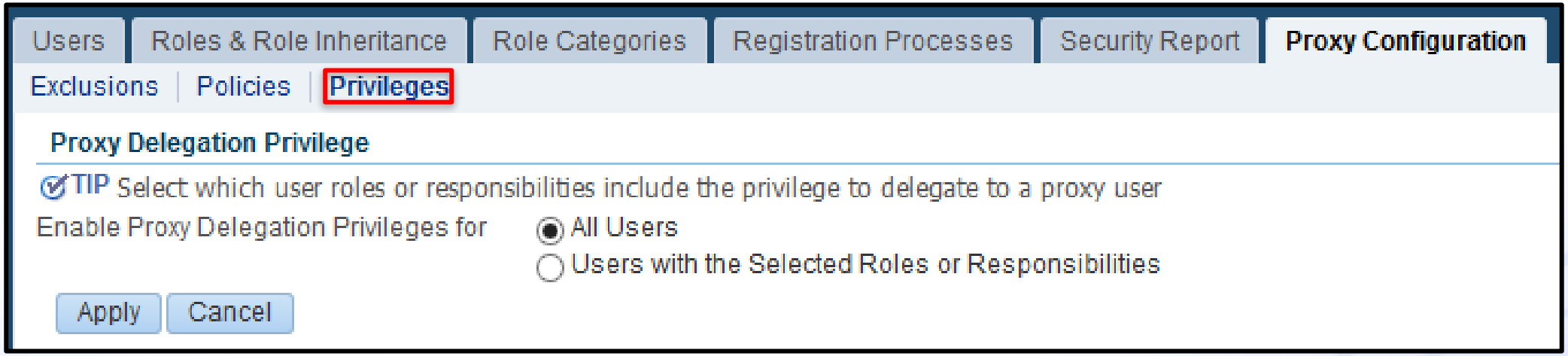
Proxy Configuration – 12.2.4+

- 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**



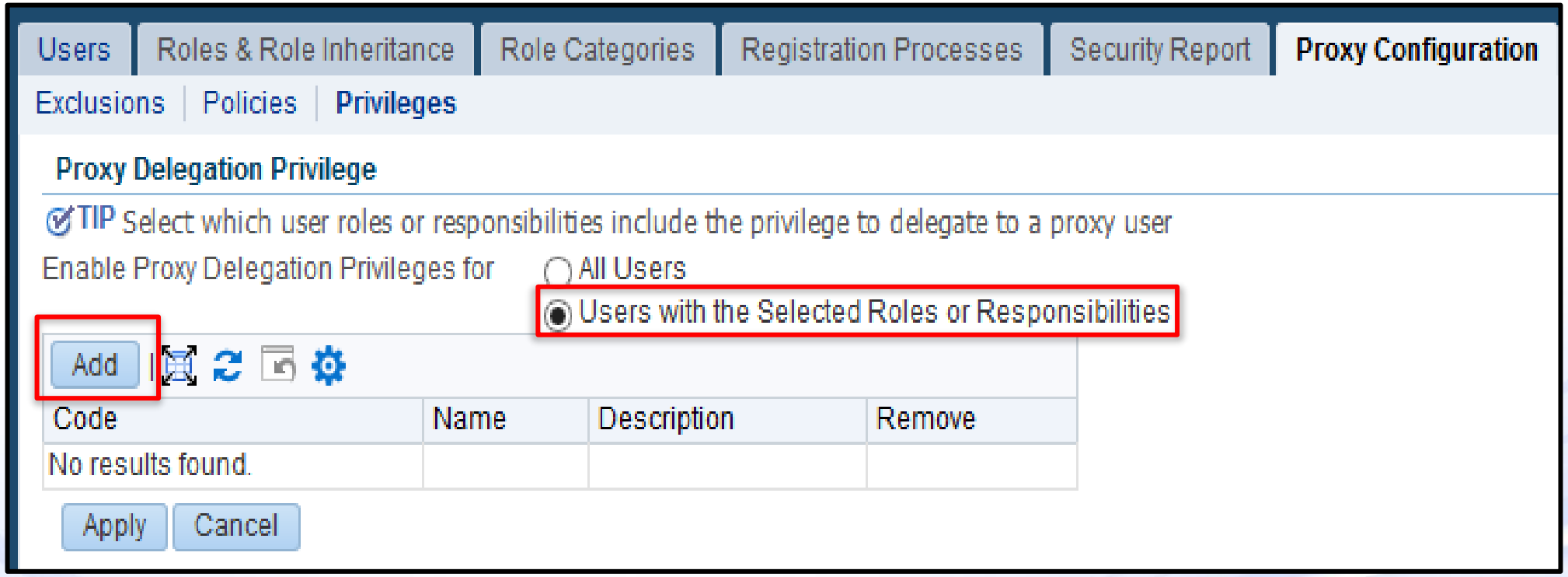
Proxy Configuration – 12.2.4+

- 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)



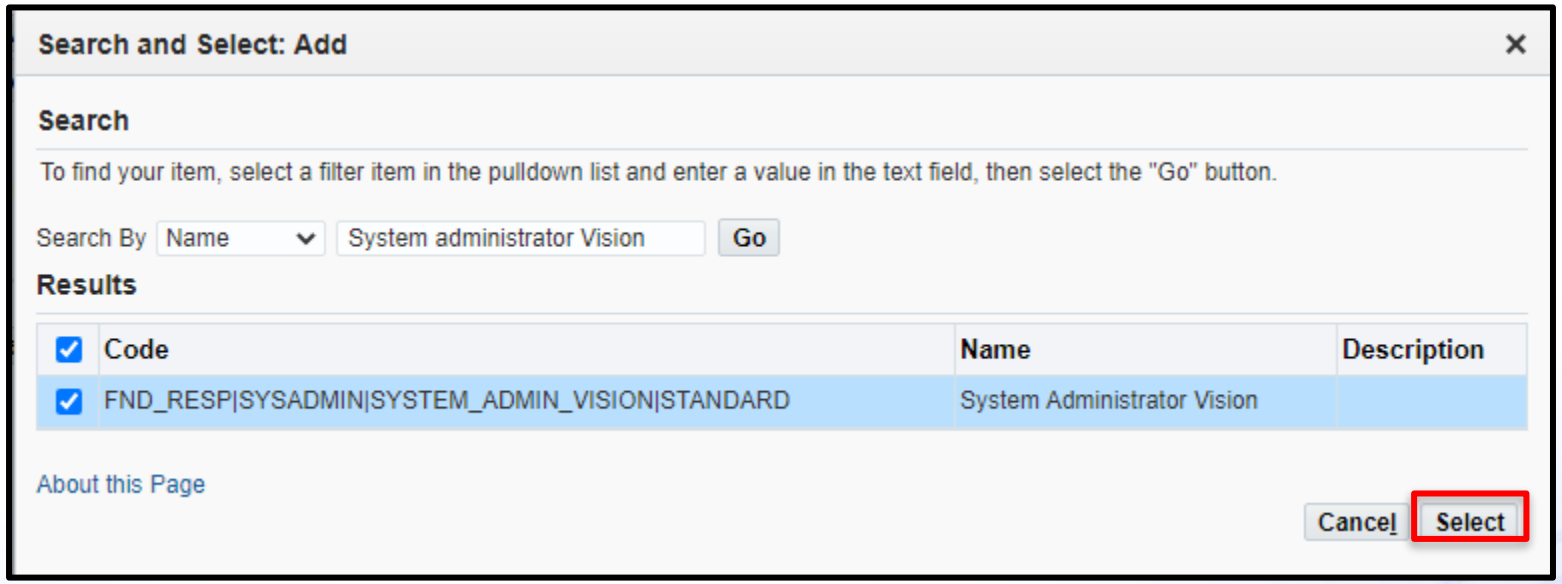
Proxy Configuration – 12.2.4+

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



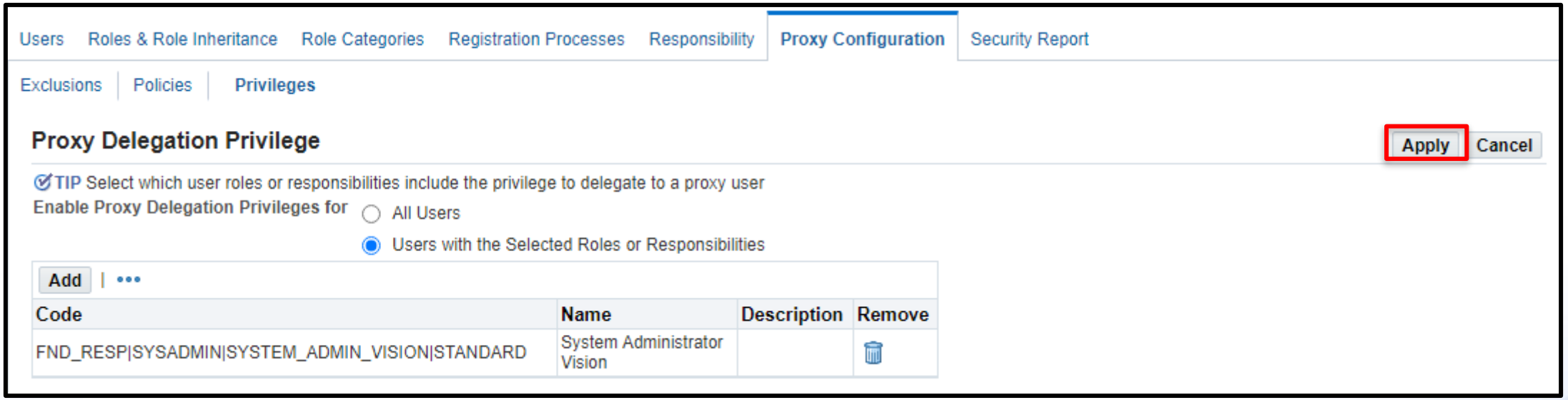
Proxy Configuration – 12.2.4+

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



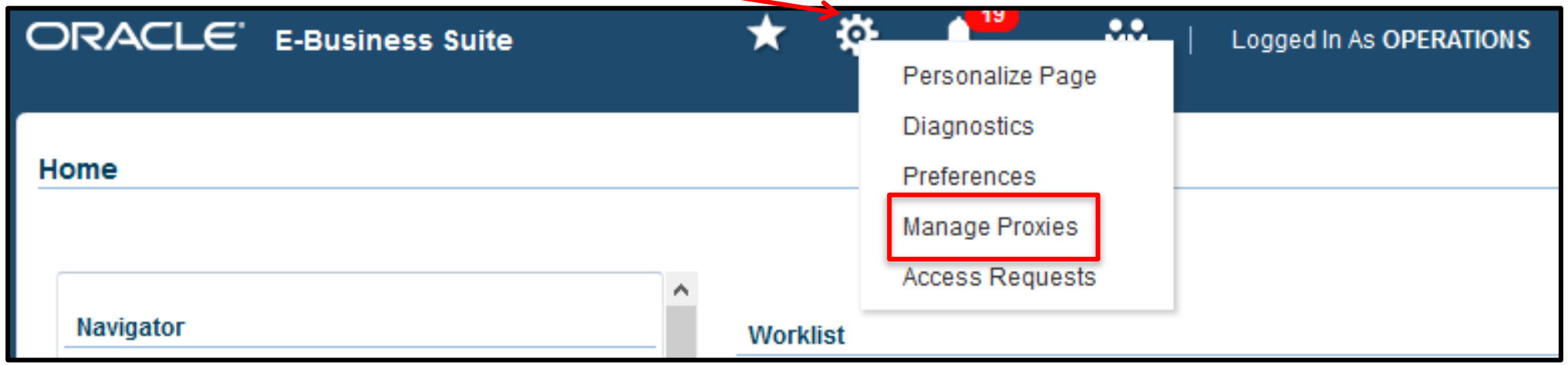
Proxy Configuration – 12.2.4+

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



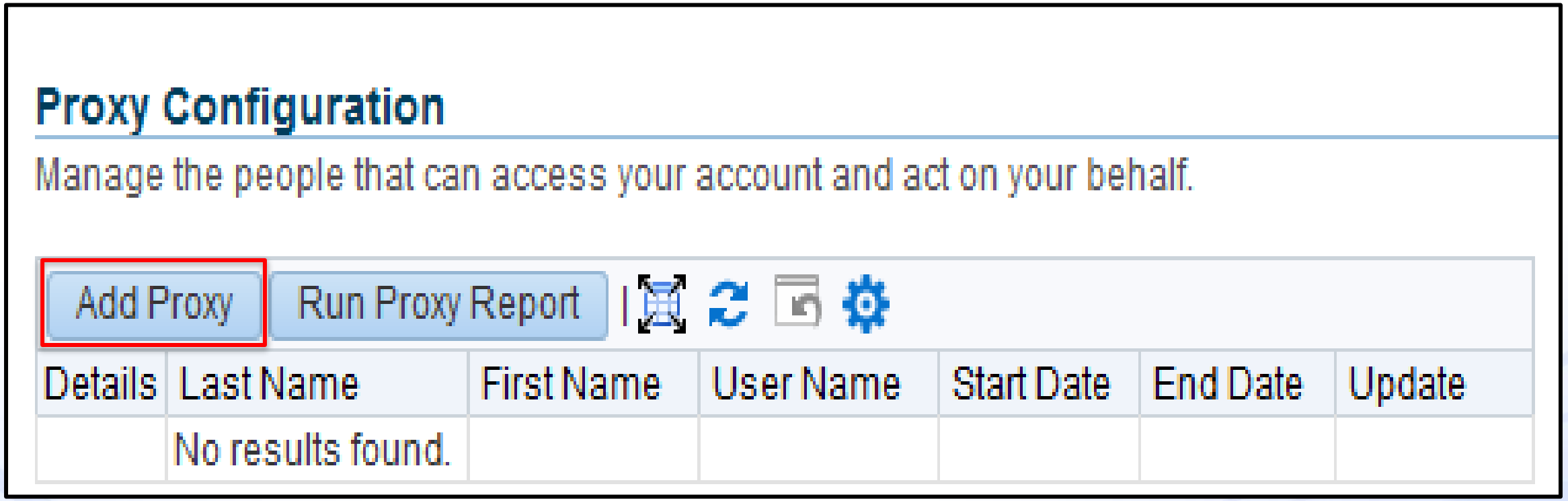
Proxies – 12.2.4+

- Click the settings gear, then Manage Proxies



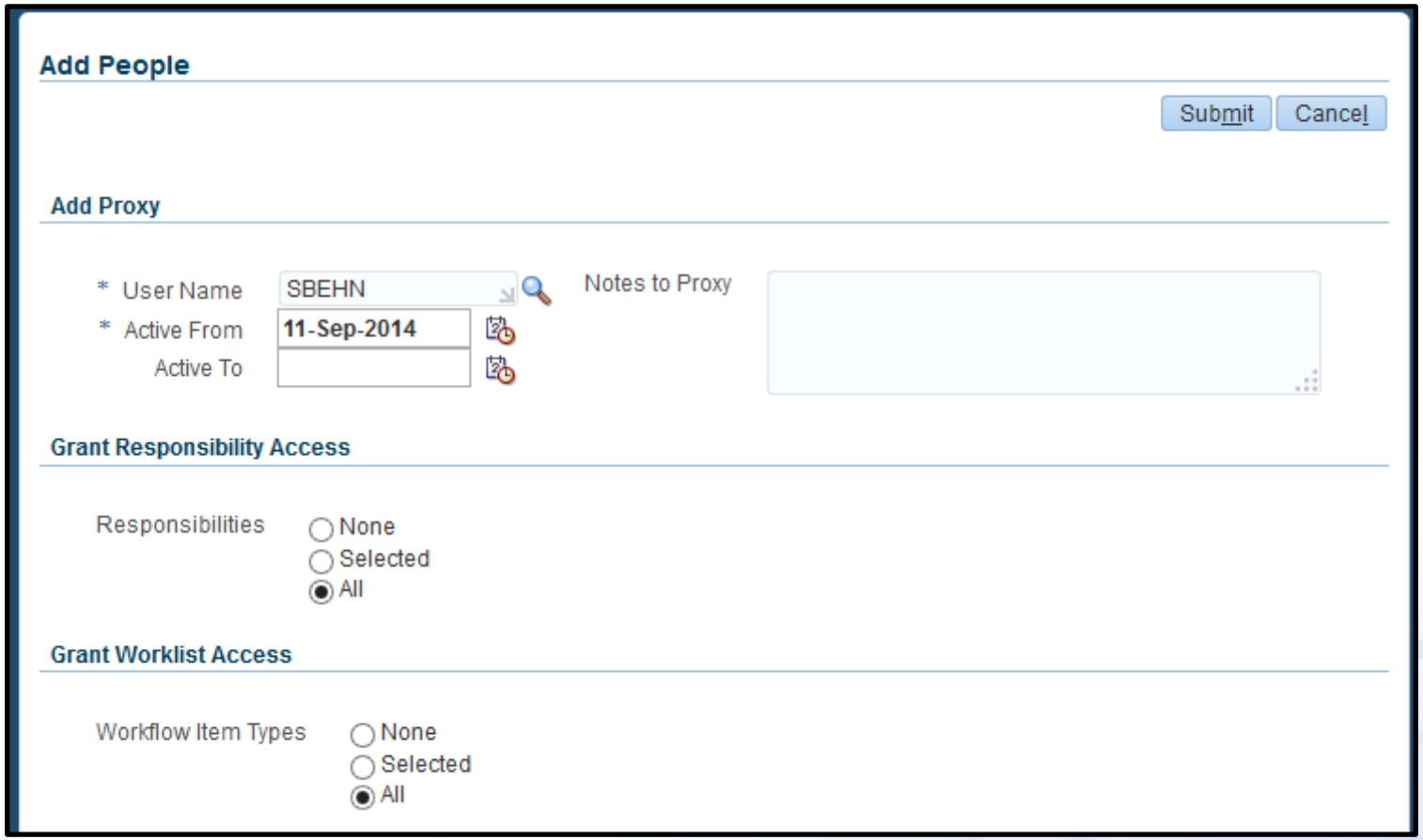
Proxies – 12.2.4+

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



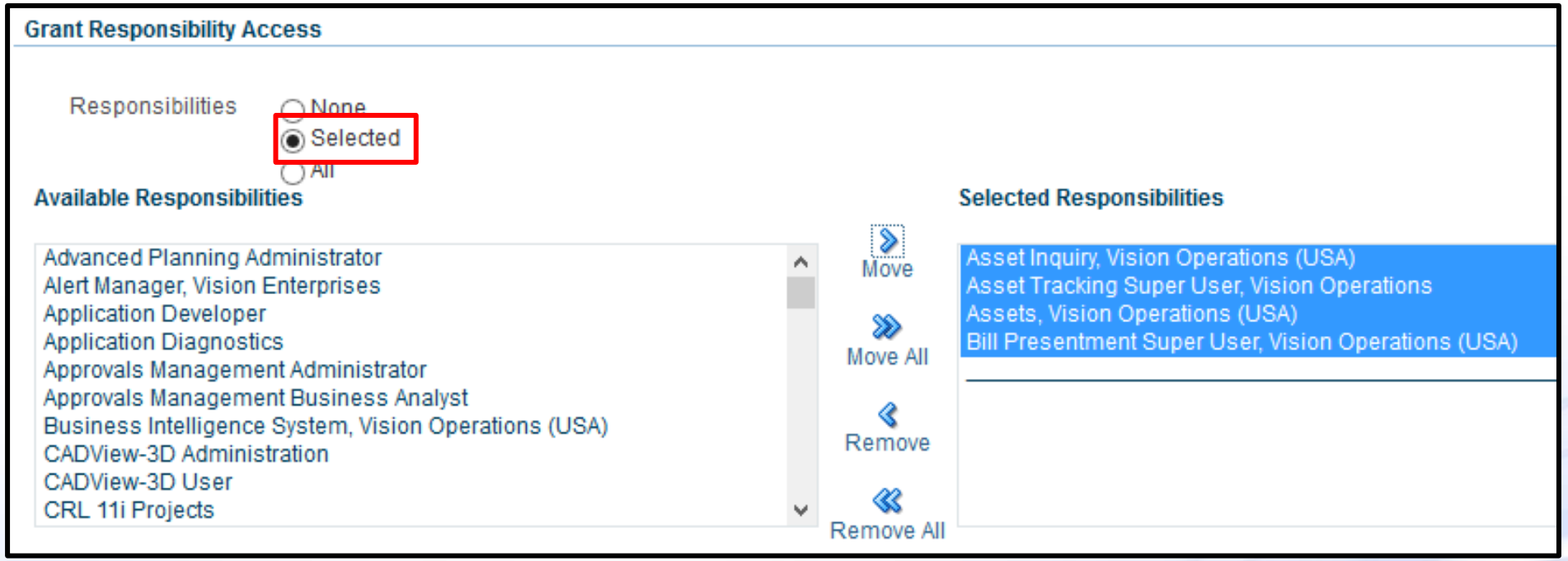
Proxies – 12.2.4+

- 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



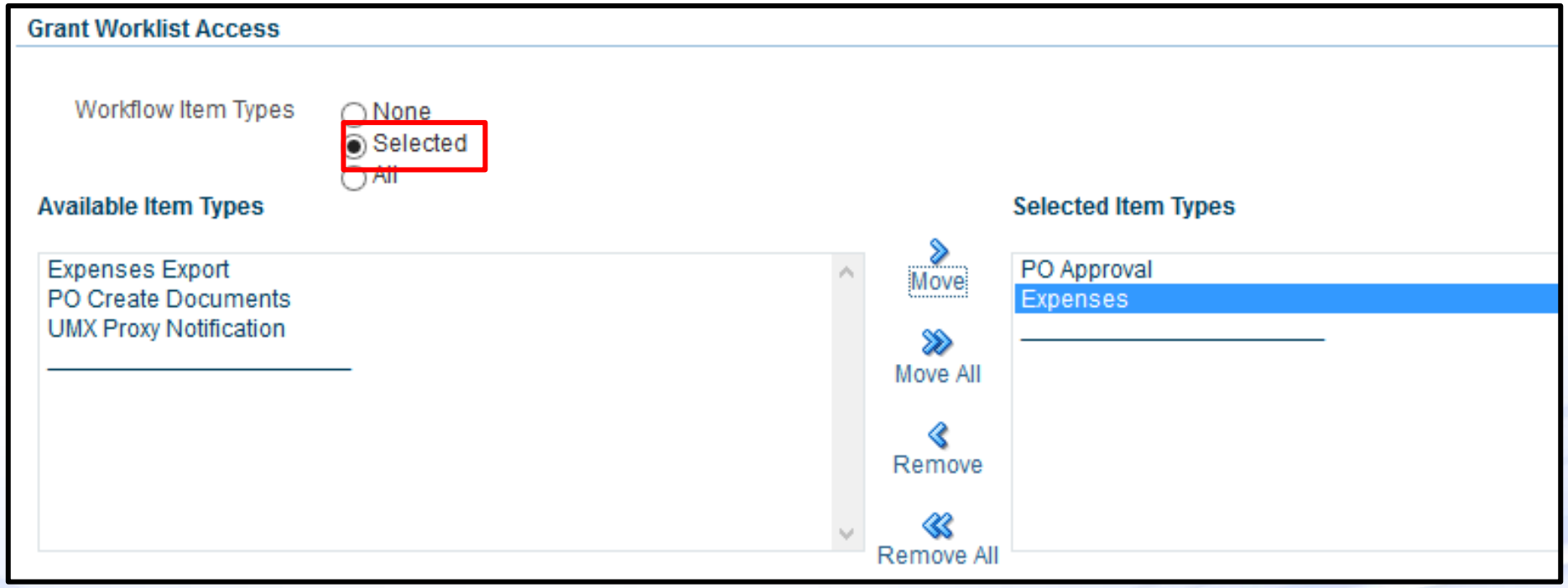
Proxies – 12.2.4+

- 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



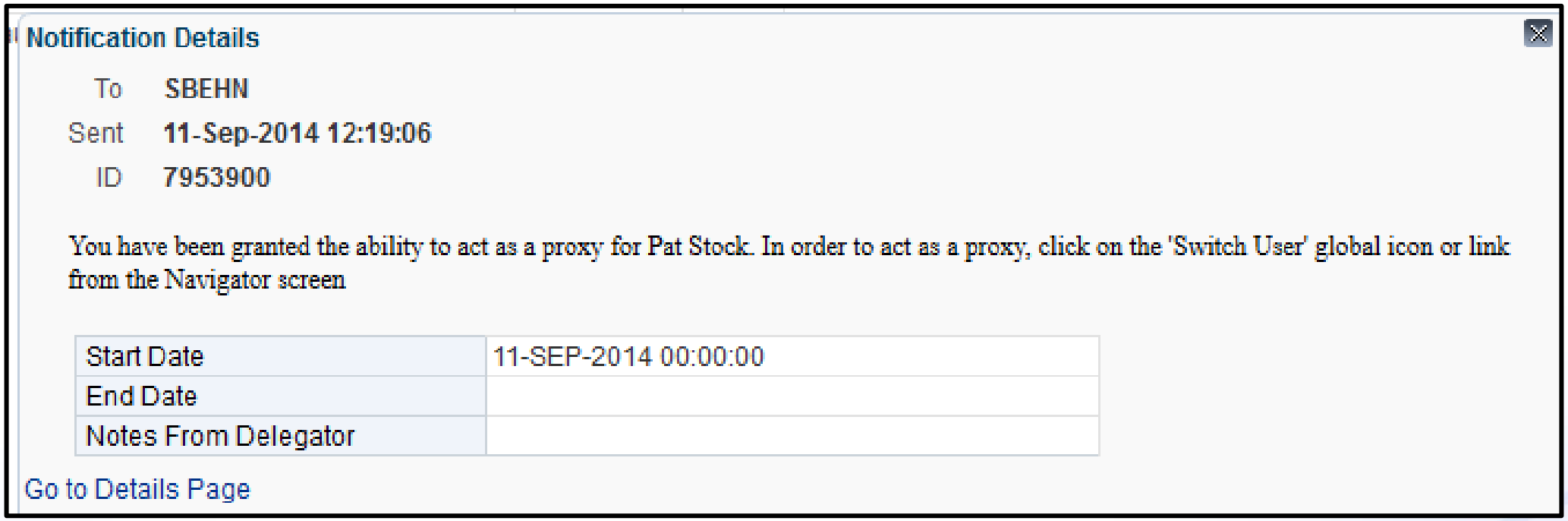
Proxies – 12.2.4+

- 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**



Proxies – 12.2.4+

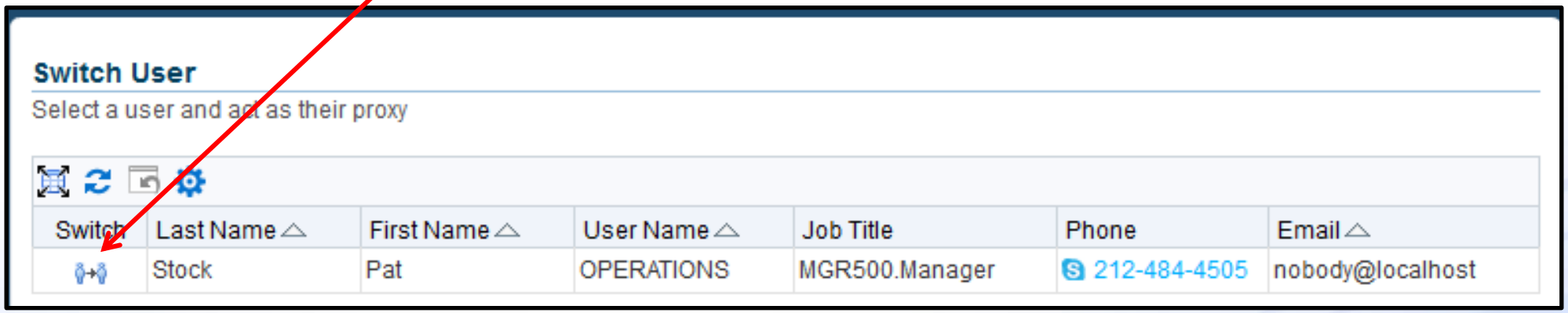
- A workflow notification is sent to the user who is granted proxy access



Proxies – 12.2.4+

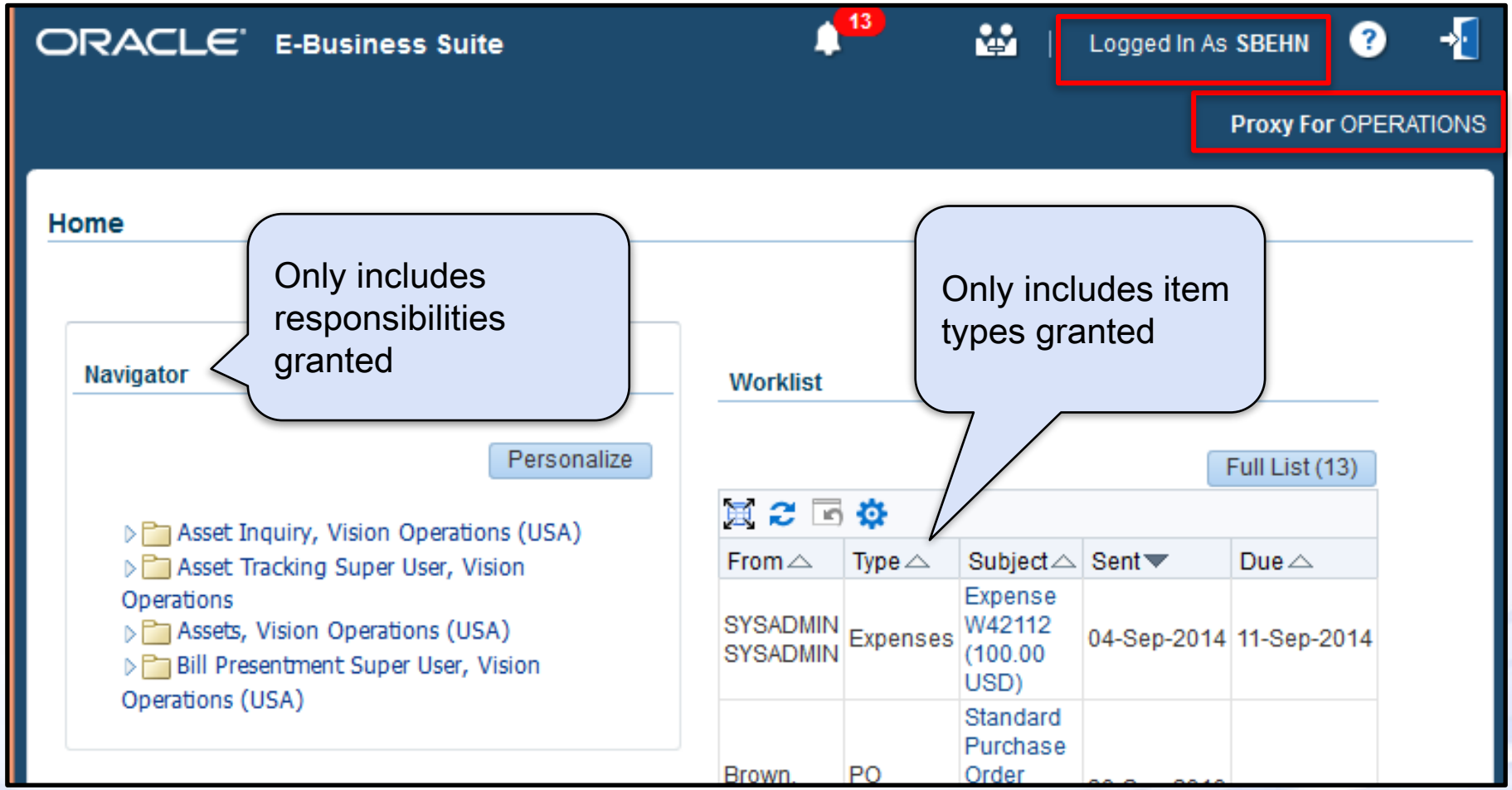
- As the SBEHN user, click the switch user icon

- Then click the switch icon



Proxies – 12.2.4+

- Now logged in as SBEHN as Proxy for Operations



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 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