PeopleSoft Security Administrator Training 101

September 2015
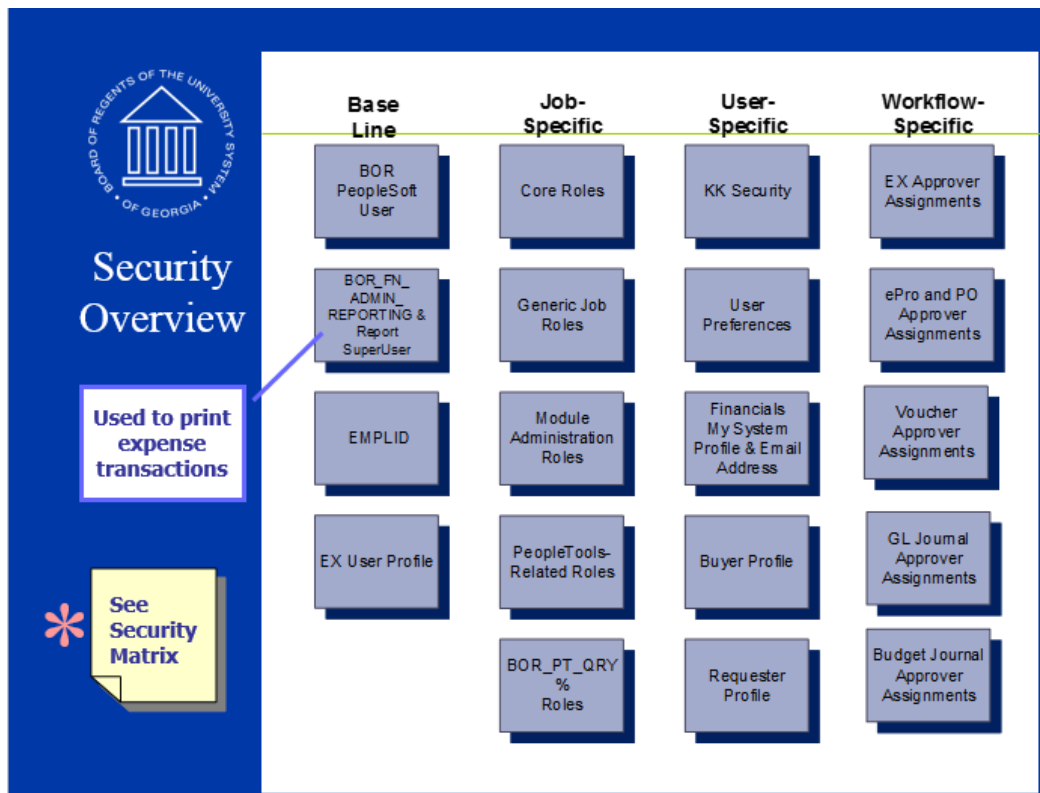
Contents

PeopleSoft Security Basics

Security Design Strategy

Before we get into Security, let's discuss the Financials Security Design Philosophy. The Model Roles are "granular" and they are based upon specific business processes. The specific access needed to complete a job/business process is mapped into corresponding role/roles. Some business processes require only one role to complete. More complex business processes may require multiple roles to complete. Our granular approach promotes flexibility across institutions and reduces the risk of segregation of duties issues. ITS designs and creates the roles and permission lists, and allows the institutions to administer the delivered roles to their individual users through a distributed user profile. We will cover this a little more in the security administration area of this document.

Managing User Security
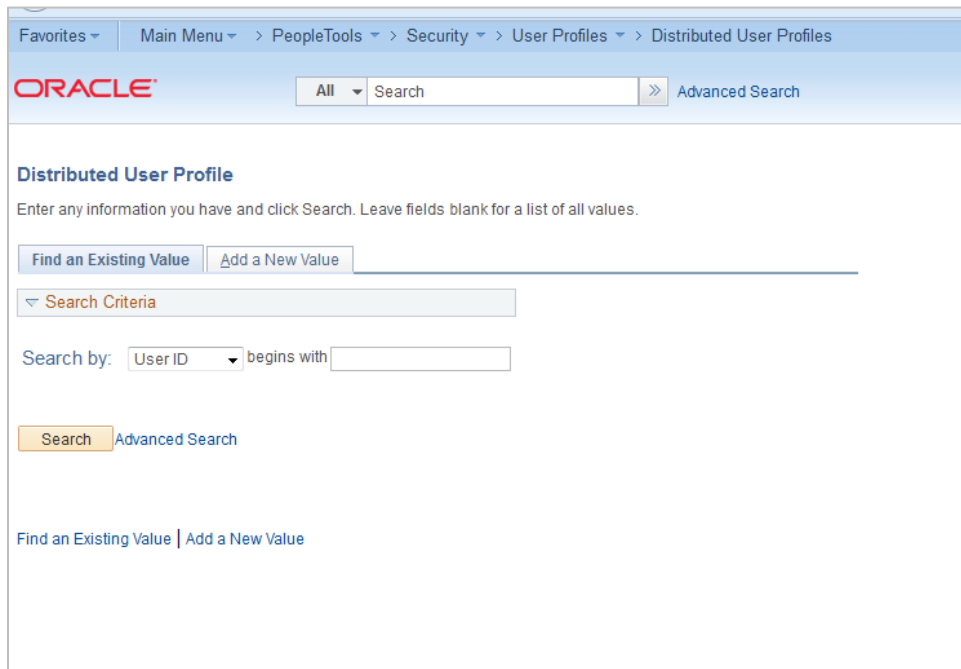
User Profiles

User Profiles define individual PeopleSoft users. You define user profiles and then link them to one or more roles. A user profile must be linked to at least one role in order for it to be a valid profile. The majority of values (permissions) that make up a user profile are inherited from the linked roles.

> Note: It's possible to have a User Profile with no Roles. This might be a user that isn't allowed access to the PeopleSoft application; however, you want them to have workflow generated emails sent to them.

You define User Profiles by entering the appropriate values in the User Profile pages. The User Profile contains values that are specific to a user such as a user password, and email address, and employee ID, and so on.

You can click on **Add a New Value** to create a new Profile or use the **Copy User Profile** feature to duplicate a similar profile. The name of your new profile will need to be unique from the one you are about to copy. The User ID in this case is a Kew Field. People Tools version 8.5+ allows you the naming length of up to 30 characters.
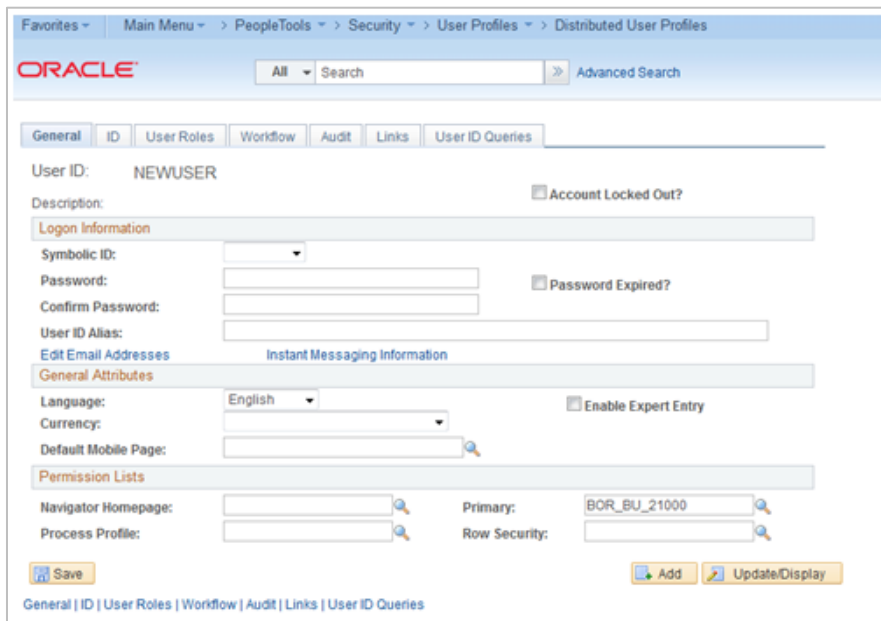
General Tab

Type in the name of your new profile and click the **Add** button. The User ID should be a unique value and it is suggested that it not be tied to the user's name. The name that you specify cannot contain any white space or any of the following specials characters:

```
;  :  &  ,  <  >  \  /  "  [  ]  (  )
```


As you can see, the User Profile General Tab is more specific and requires more data than both the Role and Permission list. Start by entering the Symbolic ID. Click the down arrow and select the system default (SYSADM1). Users that will only be authenticating through a Directory will not need a Symbolic ID for access into the system.

Symbolic ID

Associated with a user's encrypted Access ID and Access Password. The correct Symbolic ID must be entered to retrieve the appropriate Access ID and password for sign on. This value determines what Access ID and password is used to log the user onto the database after the system validates their User ID.

The Access ID is only required when a user needs to connect directly to the database (in two-tier). The Access ID is not required with the portal or if you use an LDAP directory server to manage user IDs.

With PIA, the application server maintains the connection to the database so the application server must submit an Access ID.

Enter a password and then confirm the password by entering it again in the Confirm Password field. This password should conform to existing password constraints set in the system.

When a password is entered, the system will automatically make the password longer and return dots (pictured above) after you have entered the password and saved the profile. See Appendix A for more information about passwords.

Password Controls

Control	Setting
Enable Signon PeopleCode	**YES**
AGE	Password Expires in **180** Days
	Warn for **5** Days
Account Lockout	**5** Maximum Logon Attempts
Miscellaneous	**DO NOT** Allow password to match User ID
Minimum Length	10 Minimum Password Length
Character Requirements	1 UpperCase
	2 Required Number of Digits
Purge User Profiles	N/A
Password History	**8** Number of Passwords to Retain

The only other possible required fields to complete on the General tab are the Process Profile and Primary Level fields in the Permission list portion of the page.

Note: This is the only instance where a Permission list is attached directly to the User Profile.

The Process Profile permission list enables what features of Process Monitor operations the User will have and can control what processes a user has access to. In the USG model, we have not separated processes out into different permission lists. They are all contained in one. Below is the text from PeopleBooks.

Just as you define permissions for the pages a user can access, you also must specify the batch (and online) processes that users can invoke through PeopleSoft Process Scheduler. Typically, process groups are arranged by department or task. For example, the batch programs used by your payroll department probably all belong to the PAYROLL process group, or a similarly named group.
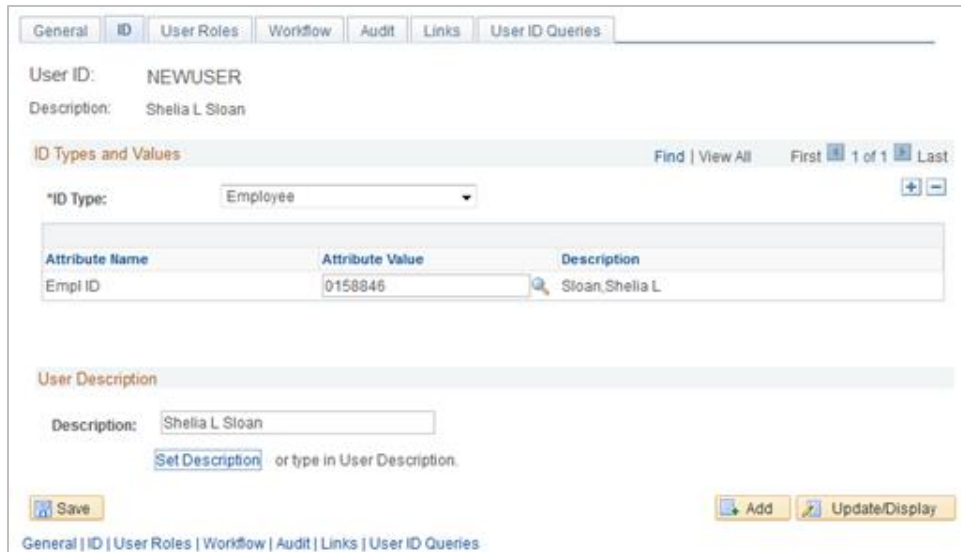
When you create a process permission list, you add the appropriate process groups so that a user belonging to a particular role can invoke the proper batch programs to complete their business transactions. You do this using the Process Group Permission page.

You use the Process Profile Permission page to specify when a user or role can modify certain PeopleSoft Process Scheduler settings.

Note: You grant Process Profile permissions directly to the user profile and Process Group permissions through permission lists.

The Primary field will determine what data or row level security settings the User will have. These Permission Lists will be defined in our Security design matrix and assigned to each user accordingly. This is what specifies what Business unit data the user can access. It will default in according to the primary permission of the local security administrator.

.

ID Tab

The next tab on the User Profile is the ID tab. This tab is used to set the ID type for the user. For end users who are employees, this will be set to Employee. After setting the ID type to Employee, the Attribute field will be activated.

You will be required to complete the Attribute Value filed before you can save the Profile. This field should match the User ID from the first page on the profile. For quick lookup and validation, type in the first several digits and click the **Lookup** button. The description field should match the name of the user.

Roles Tab
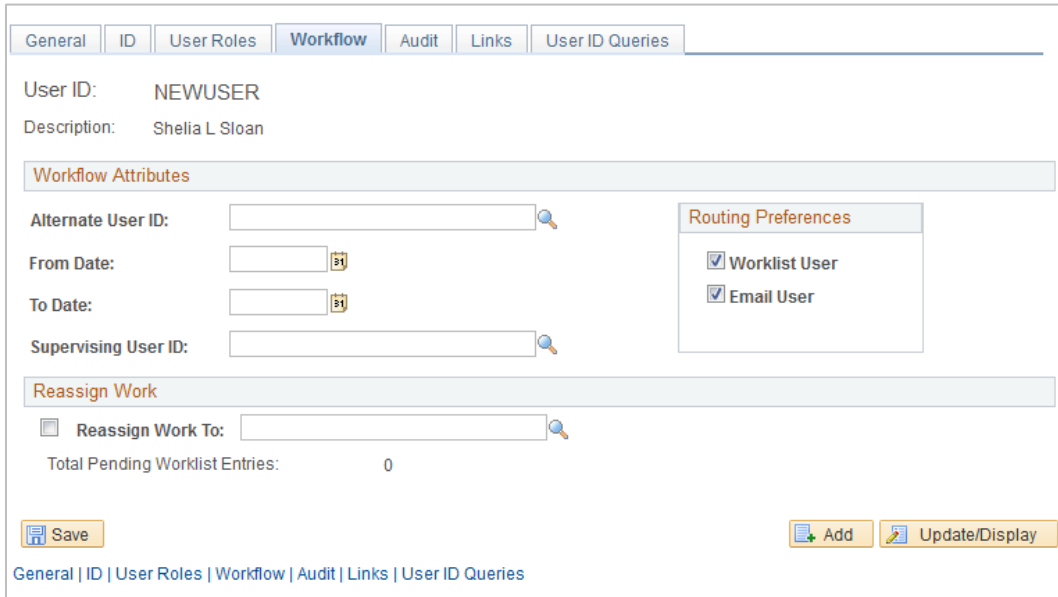
The Roles tab is where you attach the functional and system roles you need to complete the profile definition. Each Generic Job profile will be defined in the Security Design matrix document and built according to this design. Job profiles will be categorized by business processes as defined by the functional end user team and the roles will enable each member of the team to navigate processes and reports according to these business process requirements. Each profile will have one to many roles attached on this page. Some will be business functional roles and others will be system roles (ie Query, Report Manager). Once the appropriate roles are attached, click the save button and your profile is completed.

Workflow Tab:

The Workflow tab is where you define routing preferences or workflow attributes. For Routing Preferences, select Worklist User if the user is an approver or may receive a system notification in their worklist. This is selected by default, and I suggest leaving it checked for active employees.

The Email user checkbox allows end users to receive system notifications via email. This notifications will be sent to the email address on the user's general tab. This is selected by default, and I suggest leaving it checked for active employees.

The Workflow Attributes section allows a user to have an alternate approver defined. If This individual is an approver, but they are going to be out of the office for a predefined date range, they can redirect their approvals to a specified User id for a date range.
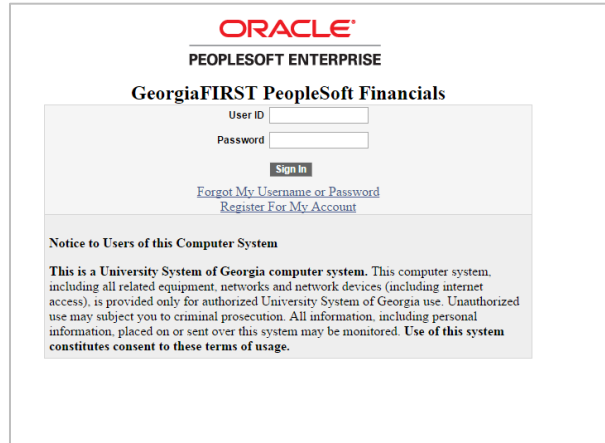
**I have seen where after this can cause issues after the date range has expired. Sometimes if the person that was listed as the alternate leaves the institution and goes to a different institution, it can cause a multi campus user error to flag on this user profile the next time it has changed. The other issue I have encountered is with routing to the alternate even after the date range has expired. I suggest running a query to identify all of your alternate users and clearing them out after the date has expired.

The Reassign work to section, allows the security administrator to reassign ALL transactions in this individuals worklist to a new approver if that person is gone or on extended leave.
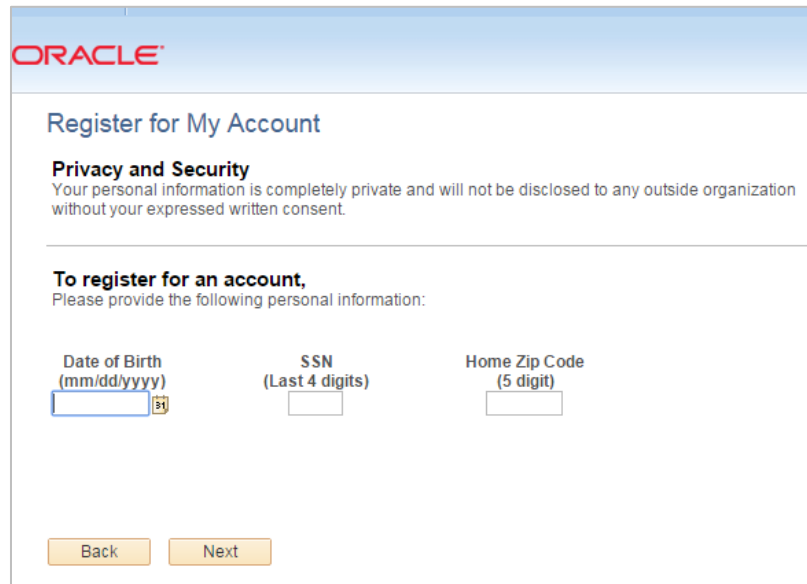
**This will reassign EVERYTHING. If this person is a ePro Approver and a GL Approver, it will send all Requisition and Journal approvals to the person you identify. It cannot separate them out. If the GL transactions need to go to a different approver than the ePro transactions, use the Monitor Worklist page to reassign these transactions individually.

The other way to create user ids is through self-registration. Have the new employee login to the self service site at fprod-selfservice.gafirst.usg.edu.

Click on Register for My account:

Once you are there, fill in the required fields:

It will pull up the job row for the employee that is self registering. They need to click the box beside the active job row and select next. At this point the user can create their own user id, and setup their password and email address. At this point, registration is complete. They have to sign out and sign in with their newly created user id and password.

This provides the employee with Basic sign in rights and if their institution uses expenses, ijt assigns the basic expenses access required to create expense transactions and print expenses

transactions. No security form is required for self registered individuals until they need additional roles. At that point, approvals and documentation are required.

Roles (Dynamic vs. Static)

Roles are intermediate objects that exist between permission lists and user profiles. Hey are designed to aggregate permission lists so that you can arrange permissions into meaningful collections. Role definitions will align with the delivered business processes. Dynamic roles enable you to add permissions to users dynamically, which reduces administration tasks.

Currently, ITS only has one Dynamic Role and it is the BOR_EX_APPROVAL role. Any user who is on the Expenses Approver Assignments page automatically gets this role. Upon termination, the user should be removed form the Expenses Approver Assignments page. The role will automatically be removed from their user profile.

Note: In previous releases, roles were associated with PeopleSoft Workflow. PeopleTools has expanded their definitions to include system permissions. There is only one role definition, and you maintain this within Security.

Role users are the User Profiles or users who have membership to a particular role. Users inherit most of their permissions from the roles assigned to the User Profile. However, you assign some Permission Lists directly to the User Profile.

Data permissions are assigned directly to the User Profile either through a Primary Permissions list or Row Security Permissions list (this will vary in HR or Finance). Navigator Homepage and Process Profile permission lists are also assigned directly to the user profile.

Some users obtain their membership by an administrator adding a role to their user profile manually through the Security pages devoted to users. These users are **Static Role Users.**

Workflow Roles

There are delivered business processes that when enabled will provide for the routing of work through an automated process called workflow. Each business process needs to be configured to include a rule set to route the work to the appropriate users. In some cases, this is a role assigned to the user profile. Roles used in this manner will be designed and created to allow for the routing of work and only provide this function. They will be separate from the standard navigation roles.

> ### Activity 1:
>
> Login to FPLAY with your user id and password that you use in current production.
>
> Create a new user id and assign it the following roles: BOR PeopleSoft User, BOR_FN_ADMIN_REPORTING, ReportSuperUser, BOR_EP_REQUESTER, BOR_EP_MAINT_REQ, BOR_EP_MAINT_REQ_SCI, BOR_PT_QRY_PUBLIC,and BOR_PT_QRY_ALLACCGRPS.
>
> Save the user profile and write down the user name/password you created.

Permission Lists

Permission Lists are the building blocks of your end user security authorizations. A Permission List may contain any number of the following permissions, including sign-on times, page permissions, component interface permissions, web libraries, and so on. A Permission List may contain one or more permissions and the smaller the number of permissions within a particular Permission List the more flexible and scaleable that Permission List is.

Recall that roles are intermediary objects that exist between permission lists and users. Roles enable you to assign permissions to users dynamically.

In the following example notice that the permission lists are assigned to roles, which are then assigned to user profiles. A role may contain numerous permissions and a user profile may have numerous roles assigned to it. Because permission lists are applied to users through roles, a user inherits all the permissions assigned to each role to which the user belongs. The user's access is determined by the combination of all of the roles.
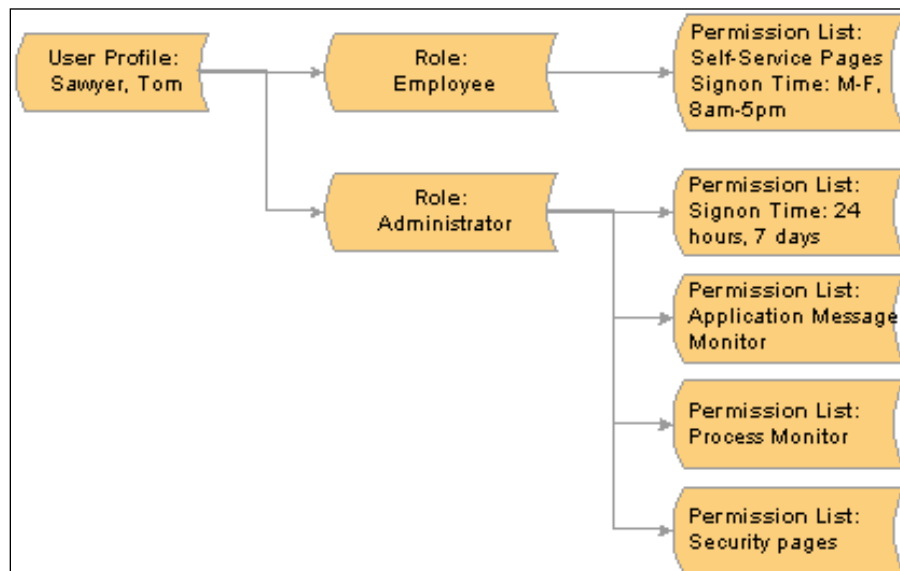
All permission lists will begin with XX__ to designate this as a custom BOR security object and showing the module (GL=General Ledger). Tools version 8.4+ allows you the naming length of 30 characters for a permission list.

There are two tables that will contain the information about this permission list, they are:

PSCLASSDEFN - Permissions Lists Definition

PSAUTHITEM - Authorized Menu Item

It is recommended that all navigation permission lists (access to pages/components) are specific to just navigation.

Other permissions should be enabled separately and include:

General | Pages | PeopleTools | Process | Sign-on Times | Component Interfaces | Web Libraries | Web Services |

They would include: application designer, process security/operations, sign-on times, component interfaces, WEB libraries, and WEB services.

Personalizations | Query | Mass Change | Links | Audit | Permission List Queries

They would include: Personalization, query security/operations, Mass change templates, links, audit stamp and delivered security queries.

Glossary

Menu: Menus are delivered with the system to group business processes into logical navigation paths. Each menu contains components/pages that allow tasks to be performed within this business process. This could include reports, processes, inquiry, maintenance and setup actions.

Component: A logical grouping of pages. A component associates pages to specific menus in the system. A component or page can be assigned to multiple menus throughout the system. This allows for multiple navigation points to the same component. To grant access to a particular page, determine the component it is in and the menu name the component falls under. This enables you to drill down to the appropriate page. If a page is authorized in a component, the component inherits this authorization and is also enabled along with the associated menu.

WEB Services: The web services offered by the PeopleSoft Integration Broker can be secured at the user ID level through the use of the web services permissions you specify. This applies to external web service requests only, not internal web service requests.

WEB Libraries: A web library is a derived/work record whose name starts with WEBLIB_. All PeopleSoft iScripts are embedded in records of this type. An iScript is a specialized PeopleCode function that generates dynamic web content. All WEB libraries will be included in the base user permission list.

Managing Query Security

Setting up Query Security

This section discusses how to:

- Establish a security scheme for PeopleSoft Query.

- Build Query Access trees to organize your record components into logical groups for security access.

- Set up your record definitions so that Query enforces row-level security.

> **Note.** You perform these setup tasks using the Query Access Manager, Application Designer, and permission lists. After you define Query Access Group trees, you provide user access using the Query tab in Permission Lists.

PeopleTools Used to Setup Query Security

Page Name	Navigation	Usage
Query Access Manager	PeopleTools, Security, Query Security, Query Access Manager.	Create and update Query Trees.
PeopleTools Security	PeopleTools, Security, Roles and Permission Lists, Permission Lists, Query.	Add Query Profiles to permission lists. Attach Query Access Groups to permission lists.
Application Designer	Go, Application Designer.	Create Query Security record definitions.

Defining Query Profiles

Query takes advantage of a user's security settings, row-level security, and primary permission list. Query is a PeopleTool that helps you build SQL statements to retrieve information from your application tables. The Query Profile defines what features of Query operations the user has.

Query Operations

Level I: Query Viewer-User has the ability to view all public queries for records that the user has access to through Access Group security.

Level II: Query Manager-User has the ability to create and run Private queries-run Public queries. The user will only be able to create and run those queries on records that they have access to through Access Group security.

Level III: Query Manager-User has the ability to only run Public queries. The user will only be able to run those Public queries on records that they have access to through Access Group security.

Level IV: Query Manager-User has the ability to create and run both Private and Public queries. The user will only be able to create and run those queries on records that they have access to through Access Group security.

Level V: Query Manager/Monitor- User has the ability to create and run both Private and Public queries. The user will only be able to create and run those queries on records that they have access to through Access Group security. Query monitor allows a user to gather statistics on Query use.
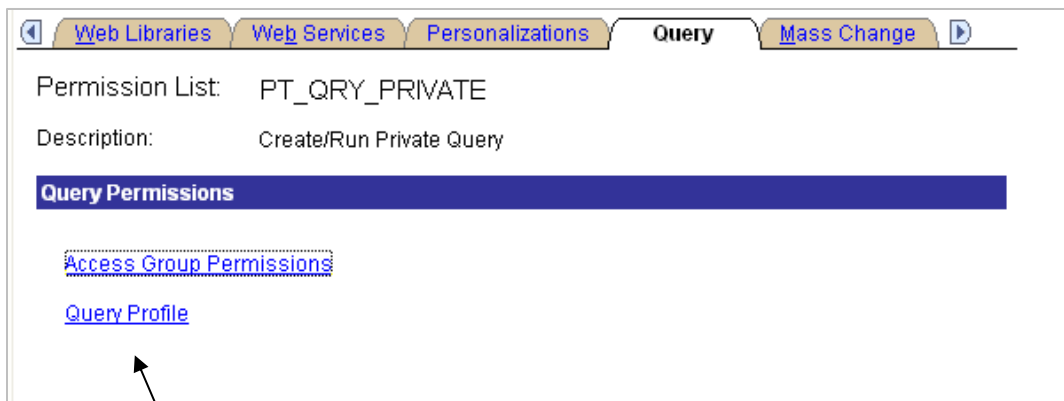
PeopleTools>Security>Permissions and Roles>Permission Lists>Query tab

Click on the Query Profile Link
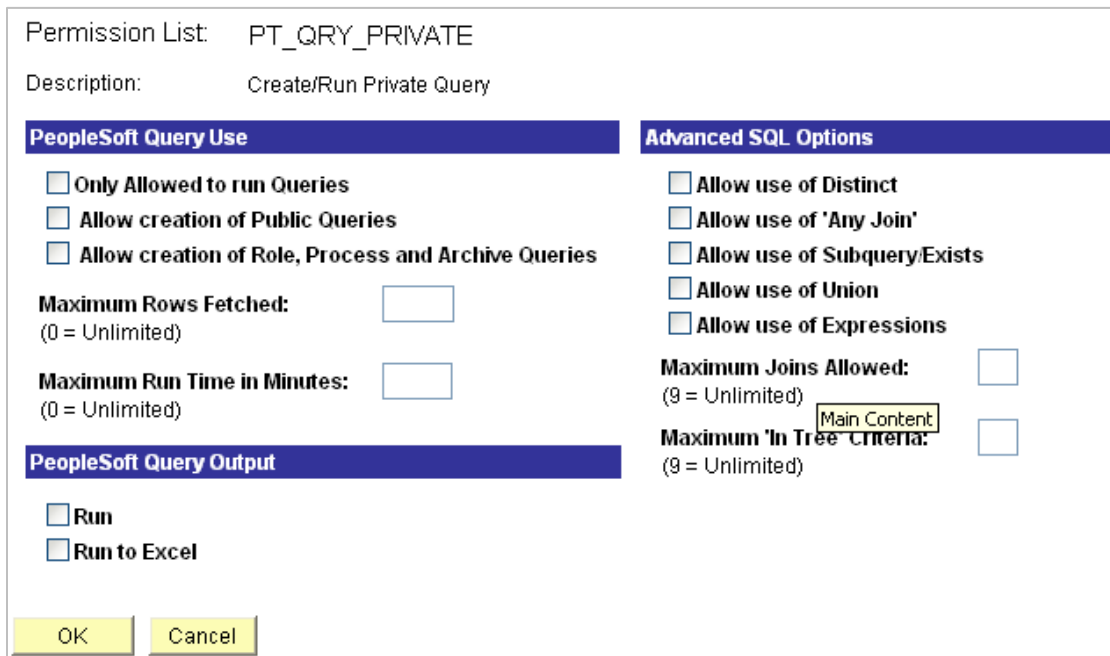
Query Access Groups

For each Query user, you can specify the records they are allowed to access when building and running queries. You do this by creating Query Access Groups in the Query Access Group Manager, and then you assign users to those groups with Query permissions. Keep in mind that Query permissions are enforced only when using Query;

it doesn't control run-time *page* access to table data. In the example below, if you give the User access to the AP_Access_Group, they will be able to query all records stored in the tree Query_Tree_AP. The User must have access through Access Group permissions for all records needed to create or run a query.

PeopleTools>Security>Permissions and Roles>Permission Lists>Query tab

Click on the Access Group Permissions Link

Click the lookup button under the Tree Name and a listing of trees will be displayed to choose from. After you have selected your Tree, click on the lookup button for the Access Group. In this lookup screen, all the nodes from the tree will be listed. If you want to give access to all the records in the tree, select the Access Group for that tree. For all the delivered trees, this will be the highest node on the tree.

EXAMPLE: Query_Tree_AP   AP_Access_Group
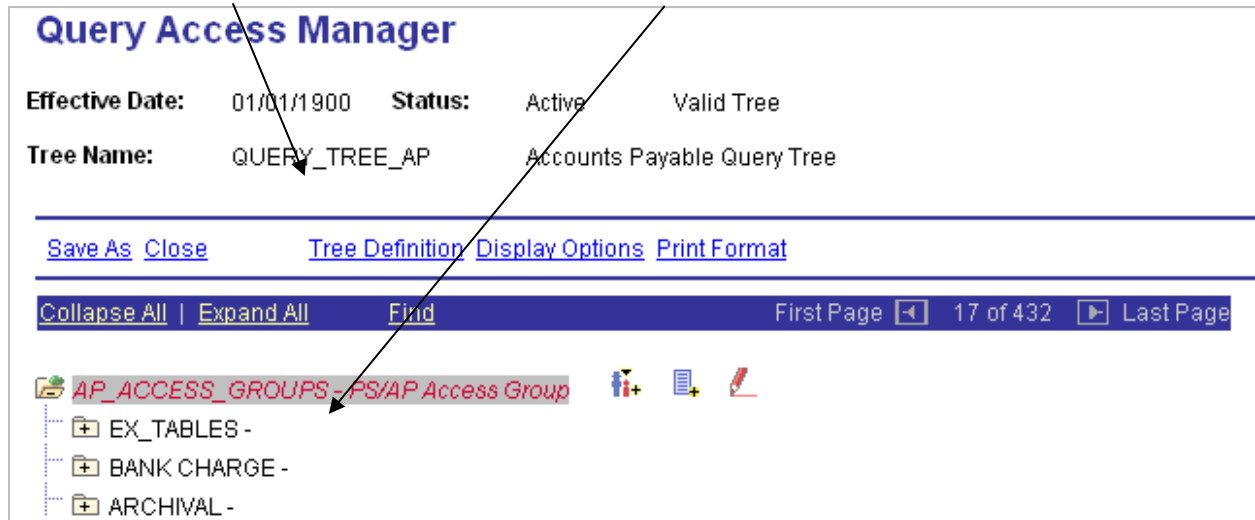
PeopleTools>Security>Query Security>Query Access Manager

Navigation to Query Manager Components

To perform query operations, the user will need access to navigate to the query manager components. These components are accessed through the Reporting Tools folder in the portal navigation.
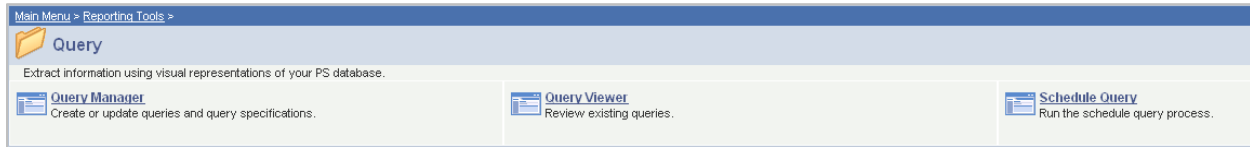
Query components will be enabled for the user to match the level of query operations they are authorized through the query profile permissions.

Query Trees

Building Query Access Group Trees

Trees are a graphical way of presenting hierarchical information. PeopleSoft Query uses *query access group trees* to control the access to the records in your PeopleSoft database. You define a hierarchy of PeopleSoft record definitions, based on logical or functional groupings, and then give users access to one or more nodes of the tree. Users can only retrieve information from those tables whose record definitions are included in their query access group security permission list(s).

You create and update query access group trees using Query Access Manager. PeopleSoft has included some sample query access group trees with your applications. Which trees you have depends on which PeopleSoft applications you've installed. Each tree contains access groups and record definitions categorized by business function (module).

Access groups mark and define a functional group of records or other access groups—in other words, they are descriptive placeholders used to categorize actual record definitions in a logical, hierarchical format. When you define users' security rights to a tree, you specify which access groups they are permitted to query.

This section explains how to create query access group trees. It assumes that you're familiar with the concept and terminology of PeopleSoft trees.

**ITS is responsible for creating the query trees.

Query Access Group Tree Considerations

You should create your own query access group trees based on your organization's needs and on any customizations you've made.

NOTE: Remember that the sample trees provided may be replaced when you upgrade to a subsequent PeopleSoft release, so if you modify the samples rather than create your own trees, you may lose your customizations.

Every record definition that you want users to be able to query must be in a query tree. However, they don't all have to be in the same query tree. One strategy is to use the sample query trees to provide access to the standard PeopleSoft record definitions, but create separate query trees for record definitions that you add in the course of customizing the system. This way, you take advantage of the sample trees but avoid overwriting your changes during future upgrades.

How you organize the contents of your query tree depends on the needs of your organization and your users. For example, you might want to create small trees that are not intimidating to non-technical or casual users. The sample query trees provided in your PeopleSoft application are divided by business functions, but to simplify the trees, you may want to create separate trees that contain subcategories of each function. For example, you could create separate trees for U.S., Canadian, and international record components in order to grant users in each region security access to only those record components they should use.

> **Note.** You should consider adding record definitions to your query trees in a hierarchy that matches the parent/child relationship of records in your database. Though you don't have to organize records this way—Application Designer actually controls the parent/child hierarchy in your database—you'll probably find it helpful to keep your query trees consistent with your database structure.

Working with Query Trees

The following sections cover topics related to opening, viewing, and modifying Query trees.

Understanding Query Access Group Trees

If you have worked with Tree Manager and/or trees before, you should take a moment to review the following information describing the differences between typical trees and the Query access group trees.

Nodes

- Query access group trees contain two types of Nodes: groups and records.

- Groups are a logical representation of a set of child groups or records. It is similar to folder in Windows.

- Records represent a PeopleSoft record definition.

Structure

- Always use the ACCESS_GROUP Tree Structure.

- Do not use SetID or Business Unit.

- Do not have Details.

- Do not use Levels.

- No Branches.

Requirements

- The Root Node is always a group.

- Groups must be unique in a given Tree while records definitions can be repeated.

- Groups and records could have Child Groups and Child Records.

- Each record needs a unique fully qualified path in the tree. You can't add the same record under the same parent node (group or record).

Opening Query Access Group Trees

Before you can view and modify a query access group tree definition, you need to locate the correct tree definition.

To open a Query tree definition:

1. Select **PeopleTools, Security, Query Access Manager.**

2. On the Basic Search page select your search criteria.

   You can search by Tree Name, Tree Category, or Tree Description.

3. Click **Search.**

   After clicking Search, a list appears containing the definitions that meet your criteria.

4. Double-click on the appropriate definition.

   The list of trees in the lower part of the page also serves as a maintenance utility enabling you to Delete or Copy a tree. If you click **Delete**, the system prompts you to confirm the action, and if you click **Copy,** the system displays the Copy Tree page where you can select a name for the copied tree.

   Some of the trees in the grid may appear without Copy/Delete buttons visible. This occurs when Object Security settings are such that you only have read-only access to these trees.

Defining Your Query Tree

Before you can insert nodes for access groups and record components, you must first define a number of important characteristics for your tree.

Access the Tree Definition and Properties page by selecting Create New Tree on the Basic Search Page.

Tree Definition and Properties page

Tree Name	For the tree name, we recommend that you start the name with QRY_ so that you can easily identify the tree as a custom query tree. The standard query trees we deliver with the system start with QUERY_.
Structure ID	The Structure ID is read only and always reads ACCESS_GROUPS for Query access trees.
Description	This description will appear along with the name and effective date in the list box whenever you select from a list of trees.
Effective Date	The status default is set to Active. Query trees are available immediately if the effective date is active; you don't need to run an SQR utility like you do for organizational security trees.
Category	If necessary add a category, which are groupings of the definitions.
Item Counts	Item Counts shows the number of nodes within the access group.

Once you've completed the tree definition, click OK. On the Enter Root Node for Tree page, select an existing Access Group using the Lookup Access Group control, or create a new one.

Viewing and Modifying Definitions

This section describes the controls you use to modify Query Access Group Trees after you have opened one from the search page.

Query Access Manager

Effective Date:	01/01/1900	**Status:** Active Valid Tree
Tree Name:	QUERY_TREE_AP	Accounts Payable Query Tree

Save As Close   Tree Definition Display Options Print Format

Collapse All | Expand All   Find   First Page ◄ 17 of 432 ► Last Page

📂 *AP_ACCESS_GROUPS - PS/AP Access Group*
⊞ EX_TABLES -
⊞ BANK CHARGE -
⊞ ARCHIVAL -

PeopleTools, Security, Query Security, Query Access Manager

Tree Name	Shows the name of the current tree.
Effective Date	Shows the current effective date.
Status	Shows either Active or Inactive.
Save, Save As,	These are the two save options. Each option appears only if it relates to your current activity. Save enables you to save your changes to the database. Save As enables you to clone tree definitions at save time.
Tree Definition	Shows the Tree Definition and Properties page that you modified when you created the definition.
Display Options	Shows the Configure User Options page where you can adjust the presentation of the trees. For example, you can choose whether the Node ID appears and how many lines of the definition appear at a time. Most of these don't apply for Query Access Trees so they're disabled.
Print Format	Shows what your tree definition will look like when you print it. Essentially, this is a print preview.
Close	Closes the definition and returns you to the search page.
Bread Crumbs	Once you have drilled down into a definition, a bread crumb display appears just above the Collapse/Expand All controls. This is to provide orientation, especially within large trees.
Collapse All	Collapses all nodes of the tree into their parent groups so that you only see the root node and the first layer of child groups.
Expand All	Expands all nodes of the tree so that each child object is visible.
Find	If you are looking for a specific access group or a record you can use the Find Value page rather than drilling down into your tree. You specify an access group or a record and/or it's description. You can select a case sensitive search and specify that an exact match must be found.

You can use pattern search option by deselecting the Exact Matching checkbox. This performs platform independent search for the Record/Group starting from the specified pattern.

If you want to perform pattern search not starting from the beginning of Record/Group name, specify a platform dependent wildcard character at the |

beginning of the pattern.

For example, to find all occurrences of 'TBL' in the Records, you specify *%TBL* as a search condition (for Microsoft SQL Server database).

If you specify both Group and Record search conditions are specified the search is performed on Group condition. If both Group/Record ID (name) and Description conditions are specified the search is performed on ID/name condition.

NOTE: Always make sure that any modifications to the tree are saved prior to using the Find feature.

Collapse Node	When a node folder is open, you click on it to collapse the node.
Expand Node	When a node folder is closed, you click on it to expand the node.
Node/Record Controls	When you have a node or record selected, the actions you perform are controlled by the icons that appear to the right of the definition. The descriptions of the actions are below. You can roll the mouse over the icon to reveal a label.
Insert Sibling Group	Inserts an access group node at the same level as the currently selected node.
Insert Child Group	Inserts an access group node at the next level lower than the currently selected node.
Insert Child Record	Inserts a record definition within an access group node.
Edit Data	For access groups you can edit the Description and the Definition (long description) on the Access Group Table. Records are not editable. You can't rename a group.
Delete	You can delete both access groups and records. You can't delete the root node.
Cut/Paste as Child	You can cut and paste access groups and records to move them within the tree. Once a cut has been executed, then the Paste as Child icon becomes enabled. You can't cut the root node. **Note.** After you perform the "cut" function, only navigation and search features are available until you execute the "paste" function. This protects the node in the clipboard.

Row Level Security

Row-Level Security and Query Security Record Definitions

By default, when you give Query users access to a record definition, they have access to all the rows of data in the table built using the associated record definition. In some cases, though, you want to restrict users from seeing some of those data rows. For example, you might not want your human resources staff to have access to compensation data for vice presidents or above. In other words, you want to enforce *row-level security*, which is offered by many PeopleSoft applications.

Row-Level Security

With row-level security, users can have access to a table without having access to all rows on that table. This type of security is typically applied to tables that hold sensitive data. For example, you might want users to be able to review personal data for employees in their own department, but not for people in other departments. You would give everyone access to the PERSONAL_DATA table, but would enforce row-level security so that they could only see rows where the DEPTID matches their own.

PeopleSoft applications implement row-level security by using a SQL view that joins the data table with an authorization table. When a user searches for data in the data table, the system performs a related record join between the view and the base table rather than searching the table directly. The view adds a security check to the search, based on the criteria you've set up for row-level security. For example, to restrict users to seeing data from their own department, the view would select from the underlying table just those rows where the DEPTID matches the user's DEPTID rows.
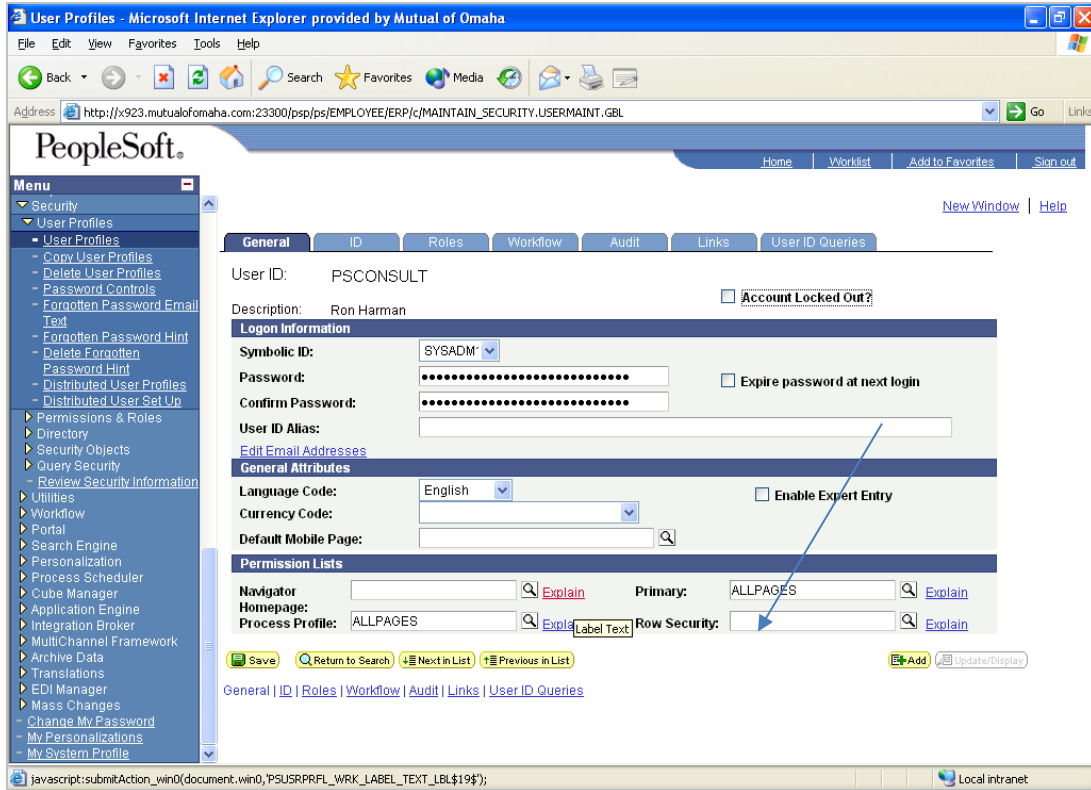
Query Security Record Definitions

You implement row-level security by having Query search for data using a query security record definition. The query security record definition adds a security check to the search.

Query security record definitions serve the same purpose as search record definitions do for pages. Just as a page's search record definition determines what data the user can display in the page, the query security record definition determines what data the user can display with Query.

To get Query to retrieve data by joining a security record definition to the base table, you specify the appropriate Query Security Record when you create the base table's record definition.

To apply row level security:

1. Select **PeopleTools, Application Designer** to open the Application Designer, and open the record on which you want to apply row-level security.

2. With the record definition open in the Application Designer, click the **Properties** button, and select the **Use** tab from the **Record Properties** dialog box.

   Note. You use this dialog box to set a number of different aspects of the record definition. The only item related to Query security is **Query Security Record** list box.

3. Select the security record definition (usually a view) in the **Query Security Record** list box.

31

Each PeopleSoft product line comes with a set of views for implementing its standard row-level security options. See the product documentation for details.

> **Note.** The **Parent Record** list box is also relevant to Query. It identifies a record definition that is the current definition's *parent*, meaning that it holds related data and that its keys are a subset of the current record definition's keys. If you designate a parent record, Query automatically knows what fields to use when you join these two tables for a query.

In most cases, the Query Security Record definition you'll want to select is the same one you use as the search record definition for the page that manages this table. If you're enforcing one of the standard row-level security options from a PeopleSoft application, select the PeopleSoft-supplied security view for that option. See the application documentation for a list of the available views. If you've designed your own security scheme, select a record definition that appropriately restricts the rows a query will return.

4. Once you've set the query security record definition, click **OK** to close the Record Properties dialog box, then save the record definition.

If you've already used SQL Create to build a table from this record definition, you don't need to rebuild it.

> **Note.** PeopleSoft row-level security views restrict users from seeing certain rows of data. To secure data through the search record, simply put one of the three Row Level Security fields on your record as a Key, not a List Box Item. The three Row Level Security fields are OPRID (User ID), OPRCLASS (Primary Permission List), and ROWSECCLASS (Row Security Permission List). If one of these fields is on the search record as a Key, not a List Box Item, PeopleTools does the following. PeopleTools adds a WHERE clause when it performing a SELECT through the record forcing the value to be equal to the current user's value.

Using Query Viewer

Query Viewer is a read-only version of Query Manager. It allows security administrators an easy way to limit some users to read-only access for all queries. The Security Administrator can easily provide read-only access to users who should only view or print queries.

Query Viewer enables you to:

- Search for a query:

  To preview a query, click the name of the required query.

- Preview a query (which displays results in current browser window):

  From the Preview page, view results of your query, rerun the query, and download the results to Excel.

- Run a query (which displays results in a new browser window):

  Once you run your query, you can download the results to an Excel spreadsheet or a CSV Text file.

- Print a query:

  - To print query results, you must first run the query and display the results in your browser.

    Click the Print button from your browser, or select File, Print from you browser menu. The query prints on your default printer.

  - If you choose to download the query in Excel or another tool, you can print the query using their print functions.

- Schedule a query:

  - From the Search results page, click the Schedule link associated with the required query.

  - Query Viewer interacts with PeopleSoft Process Scheduler to give users the ability to schedule queries.

    You can submit requests to schedule a query, check the status of your request using Process Monitor, and view your output using Report Manager.

Query Administration

This section provides an overview of Query Administration and discusses how to use Query Administration.

Understanding Query Administration

System administrators can use Query Administration to monitor query performance and usage. Some of the conditions that you can monitor include average runtime, number of times run, and the dates last run. Using a predefined search, you can also select queries to review and report on.

> **Note.** Workflow queries are excluded from the statistics because of the large volume that can be run as part of workflow processing. Therefore, you should take care that workflow queries are as efficient as possible.

Query Administration also enables you to cancel queries that are currently running in Query Manager and Query Viewer as well as enable and disable queries and logging.

> **Note.** You cannot cancel currently running scheduled queries.

Using Query Administration

This section discusses how to:
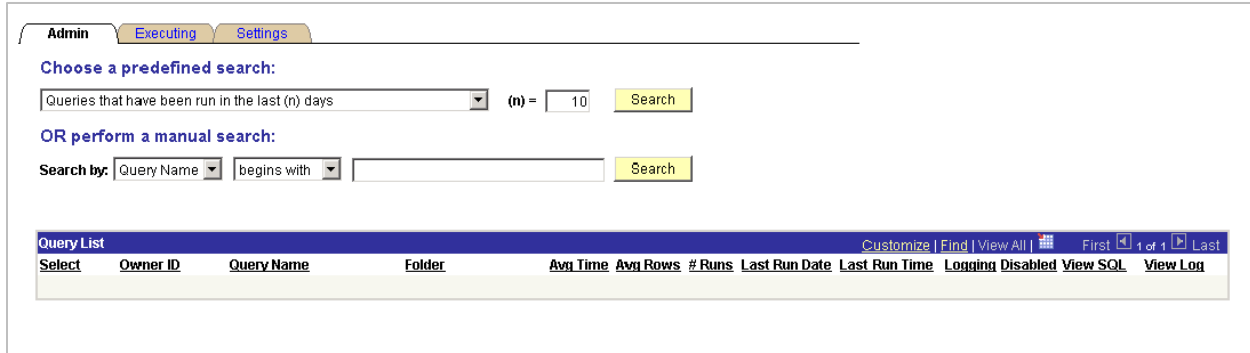
- Administer queries.

- Cancel currently running queries.

- Set additional options.

Pages Used for Query Administration

Page Name	Object Name	Navigation	Usage
Admin (Administration)	QRY_ADMIN	PeopleTools, Utilities, Administration, Query Administration, Admin	Administer queries.
Executing	QRY_KILL	PeopleTools, Utilities, Administration, Query Administration, Executing	Cancel currently running queries, and enable or disable queries and logging.
Settings	QRY_SETTINGS	PeopleTools, Utilities, Administration, Query Administration, Settings	Set additional options such as enabling the query timeout feature and running query statistics.

Administering Queries

Access the Admin page.

Admin page

To administer queries:

1. Use either the predefined search or manual search option to restrict the list of queries that are displayed.

   For a predefined search, enter the desired value for the selected search option in the (n)= field and select one of the following options:

   - *Queries that belong to locked out accounts.*

   - *Queries that have been disabled.*

   - *Queries that have been run in the last (n) days.*

   - *Queries that have logging turned on.*

   - *Queries that have never been run.*

   - *Queries that have run but not in the last (n) days.*

   - *Top (n) queries by largest average number of rows.*

   - *Top (n) queries by longest run time.*

   - *Top (n) queries most frequently run.*

      For a manual search, select to search queries by query name or owner ID.

      You can define your search further by selecting either *begins with* or *contains* search type.

2. Click the Search button to display a list of queries that match your search criteria.

   The Query List group box lists those queries that match your search criteria.

3. Review the following statistics for each query that is listed:

   - Owner ID.

   - Query name.

   - Folder.

   - Average time to run.

   - Average number of rows.

   - Number of times run.

   - Last run date and time.

- Logging status.

- Disabled status.
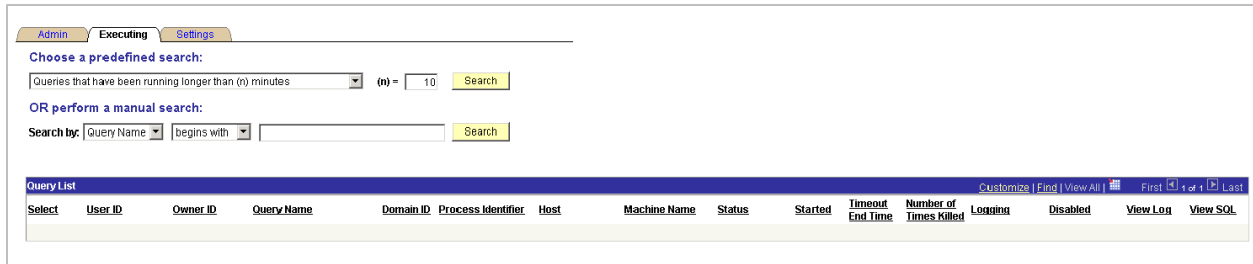
> **Note.** If a query appears in the list as *<UNTITLED>,* a user has created and run one or more queries without saving them. Results from all unsaved queries appear as a single untitled row. You can clear statistics only for untitled queries. Attempting to perform any other action on untitled queries will result in an error message.

4. For the appropriate query, click the View Log link to view the log for that query.

   A message appears if no logs are available.

5. For the appropriate query, click the View SQL link to view the SQL for that query.

6. Select the check box for each query on which you want to perform an action.

   You can also click Check All to select all queries, or click Uncheck All to clear all queries.

7. Perform an action by clicking one of the following buttons:

   - Logging On: Enables logging for the selected query.

     When you enable the logging feature, detailed statistics will be logged on the query after every time it has run to completion. The statistics are stored in a separate Query Log table.

     > **Note.** The statistics log is updated with data only if the query runs to completion.

   - Logging Off: Disables logging for the selected query.

   - Enable: Enable the selected query to be run, previewed, or scheduled.

   - Disable: Disables the selected query from being run, previewed, or scheduled.

   - Assigns New Owner: Assign a new owner to the selected query.

   - Delete: Deletes the selected query.

   - Rename: Renames the selected query.

   - Move to Folder: Moves the selected query to a folder.

   - Clears Stats/Logs: Delete the statistics and logs for the selected query.

8. For the appropriate query, click the Logging button to enable logging for that query.

> **Note.** Your changes are saved automatically. No Save button is available.

Canceling Currently Running Queries

Access the Executing page.

Executing page

The Executing page displays all of the currently running queries, allowing you to enable or disable queries, enable or disable logging, and cancel currently running queries. If an administrator needs to verify that a query has been canceled, he or she can look in the Appsrv.log and verify that the *PSMONITORSRV* service has canceled the selected query.

To cancel currently running queries:

1. Use either the predefined search or manual search option to restrict the list of queries that are displayed.

   For a predefined search, select one of the following options:

   - *Queries that have been running longer than (n) minutes.*

   - *Top (n) queries by longest run time.*

2. In the (n)= field, enter the value that you want for the search option.

   For a manual search, select to search queries by query name or owner ID.

   You can define your search further by selecting either the *begins with* or *contains* search type.

3. Click the Search button to display a list of queries that match your search criteria.

   The Query List group box lists those queries that match your search criteria.

4. Review the following statistics for each query that is listed:

   - User ID.

   - Owner ID.

   - Query name.

   - Domain ID.

   - Process identifier.

   - Host.

   - Machine name.

   - Status.

   - Time started.

   - Timeout end time.

   - Number of times killed.

   - Logging status.

   - Disabled status.

5. For the appropriate query, click the View Log link to view the log for that query.

   A message appears if no logs are available.

6. For the appropriate query, click the View SQL link to view the SQL for that query.

7. Select the check box for each query on which you want to perform an action.

   You can also click Check All to select all queries, or click Uncheck All to clear all queries.

8. Perform an action by clicking one of the following buttons:

   - Kill Selected Processes: Forces the selected query to stop running.

   - Logging On: Enables logging for the selected query.

     When you enable logging, detailed statistics are logged on the query after every time it has run to completion. The statistics are stored in a separate Query Log table.

   - Logging Off: Disables logging for the selected query.

   - Enable: Enables the selected query to be run, previewed, or scheduled.

   - Disable: Disables the selected query from being run, previewed, or scheduled.

9. For the appropriate query, select the Logging check box to enable logging for that query.

Note. Your changes are saved automatically. No Save button is available.

The kill (cancel) query/timeout mechanism represents each query that is run from Query Manager or Query Viewer as a row in the table PSQRYTRANS. Query Monitor, which implements the kill query/timeout functionality, has a mechanism that looks for orphan rows in PSQRYTRANS. Orphan rows are rows in PSQRYTRANS that do not have a query actively running. Orphan rows can be created because the server crashed while running a query, or other reasons.

Query Monitor looks for orphan rows only for the application server domain that it is running in. For this reason, orphan rows could be in PSQRYTRANS when no active domain exists. These rows are not seen by the online query monitoring facility, but could potentially exist in the database. Such rows are rare, and you can use the database query tool to clean them up. You can use the *machine* and *domain* fields to determine whether rows exist that should be cleaned up.

Setting Additional Options

Access the Settings page.
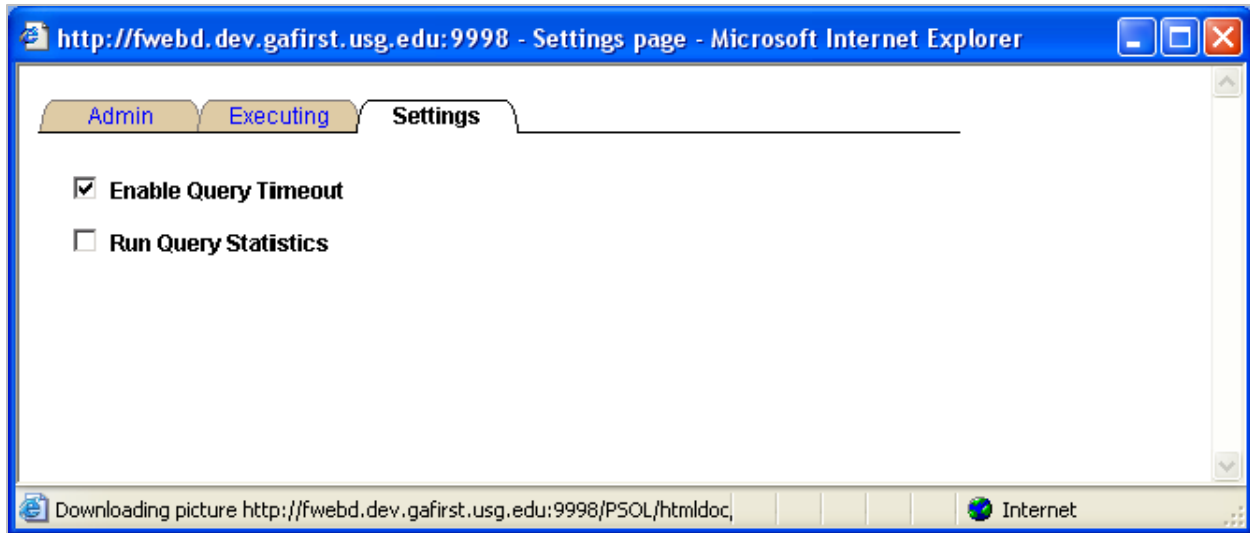
Settings page

Enable Query Timeout	Select or clear this check box to enable or disable the query timeout feature on a system-wide basis. The timeout values are stored in each permission list.
	Note. The query timeout feature applies to queries that are run in Query Manager and Query Viewer. This feature does not apply to scheduled queries.
Run Query Statistics	Select or clear this check box to enable or disable the query statistics feature on a system-wide basis.
	Note. By default, the query statistics feature is *disabled.* PeopleSoft recommends that you use the query statistics feature only for analysis, and that you not leave it enabled on an ongoing basis. Enabling this feature may compromise the performance and the system may have an increased possibility of query timeouts or may return query results with zero values. This recommendation also applies to users of queries in reports.

Query Types

User query	User queries retrieve data from the database directly from Windows-based Query Designer or the web-based Query Manager/Query Viewer applications.
	Note. Because of the range of possible circumstances in which you might run an ad hoc query, there are no special considerations or requirements that apply to all of them.
Reporting query	Reporting queries are essentially the same as user queries, except that they are designed to be used by another reporting tool. Reporting queries can be used as data sources for ad hoc queries, scheduled queries, Crystal Reports, PS/nVision, Cube Manager, or XML Publisher. When you define a custom report, you often include runtime variables that users specify when they run the report. For example, you might want users to be able to say which business unit, location, or time period to report on. Therefore, your reporting query may include one or more runtime prompt variables.

If your query requires input parameters, you must decide how users should enter them. If they run the report from any of the PeopleSoft Query applications, they can enter values into the page that appears in Query Manager, Query Viewer, or Scheduled Query.

When reporting queries are used as a data source to another third party reporting product, you may need to:

- Create or modify a page to collect the necessary input parameters.
- Create or modify a record definition, based on the input parameters.
- Add a process definition to PeopleSoft Process Scheduler.

Process query	Process queries are queries that you intend to run periodically using a batch process. Create these automated batch processes using PeopleSoft Application Engine and the Query API. For example, you could write a query that returns any overdue receivables and schedule a batch process to run the query once a week.
	Note. Process and role queries override the automatic row-level query security logic that is applied to all other types of queries. For this reason, you should restrict access to creating these types of queries to administrative roles and not include any sensitive data columns in the select list for these types of queries. You can restrict access to creating/modifying these queries based on Query Profile settings assigned to a Permission List. Also note that Workflow queries also override the row-level security logic.
Role query	PeopleSoft Workflow uses role queries to determine to whom to send an email, form or worklist entry. A role query needs to return one or more role IDs based on the data that has been saved on the page that is triggering the routing.
	Because a role query returns a list of role users, the record definition that you want is either PSROLEUSER (which lists role users and the roles to which they are assigned) or ROLEXLATOPR (which lists role users and their IDs).
	The only field that you will select in your query is ROLEUSER. Of course, you will use other fields and join to other record definitions to specify the criteria that role users can select. But no matter how complex the query is—how many joins or selection criteria it has—it must return ROLEUSER and nothing more.
	Define a role as a query because you want to route items differently based on the context of the transaction that the users are performing. Thus, every role query contains at least one bind variable whose value gets set at run time. The bind variable or variables correspond to the data on which you want to base the routing decision. At run time, the system sets the values of the bind variables based on data from the page that triggers the event.
	Save your role queries with names that begin with [ROLE] so that you can identify them as role queries.
	Note. Process and role queries override the automatic row-level query security logic that is applied to all other types of queries. For this reason,

Archive query	You can save a query as an archive query if you have access to workflow queries that include *Archive Query, Role Query,*and *Process Query.* These queries are generally only used by the PeopleSoft Data Archive Manager.

Note. You can only create and save archive queries as *public*.

PS/nVision query	Use PeopleSoft Query to create a query in order to specify the data source for a PS/nVision report layout. However, if you want to use your query in a PS/nVision matrix layout, you must apply aggregate functions to at least one column.
	Queries used with PS/nVision tabular layouts do not have the same restrictions as matrix layout queries; they are like other reporting queries and do not require an aggregate column.

Activity 2:

Login to FPLAY with your user id and password that you created in Activity 1.

Navigate to the Query Manager, located under Reporting Tools. Pull up query BOR_EX_DUE and run it. Did you get results?
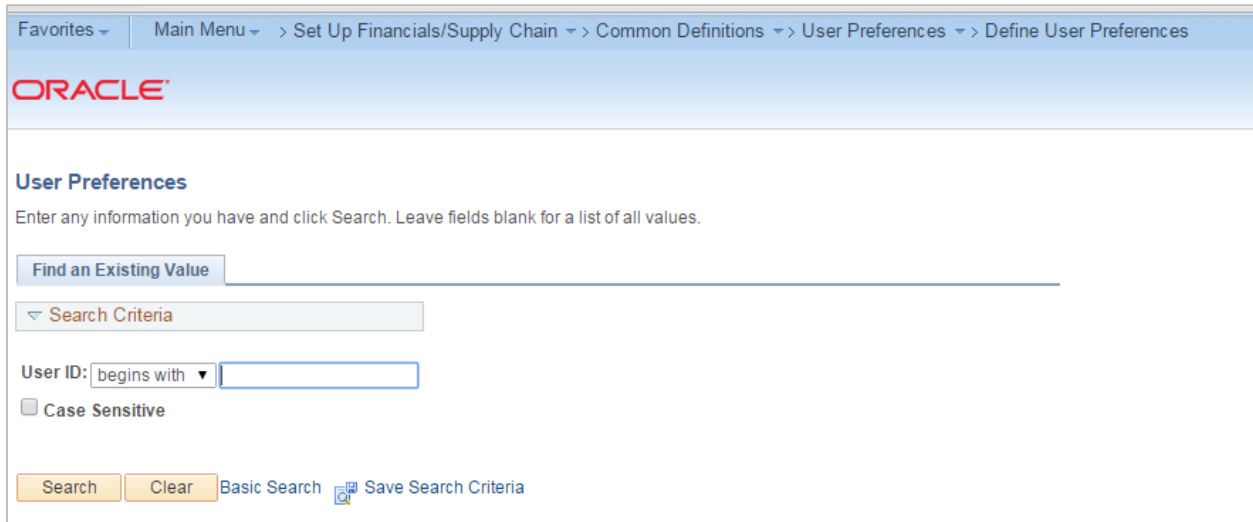
Now pull up query BOR_ADP_CES_DTL. Did you get results?

Managing User Preferences

User Preferences

Each functionality in PeopleSoft Financials System relies on every user having access (and not having access) to carry out certain actions in order for the system to function correctly and avoid costly errors. Business Unit security administrators and designates are responsible for setting up user preferences

Navigation: *Setup Financials/Supply Chain > Common Definitions > User Preferences > Define User Preferences*

- Enter the **User ID**
- Click the **Search** Button.

General Preferences

Overall Preference

ORACLE

User Preferences

General Preference	Product Preference	
Overall Preference	Asset Management	Planning
OLE Information	IT Asset Management	Procurement
Process Group	Billing	Project Costing
	Contracts	Promotions Management
	General Ledger	Receivables Data Entry 1
	Inventory	Receivables Data Entry 2
	Lease Administration	Staffing - General Preferences
	Maintenance Management	Staffing - Job Data
	Manufacturing	Strategic Sourcing
	Mobile Inventory	Supplier Contract Management
	Orders - Quotations	
	Orders - Other	
	Orders - Sales	
	Paycycle	

🖫 Save 📇 Return to Search 📧 Notify 🔄 Refresh

- The **User ID** and **Name** fields default.
- Enter the default **Business Unit**
- Enter the default **SetID** field.
- **As of Date** Displays the default as of date for the Combo Edit process.
- Enter "**USA**" in the **Localization Country** field**.**
- Do not Select **Alternate Character Enabled** to activate alternate description buttons or links, which appear to the right of fields on many of the application pages. Click a button or link to enter or display alternate characters on the auxiliary page that appears.
- **Display Debit/Credit Amounts in Subsystem** displays debit and credit amounts of the default business unit on journal entry and inquiry pages. A subsystem is any PeopleSoft application, such as Payables or Receivables that contributes entries to PeopleSoft General Ledger. Leave unchecked.
- Select the **Save** button.

OLE Information

No setup is required

Process Group

This is set up by Security

This controls the On demand features on transaction pages. For instance, a user that enters a voucher, may want to budget check and post for the voucher entry page. This is controlled and enabled through process groups. The allow Processing checkbox must be selected. You can copy these source transactions for another user.

ORACLE

User Preferences	**Process Group**

User ID OIITSLOAN   Shelia Sloan

Copy From User ID [   ] 🔍   [Copy]

☑ Allow Processing   ☐ Use Event Notification

Source Transaction   Find   First ◀ 1-10 of 10 ▶ Last

*Source Transaction [ARITSPLT] 🔍   Item Split   ⊞ ⊟

Process Group   Personalize | 🔲   First ◀ 1-3 of 3 ▶ Last

Process Group	Description		
ARACTIONA 🔍	Do Not Post	⊞	⊟
ARACTIONL 🔍	Batch Standard	⊞	⊟
ARPOST 🔍	Post Now	⊞	⊟

*Source Transaction [ARMNTWS] 🔍   Maintain Receivables   ⊞ ⊟

Process Group   Personalize | 🔲   First ◀ 1-4 of 4 ▶ Last

Process Group	Description		
ARACTIONA 🔍	Do Not Post	⊞	⊟
ARACTIONL 🔍	Batch Standard	⊞	⊟
ARACTIONN 🔍	Batch Priority	⊞	⊟
ARPOST 🔍	Post Now	⊞	⊟

*Source Transaction [AROPIE] 🔍   Online Pending Item Entry   ⊞ ⊟

Process Group   Personalize | 🔲   First ◀ 1-4 of 4 ▶ Last

Process Group	Description		
ARACTIONA 🔍	Do Not Post	⊞	⊟
ARACTIONL 🔍	Batch Standard	⊞	⊟
ARACTIONN 🔍	Batch Priority	⊞	⊟
ARPOST 🔍	Post Now	⊞	⊟

*Source Transaction [ARPAYWS] 🔍   Payment Worksheet   ⊞ ⊟

Process Group   Personalize | 🔲   First ◀ 1-4 of 4 ▶ Last

Process Group	Description		
ARACTIONA 🔍	Do Not Post	⊞	⊟
ARACTIONL 🔍	Batch Standard	⊞	⊟
ARACTIONN 🔍	Batch Priority	⊞	⊟
ARPOST 🔍	Post Now	⊞	⊟

*Source Transaction MTCHEXPTN 🔍 Match Exception ➕ ➖

| Process Group | | Personalize \| ⤢ | First ◀ 1 of 1 ▶ Last | |
Process Group	Description			
MATCHING 🔍	Matching		➕	➖

*Source Transaction MTCHOVRD 🔍 Match Override ➕ ➖

| Process Group | | Personalize \| ⤢ | First ◀ 1 of 1 ▶ Last | |
Process Group	Description			
MATCHING 🔍	Matching		➕	➖

*Source Transaction VCHR_STM 🔍 Voucher On-Demand Processes ➕ ➖
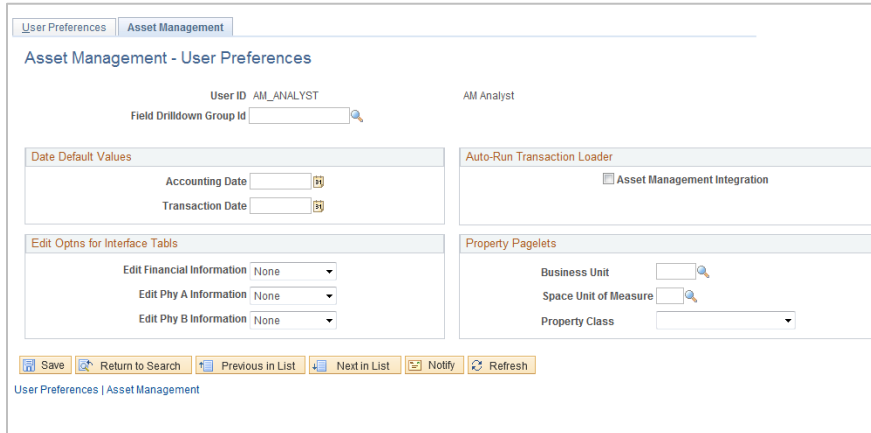
| Process Group | | Personalize \| ⤢ | First ◀ 1 of 1 ▶ Last | |
Process Group	Description			
PST_VCHR 🔍	All processes through Voucher Post		➕	➖

*Source Transaction VOUCHER 🔍 Voucher Entry ➕ ➖

| Process Group | | Personalize \| ⤢ | First ◀ 1-5 of 5 ▶ Last | |
Process Group	Description			
BUDGET_CHK 🔍	Budget Checking		➕	➖
DOC_TOL 🔍	Document Tolerance		➕	➖
MATCHING 🔍	Matching		➕	➖
MTCH_DT_BC 🔍	Matching, Doc Tolerance, Budget Check		➕	➖
PST_VCHR 🔍	All processes through Voucher Post		➕	➖
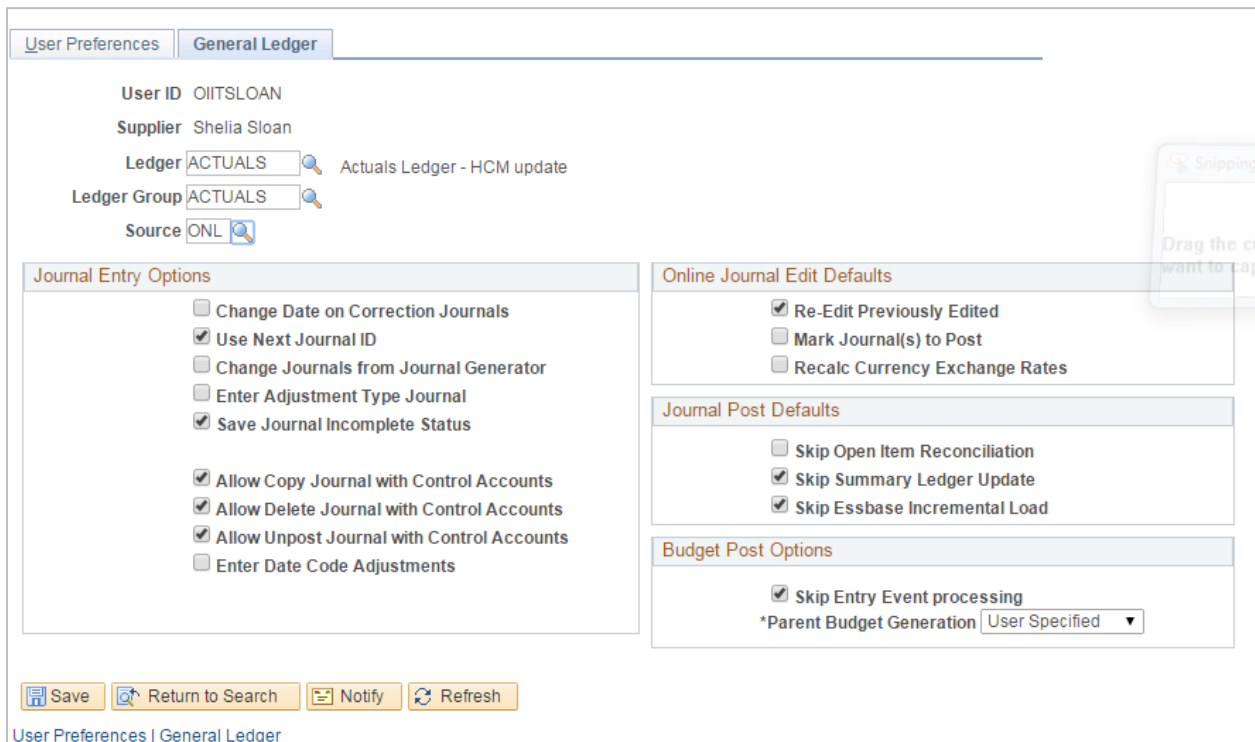
💾 Save   🔍 Return to Search   ✉ Notify   🔄 Refresh

Asset Management User Preferences:

General Ledger

- The **User ID** and **Name** fields default.
- Select the "**ACTUALS**" **Ledger.**
- Select the "**ACTUALS**" **Ledger Group**.
- Select a default **Source** (ONL)

Journal Entry Options

Change Date on Correction Journals – Select to change the journal date in the corrections journal which is on the journal suspense correction page.

If **Use Next Journal ID** is selected, the Journal ID field becomes unavailable, and the user cannot manually enter a journal ID on the journal entry page.

- Select **Change Journals from Journal Generator** to allow a user to update the ChartField and amounts on the Journal Entry page for a journal that was created by the Journal Generator process.
  - o Warning! If Change Journal from Journal Generator is selected, and the ChartField values are changed and reedit the journal, inconsistencies between the subsystem data and the general ledger data can be created.
- **Enter Adjustment Type Journal** – Select to allow a user to enter a book code adjustment type journal.
- **Save Journal Incomplete Status** – When you select this option for a specific user and the user adds a new journal the selected option appears on the journal header page of various journal entry options. This option enables the user to save journal entry transactions with an incomplete status and prevents them from being edited or posted until they are complete.
- **Allow GL Entry Event Bypass** – Select to enable the user to bypass selecting entry events in PeopleSoft General Ledger journal entry, even if they are required on the Installation Options – Entry Event page.

Online Journal Edit Defaults
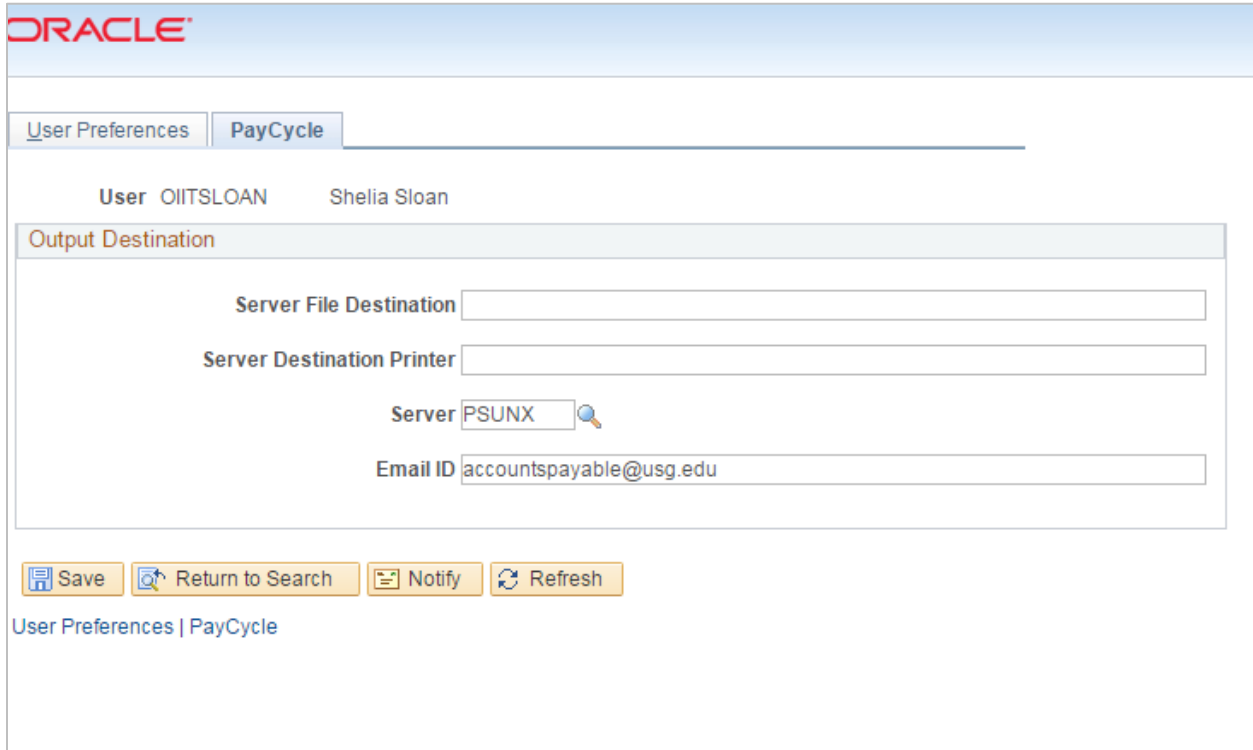
- **Re-Edit Previously Edited.** When this option is cleared, valid journals are not edited again when running Journal Edit from the Journal Entry page by clicking the Edit button. When you select this button users can reedit journals marked as valid.
- Select to **Mark Journal(s) to Post** – <mark>DO NOT USE!!!!! Bypasses Journal Workflow</mark>
- **Recalc Currency Exchange Rates** – USG does not use.
- **Journal Post Defaults**
- **Skip Open Item Reconciliation** – Select to bypass open items during the journal post process, allowing you to reconcile the open items at a later time by using the Open Item Maintenance page.
- Select **Skip Summary Ledger Update** to bypass summary ledger updates for this user ID when posting by clicking the post button during online journal entry.

Budget Post Options

- Select **Skip Entry Event Processing** to enable a user to post the budget that is associated with a journal entry or allocation without generating entry events through the Entry Event Processor. This may occur when an error occurs in a transaction; however, the entry event processing is correct.
- Select ***Parent Budget Generation** to enable a user to generate parent budget impacts when posting child budget journals. This option determines how the Generate Parent Budget(s) option on the Commitment Control - Budget Journals - Enter Budget Journals - Budget Header page acts.
  - o *Always Generate:* Select this option to always generate parent budget impacts. When this option is selected, the Generate Parent Budget(s) option on the Budget Header page is also selected and the field is unavailable and cannot be changed.
  - o *Never Generate*: Select this option to not generate parent budget impacts. When this option is selected, the Generate Parent Budget(s) option on the Budget Header page is cleared and the field is unavailable and cannot be changed.
  - o *User Specified*: Select this option to choose whether to generate parent budget impacts for each budget journal. When this option is selected, the Generate Parent Budget(s) option on the Budget Header page is available for the user to choose.

Paycyle User Preferences:

ORACLE

| User Preferences | PayCycle |

User OIITSLOAN   Shelia Sloan

Output Destination

Server File Destination [   ]

Server Destination Printer [   ]

Server [PSUNX]

Email ID [accountspayable@usg.edu]

[Save] [Return to Search] [Notify] [Refresh]
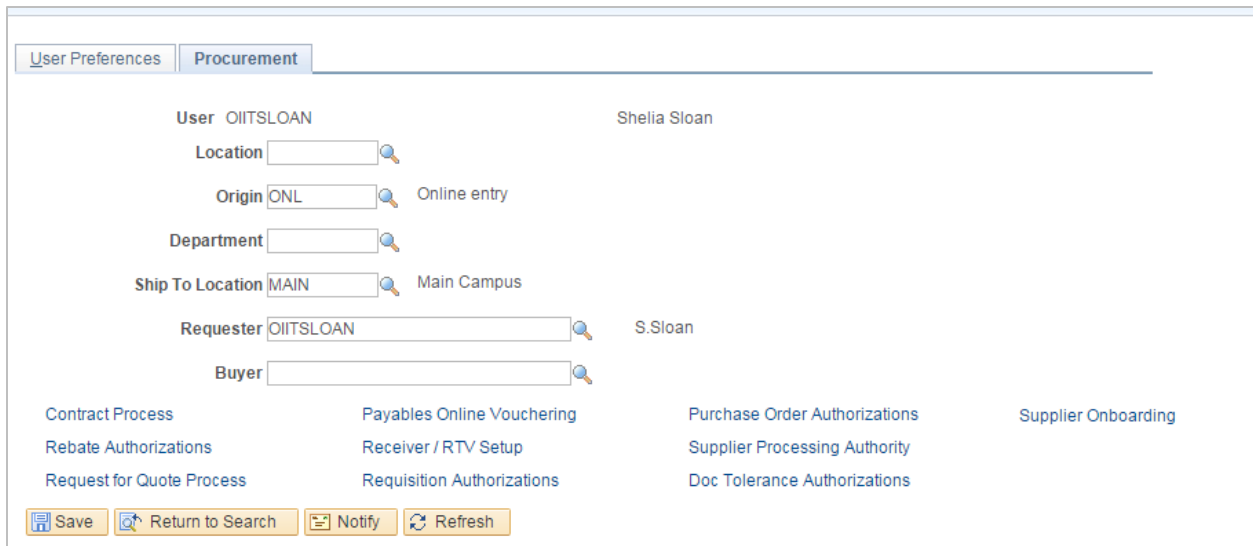
User Preferences | PayCycle

Select the PSUNX server on the user that runs the paycycle at your institution. The email ID field is new in 9.2. This EMAIL ID is the from email account used for the ACH payment Notifications.

Procurement

| User Preferences | Procurement |

User OIITSLOAN   Shelia Sloan

Location [   ]

Origin [ONL]   Online entry

Department [   ]

Ship To Location [MAIN]   Main Campus

Requester [OIITSLOAN]   S.Sloan

Buyer [   ]

Contract Process   Payables Online Vouchering   Purchase Order Authorizations   Supplier Onboarding

Rebate Authorizations   Receiver / RTV Setup   Supplier Processing Authority

Request for Quote Process   Requisition Authorizations   Doc Tolerance Authorizations

[Save] [Return to Search] [Notify] [Refresh]

- The **User** and **Name** default.
- Enter the default **Location** where requested items should be delivered when they are received.

- Enter the default **Origin**.
- Enter the **Department** (optional).
- Enter the **Ship to Location** (optional).
- **Requester** – This is Required if the user is a requester.
- Enter the **Buyer** authorized to enter Purchase Orders (PO's) (optional).
- Click the **Save** button.
- Select the **Payables Online Vouchering** link**.**

Payables Online Vouchering

- The **User ID** and **Name** default.
- **Default Values**
    - Select a voucher **Origin.**
- **Operator Voucher Authorities**
    - **Pay Unmatched Vouchers –**. This gives users the authority to pay vouchers that have not been matched up to the maximum amount that is specified in the Pay Unmatch Amt Field. Authorized users must select the Pay UnMatched Voucher Checkbox on the Voucher Attributes page in the Voucher component for the system to select the voucher during the Pay Cycle Process.

- o **Copy Matched and Closed PO** –Enables a user to copy matched and closed POs.
- o Select **Override Accounting Date Edit** to override the accounting date edit option on the Procurement Control - General Controls page.
- o **Pay Unmatch Amt**
- o Click **Security for Voucher Styles** to access the Voucher Styles page. The selected voucher style defines authority for each of the voucher styles checked.
  - ▪ Select the appropriate authorized voucher styles based upon responsibilities.
  - ▪ Click **OK**.

Voucher Styles

☑ Allow Regular Voucher

☐ Allow Register Voucher

☐ Allow Prepay Voucher

☐ Allow Journal Voucher

☑ Allow Adjustment Voucher

☐ Allow Third Party Voucher

☐ Allow Template Voucher

☐ Allow Reversal Voucher

☑ Allow Single Payment Voucher

☑ Allow Claim Voucher

OK   Cancel   Refresh

- • **Online Voucher Processing**
  - o **Do Not Check Voucher Amount** And **Check Voucher Amount**.- select one of these options to determine whether the system performs an edit during the online voucher entry against the voucher gross amount. If you selected Check Voucher Amount, specify the voucher entry limit amount for this user. When you specify the entry limit, you must also specify its currency and a rate type. If this user has the authority to prepay vouchers, you can specify a maximum amount for each prepayment that the user can enter. You must also specify a currency and a rate type for the prepayment.
  - o **Enter Vouchers Only in Groups. –** select to enable the user to enter only vouchers that are attached to a control group id as defined on the control group information page.
  - o **Post Vouchers** to post approved vouchers.
  - o **Manually Schedule Payments** to override the system's automatic payment scheduling. If the option is not selected, the scheduled payment information on the Voucher – Payments page cannot be modified.
  - o **Authority to Override Match** to override the match status of a voucher. If the voucher requires matching, the voucher match status can be changed to Not Applicable.
  - o **Record Payment** to manually record payments for a voucher. If this option is not selected, the payment action on the Payments page of the Voucher component cannot specify record.
    - Note: The Manually Schedule Payments option must be selected to record payments on a voucher.

- o **Override Withhold Calculation.** – Select to enable the user to override the timing of the withholding calculation on the withholding page of the voucher component. Withholding calculation can be at payment time or voucher posting time based on the withholding entity setting.

- **Quick Invoice Configuration**
  - o **Req. Valid Chart Field Combo's**. – Select this for the system to automatically validate chartfield combinations on the quick invoice vouchers. If the chartfield combination is invalid, the system prevents the user from saving the voucher.
  - o **Require Balanced Invoice. –** Select this check box for the system to automatically perform balancing algorithms on quick invoice vouchers. If the vouchers are out of balance, the system prevents the user from saving the voucher.

- Click **OK.**
- Select the **Receiver Setup** link.

Receiver Setup

Receiver Setup   ☒

Help

User OIITSLOAN   Shelia Sloan

Unit

☐ Change Non PO Receipt Price
☐ Interface Receipt
☐ Run Close Short
☑ Subcontract Streamline
☐ Blind Receiving Only   ○ No Order Qty   ○ Ordered Qty   ◉ PO Remaining Qty

Receiving Business Unit 98000 🔍   Board of Regents

Days +/- Today   30

RTV Dispatch Option   Default to Business Unit ▼

RTV Inventory Ship Option   Default to Business Unit ▼

RTV Inventory Destroy Option   Default to Business Unit ▼

OK   Cancel   Refresh

- The **User** and **Name** default.
- **Change Non PO Receipt Price** – Select to enable the user to change the receipt price for an item on a non purchase order receipt.
- **Interface Receipt**-Select to automate the passing of inventory and asset information through the Receiver Interface Push process.

- **Run Close Short**- Select to call the close short process automatically during the receiver interface push processing.
- **Subcontract Streamline** - Select this check box if you want the subcontract streamline check box to appear selected by default for a subcontracted purchase order receipt for this user. The user will be able to override this field setting for a subcontracted purchase order receipt. The system determines whether to perform subcontract streamlining (purchase order receipt and production completion for the production ID in a single step) from the receipt. Streamlining processing for subcontract RTVs enables you to process RTVs if the completions have been performed on the associated receipt. The system includes negative production completion and production scrap for operations being returned against the subcontract. If this box is deselected, the subcontract streamline check box ill appear deselected for a subcontracted purchase order receipt for this user. This user will not be able to change this field setting for the subcontracted purchase order receipt. That is, this assumes subcontract streamlining is not enabled for this user.
- **Blind Receiving Only** – Select to prevent the receiver from seeing the order quantity or the remaining quantity from the purchase order. The receiver needs to count the items before entering the quantity received. When you select this box, the No Order Qty, Ordered Qty, and the PO Remaining Qty check boxes are deselected.
- **No Order Qty** – Select to prevent the receiver from seeing the purchase order quantity. The receiver must specify the actual quantity that is received by doing a live count of the items.
- **Ordered Qty** – Select to user the purchase order quantity as the default quantity received.
- **PO Remaining Qty**- Select to use the remaining quantity (original order quantity minus previously received quantities) on the purchase order as the default quantity received.
- **Days +/- Today** – Enter the number of days plus or minus the current system date to be used as default search criteria on receiving pages when you are selecting purchase order schedules against which to receive.

- **RTV Dispatch Option** - Select the dispatch method as this user's preference for the return to vendor functionality. This functionality provides a default value for dispatching the RTV to the Supplier. RTV dispatch option values include: `Default to Business Unit:` Select to use the dispatch option that is defined at the business-unit level. You define the business unit RTV dispatch option value using the Business Unit Options tab on the Purchasing Definition page. When processing RTV options, the system initially checks the user preference and then the business unit when you select the `Default to Business Unit` option.

  Manual: Select to indicate that the Dispatch processing for the RTV must be performed manually.

  Often collaboration must take place between procurement personnel and another group before a RTV line can be dispatched. For example, you might have to verify the disposition of goods with warehouse personnel before dispatching the RTV.

- **RTV Inventory Ship Options -** Select the return to vendor ship option that you want to use as this user's default value for the Inventory Process field on the RTV line. This option will only be used by the RTV function when the disposition on the RTV line has a value of Ship. The system determines the ship option default value by first checking the user preference ship option value. If the user preference value is *Manual,Express,* or *Fulfillment* then the system uses the value as the default value. If the user preference value is *Default to Business Unit,* the system uses the ship option value defined at the business-unit level.
  RTV Inventory ship option values are:
  - *Default to Business Unit:* Select to use the inventory ship option that is defined at the business-unit level.
  - *Express:* Select to use the RTV express option to process Purchasing and Inventory data collection transactions at the same time. This means that the user can perform Inventory issue (automatic issue) action from within the Purchasing RTV component. If the RTV line disposition is Ship, the system creates a material stock request with a status of Shipped to update inventory.

- o Note: The value of *Express* will not be defaulted onto the RTV line if the RTV line is associated with an Inventory business unit which is defined as a Warehouse Management System (WMS) type. You define the warehouse setting using the Use External Warehouse Control check box on the Business Unit Options page for Inventory.
  - o *Fulfillment:* Select to set the user's preference to perform Inventory fulfillment processing for RTV transactions. This enables the user to create an Inventory material stock request transaction and to process it through Inventory fulfillment processing. The *Fulfillment* value is only valid for RTV processing when RTV line disposition is Ship.
  - o *Manual:* Select to indicate that the RTV ship transaction must be completed manually. This option requires that the inventory Express Issue function be used to ship the items to the supplier. When you use the *Manual* Inventory Ship option, the system does not perform RTV express functions. The user must use the Inventory Express Issue component to issue inventory returns that are being shipped to the vendor.

- **RTV Inventory Destroy Options -** Select the return to vendor destroy option that you want to use as this user's default value for the Inventory Process field on the RTV line. This option is only used by the RTV function when the disposition on the RTV line has a value of Destroy. The system determines the destroy option default value first by checking the user preference destroy option. If the user preference value is *Manual* or *Express* then the system uses that default value. If the user preference value is *Default to Business Unit,* the system uses destroy option defined at the business-unit level.
  RTV Inventory destroy option values are:
  - o *Default to Business Unit:* Select to use the inventory destroy option setting at the business-unit level.
  - o *Express:* Select to use the RTV express option to process Purchasing and Inventory data collection transactions at the same time. This means that the user can perform Inventory adjustment (automatic adjustment) actions from within the Purchasing RTV component.
  - o *Manual:* Select to indicate that the RTV destroy transaction must be completed manually. This option requires that the Inventory Adjustment function be used to update inventory for the items being returned to the vendor.

- **Select OK**
- **Select Purchase Order Authorizations** link.

Purchase Order Authorizations

- The **User** and **Name** default.
- Select **Can Work Approved POs** to change a purchase order that has already been approved or dispatched.
- **Can Dispatch Un-Approved POs** - Select to enable a user to dispatch purchase orders with a status of pending approval.
- Select **Full Authority for All Buyers** to add, update, cancel and close purchase orders for all buyers
- Select **Override Non-Qualified POs for Close** to close unqualified purchase orders.
- Enter "**View Only**" for the **Rebate ID Security Control.**
- **Select Approval** if the user is Purchase Order Approver.

Buyers User Authorization – Optional

- Enter **Buyers User Authorized For** the buyers for whom this user can enter purchase orders.
  - Select **"Add"**, **"Update"**, **"Cancel"**, **"Close"** and **"Reopen"**. (only if the full authority is not selected).

- Click **OK**
- Select the **Vendor Processing Authority** link.

Supplier Processing Authority
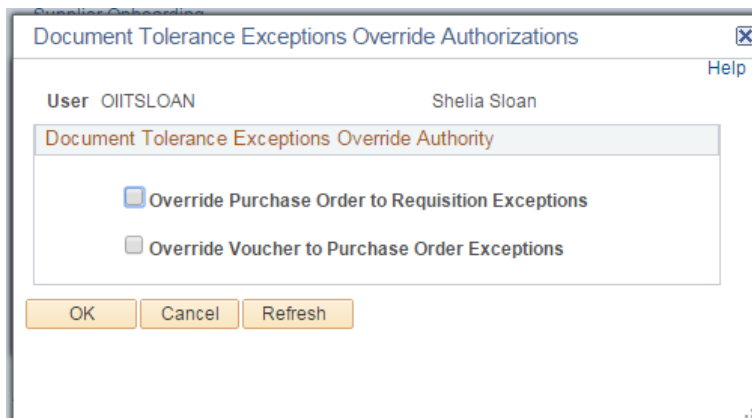
- The **User** and **Name** default.
- **Authority to Enter**- Select to allow user to enter a new supplier.
- **Authority to Approve** – Select to allow user to approve a supplier.
- **Authority to Inactivate** – Select to allow user to inactivate a supplier.
- **Supplier Audit** The Supplier Audit check box is selected by default. You can set up audit at Set ID level or supplier level if the check box is selected. If the check box is not selected, then users cannot set up audit but can inquire the supplier audit and run the audit log report.

   Use the supplier audit configuration template to select the desired fields to audit and to set the Reason flag which requires Reason Code and comments to be captured.

   Supplier Audit Template has H-Grid (Hierarchical Grid) for Supplier Address, Phone Information, and Supplier Contact Phone fields where it allows the user to enable and disable the audit and reason flag for the main field. When saved, it will enable the audit and reason flag for dependent fields attached to main field. One default Template ID is allowed per Set ID.
- Click **OK**.
- Click the **Doc Tolerance Authorizations link.**

Doc Tolerance Authorizations

- **Override Purchase Order to Requisition Exceptions** – Enables you to override document tolerance exceptions that are generated when an encumbrance exceeds the pre-encumbrance during document tolerance checking.
- **Override Voucher to Purchase Order Exceptions** - Enables you to override document tolerance exceptions that are generated when an expenditure exceeds the encumbrance during document tolerance checking.
- **Select OK**
- Click **the Requisition Authorizations link.**

Requisition Authorizations

- **Can Work Approved Req's -** Select to enable a user to change a requisition that has already been approved.
- **Full Auth for All Requesters -** Select to give the user authority to add, update, cancel, delete, and close requisitions for all requesters.
- **Override Preferred Supplier -** Select to enable a user to change the default supplier on a requisition line. If this authority is not selected, the user is unable to manually suggest a supplier.
- **Override RFQ Required Flag -** Select to enable a user to override the RFQ Required Rule option that was previously specified for a requisition in the requisition component.
- **View/Override VAT Details -** Select to view and override VAT details within the requisition component.
- **Override Non-Qualified Requisitions for Close** - Select to enable a user to close requisitions that are nonqualified for close.
- **Approval –** Allows a user to Approve Requisitions.
- **Cancel/Delete/Close/ReOpen –** Allows users to cancel/delete/close or reopen requisitions.
- **Requesters User Auth For -** Requesters for whom this user can work requisitions. Select the requester that you want to designate as the user's default requester by selecting the check box to the left of the requester's name.
- **Add/Update/Cancel/Close/Delete/Reopen -** Select to enable the user to add, update, cancel, delete, close, and reopen requisitions for this requester.

- **Select OK**
- **Click Save.**

Activity 3:

Login to FPLAY with your user id and password from fprod (not the one you created).

Navigate to Setup Financials Supply Chain, Common Definitions, User Preferences, Define User Preferences.

Pull up the user id you created in Activity 2.

Add Overall Preferences, and give them Requisition Authorization user preferences.

Give them full authority for all requesters, and save.

Managing Module Specific Security

PeopleSoft Financials modules may have module specific type security or considerations that need to be administered. Since USG has 28 different Business Units, it has to deliver security in a flexible manner. ITS has delivered Job Aids by Job Functions that each institution can use as a guide to create their own version of the job aids. See Appendix A for sample job aids. They are also the Georgia First Website for download. The benefit of creating institution specific job aids, is that security administrators can use these to setup user accounts for a specific function without having to guess what roles may be needed each time. Each institution may have different job duties in each area so it is up to the institution to define their requirements. Another important consideration within modules and cross modular is segregation of duties. Keep this in mind while creating your job aids.

Accounts Payable

The Accounts Payable module contains voucher security, paycycle security, 1099 security, new workflow security and setup and budget and budget date override security considerations. Keep in mind that a user should not be able to enter a voucher, approve it, run a paycycle and approve it also. This would be a segregation of duties issue. If you recall in the user preferences section on AP, there is a checkbox that says "allow user to enter vouchers in groups only". If this is selected, then one of your users will have to have the BOR_AP_CNTRL_GRPS_MAINT role to setup and approve Control Groups.

In 9.2 Voucher workflow was new for ITS. BOR_VOUCHER_BUD_REF_APPR role - This is approval role for vouchers with Budget Reference differences. BOR_VOUCHER_ASSET_APPR role - This is approval role for vouchers with Asset Issues. BOR_AP_ADMINXX (first two digits of institution id) -This role is for escalations or routing issues. Keep in mind that these three roles above are used only to route transactions to users. They do not contain page access. An approver will also have to have the BOR_AP_APPROVE_VCHR role to approve a voucher at any of the above levels. This role gives them the page access needed to get to the voucher to approve it. See Workflow Stage Docs in Appendix B.

If your institution makes ACH payments and would like all the from email addresses to be a generic email address such as accountspayable@XXX.edu, then there is a new user preference and setup page that must be configured. The person who normally runs the paycycle, can enter the generic email address on their user preferences on the screen below. Must only be setup for one user:

Favorites ▾ | Main Menu ▾ | > Set Up Financials/Supply Chain ▾ > Common Definitions ▾ > User Preferences ▾ > Define User Preferences

ORACLE | All ▾ Search | » Advanced Search | 🔍 Last Search Results

User Preferences | PayCycle

User arowell_54   Angela Rowell

Output Destination

Server File Destination |

Server Destination Printer |

Server | 🔍

Email ID ACHPAY@westga.edu

🖫 Save | 🔍 Return to Search | ⬆ Previous in List | ⬇ Next in List | 📧 Notify | 🔄 Refresh

User Preferences | PayCycle

Then on the PayCycle Selection Criteria page, you must enter the same user id under Payment Advice User ID.

Favorites ▾ | Main Menu ▾ | > Accounts Payable ▾ > Payments ▾ > Pay Cycle Processing ▾ > Payment Selection Criteria

ORACLE | All ▾ Search | » Advanced Search | 🔍 Last Search Results

Dates | Preferences | Source / BU | Bank / Method | Pay Group / Netting | Draft Options

Pay Cycle 54ACH   ACH pay cycle

Pay From Date 01/01/1900   Pay Through Date 07/30/2015   Payment Date 07/29/2015

- [ ] Use Supplier Pay Group
- [x] Process EFT/ACH Pre-Note
- [ ] Print LC Advice
- [ ] Automatic Increment Dates
- [x] Email Payment Advice
- [x] Print Email ACH/EFT Advice

- [x] Include Lost Discount
- [ ] Process Bank Charges
- [ ] Calculate Value Date
- [ ] Use Recipient's Pref. Lang.
- [x] Suppress Zero Amount Check

Report Output BI Publisher

Preferred Language English ▾

*Approval User Approval ▾

*Netting Option Not Applicable ▾

*Step Group [Model 🔍] All pay cycle steps

Credit Options

Credit Vouchers Process When DRs >= CRs ▾

*Date Limit No Date Limit ▾

Notification

Payment Error User ID [🔍]

Payment Advice User ID [arowell_54 🔍]

Bank Replacement Rule

SetID 54000 🔍   Rule Name UCB_CARRO 🔍

Minimum Amount Limits

Per Paycycle [0.000]   Currency Code [🔍]

Per Payment [0.000]   Rate Type [🔍]

Check Payment Message

Message |

If your Accounts Payables Users want to take advantage of the new dashboard/workcenter features, they will need the BOR_AP_DASHBOARD role, the BOR_AP_WORKCENTER role and the BOR_WORKCENTER_USER role.

Other Accounts Payable considerations includes User preferences as mentioned in the User Preference Section. These include Process Groups, which allow a user to run budget check, doc tol, post, etc directly from the voucher pages without relying on batch. This also include Matching process groups that allow a user to override a match exception. Don't forget to check user's commitment control rules for AP. If your user needs to override a Budget Date or a Budget Exception error on a Voucher, they will need OVRD_AP and/or BUDG_DT_AP commitment control rules. It is located under Commitment

Control, Define Budget Security, Assign rule to a User. See Commitment Control Section below. And, don't forget to run the request build process after assigning the rules to the user, or the change will not take effect. (IF you forget to run the request build process, the BORBATCH process that runs every night will run it for you.)

Expenses

The Expenses Module allows employees to enter expense reports, travel authorizations and cash advances for travel related purposes. Basic self-service access can be granted by self-registering for a user account. The Base role of BOR PeopleSoft User contains expenses access in self-service for Expense reports and travel authorizations. If you institution uses Cash advances, those are administered via a separate role. If your institution chooses not to use travel authorizations, the base role would be BOR PeopleSoft User – no tauth. If your institution doesn't use expenses at all, the base role would be BOR PeopleSoft User – no exp. So travelers, would be able to login to the self service portal from anywhere and complete their expense reports.

Expenses should have an overall administrator since there a lot of setup pieces to expenses. The BOR_EX_ADMINISTRATION role should be granted to this individual. This individual would maintain default chartfields and bank accounts for travelers, update delegates, update designates, potentially maintain approver assignments for workflow.

Expenses uses workflow as well, although it is setup differently from most modules and isn't as flexible. It doesn't route via a role, as the other modules do, it routes to the individual that is defined on the approver assignments pages. The approvers in Expenses need the BOR_EX_APPROVAL role. This role is the only role in the system where we use the Dynamic role assignment. In other words, do not manually assign this role to a user. Once you place the user id on the approver assignments pages, they are automatically assigned that role via a role query in the background. In addition to the approvers that are assigned on the approver assignments pages, an Expenses Admin is needed, and this individual will need the BOR_EX_ADMINXX role (XX is the first two digits of your institution id). This individual will receive transactions that can't find an approver, or have escalated.

It is important to note that with Expenses and some of the other modules, a lot of employee notifications are sent out. These notifications go to the email address listed on the user id of the employee. Also the Email checkbox on the user profile, workflow tab must be selected for the individual to receive notifications.

Like Accounts Payable, don't forget to check user's commitment control rules for EX. If your user needs to override a Budget Date or a Budget Exception error on a Expenses Transaction, they will need OVRD_EX and/or BUDG_DT_EX commitment control rules. It is located under Commitment Control, Define Budget Security, Assign rule to a User. See Commitment Control Section below. And, don't forget to run the request build process after assigning the rules to the user, or the change will not take effect. (IF you forget to run the request build process, the BORBATCH process that runs every night will run it for you.)

> **Activity 5:**
>
> Login to F92PLAY-selfservice.gafirst.usg.edu with the user id you created in activity 4.
>
> Navigate to Employee Self Service, Travel and Expenses Center, and confirm you can see Create Expense Report.

eProcurement

The eProcurement modules features many different security components. Not only does it have Regular Page Access type roles and Workflow Roles, but it also has Role Action type roles. The Security Job Aids by Job Functions outline a lot of the ePro roles and responsibilities, and the Workflow Stage Documents explain the workflow options as well.

Types of Roles Involved
In order for the ePro and Georgia*FIRST* Marketplace functionality to work properly, users are set up with specific roles and responsibilities. They include:

- Shoppers: These users are the ones who select items in the Georgia*FIRST* Marketplace.
- Browsers: Users without any Georgia*FIRST* Marketplace roles assigned will default to a Marketplace Browser. Browsers can view the items, contracts, and prices in the Marketplace but cannot shop or create requisitions.
- Requesters: These users take the shopping carts created by Shoppers and turn them into ePro Requisitions. Requesters can also build their own shopping carts, just like Shoppers.
- Approvers: These users are set up to approve ePro Requisitions.
- Buyers: These users are responsible for ensuring approved requisitions are sourced into a Purchase Order and dispatched to the vendor.

- AP Personnel: The AP office processes the resulting invoice from the vendor.
- ePro Administrator: This user monitors the approval workflow, to make sure requisitions are worked in a timely fashion
- Local Security Administrator: This user is responsible for setting up others users in their appropriate roles.

As the Local Security Administrator, you are primarily responsible for setting up users with the proper roles and access. In addition, you will need to work with the ePro Administrator occasionally to perform maintenance on these users, such as updating email addresses. Since Workflow is such a critical piece of eProcurement, the user setup is very important.

Let's start with Requesters.

Requesters are those individuals who will be creating ePro Requisitions either from Special Request items or from shopping carts in the Georgia*FIRST* Marketplace.

Requester Security Roles

The Requester position (as well as many additional roles for ePro) requires the proper 'maintain' role to maintain requisitions. The role that you choose is dependent on whether or not your institution is implementing SciQuest, or the Georgia*FIRST* Marketplace. The BOR_EP_MAINT_REQ and BOR_EP_MAINT_REQ_SCI roles are the same, except the BOR_EP_MAINT_REQ_SCI role has access to the "Web" tab for access to the Georgia*FIRST* Marketplace. The BOR_EP_MAINT_REQ role will not have access to the Web tab to enter and maintain Marketplace requisitions.

Role Name	Purpose
BOR PeopleSoft User	Basic PeopleSoft User access
BOR_CAT_Requester*	Enables the Requester to create requisitions from Georgia*FIRST* Marketplace shopping carts, as well as create their own shopping carts (this role is not needed if the institution is not implementing the Georgia*FIRST* Marketplace)
BOR_EP_REQUESTER BOR_EP_REQUESTER_YE_CUTOFF**	Enables the Requester to be set up as a Requester in the system
BOR_AD_HOC_APPROVE	Enables the Requester to insert additional approvers in the approval Workflow when needed
BOR_EP_MAINT_REQ BOR_EP_MAINT_REQ_SCI BOR_EP_MAINT_REQ_YE_CUTOFF** BOR_EP_MAINT_REQ_YE_CUTOFF**	Enables the Requester to edit and track requisitions in the system. If your institution is implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ_SCI. If your institution is not implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ.

If the requester will also be a Shopper, give them the BOR_CAT_Requester role only. Users should not have multiple "BOR_CAT" roles.

*** If you want to cutoff your requesters access to create requisitions at year end, give them the roles with the _YE_CUTOFF at the end, instead of the regular roles. Then on a date in June, determined by USO, access to create requisitions is removed from those roles. This access is re-established in early July.*

Requester Setup

After setting up the security roles for a Requester, you also must set up the individual as a Requester. If you have a user that is Just a Shopper, they will still need the Requester Setup page completed so that the person they assign their carts to, can choose them as the requester once it is turned into a requisition.

How To: Set Up a Requester

1. In the menu, select **Set Up Financials/Supply Chain**.
2. Select **Product Related**.
3. Select **Procurement Options**.
4. Select **Purchasing**.
5. Select **Requester Setup**.
6. Select the **Add a New Value** tab.
7. Enter the requester's **User ID** in the **Requester** field.
8. Click the **Add** button.
9. Ensure the status is set to **Active**.
10. In the **ShipTo SetID** field, enter your institution's **SetID**.
11. In the **ShipTo** field, enter/select the default **Ship To address** for this Requester.
12. In the **Location SetID** field, enter your institution's **SetID**.
13. In the **Location** field, enter/select the default **Location** for the Requester.
14. In the **PO Origin SetID** field, enter/select **SHARE**.

15. In the **Origin** field, select **ONL**.

16. In the **Currency** field, enter/select **USD**.

17. Enter a phone and fax number if desired.

18. Select the **Pending** option in the Requisition Status box.

19. In the **GL Unit** field, enter/select your institution's business unit.

20. In the **Fund** field, enter/select this Requester's Default Fund Code.

21. In the **Dept** field, enter/select this Requester's default Department.

22. In the **Program** field, enter/select this Requester's default Program Code.

23. In the **Class** field, enter/select this Requester's default Class Field.

24. In the **Project** field, enter/select this Requester's default Project ID (if any).

25. In the **Bud Ref**, enter/select the current budget year.

26. Leave the Account field blank.

27. In the **Catalog Information** section, select the **Default** checkbox.

28. In the **SetID** field, enter/select **SHARE**.

29. In the **Catalog ID** field, enter/select **NIGP_TREE**.

30. **Save** the page.

Don't forget to setup user preferences as well. These were defined in an earlier user preference section. You also have Buyer setup to complete but I will cover this in the Next Section which is Purchasing.

A critical component to the whole eProcurement process is the ability to submit requisitions for approval electronically. Because approvals are handled online within the PeopleSoft Financials system, each institution can customize the approval process to their own specifications. In this chapter, we are going to outline the possible approval stages that your institution may choose to use.

How Do Approvals Work?

As mentioned earlier, a Requester builds a requisition in ePro. Each item on a requisition is actually placed on its own requisition line. Theoretically, each line in a requisition can be charged to a different set of Chartfields. Therefore, there may be different approval paths for each line on a requisition.

Once the Requester submits the requisition for approval, each line has its own approval path. This approval path is determined by a number of factors. At a minimum, each requisition line will go to the Department Manager and Project Manager (if a Project is to be charged). These are the managers that are tied into the Department and Project Chartfields on that requisition line.

Depending on how your institution has set up approvals for eProcurement, the requisition line may go to many additional approvers as well. This includes approvers for assets, IT items, and items above a certain amount. Below is a summary of all of the approval stages and paths available for eProcurement. To determine what stages and paths your institution is using, check with your Purchasing Department or Local Security Administrator.

Approval Stages

Overall, there are five approval stages that can be used for eProcurement requisitions. They include:

- Stage 1: Department and Project Approval
- Stage 2: Fund Approval
- Stage 3: Amount Approval (for requisitions built from the Georgia*FIRST* Marketplace)
- Stage 4: Item-Type Based Approvals
- Stage 5: Buyer Approval (for requisitions not built from the Georgia*FIRST* Marketplace)

Here is a summary of each stage:

Also Keep in mind that each stage/path have different security workflow roles that control the routing of the transaction. Each approver will still also need the BOR_EP_REQ_APPROVE role in addition to the workflow roles, since it contains the page access to allow approval.

Stage 1: Department and Project Approval

This is a mandatory approval stage for all requisition lines. Each requisition line must be charged to a Department. In addition, requisition lines can be charged to a Project. The requisition line is routed to the Department Manager (as entered in PeopleSoft) for approval. If the Project Chartfield is used on the requisition line, the system also routes it to the Project Manager.

Stage 2: Fund Approvals

This approval stage is an optional one for institutions. There are three options on this stage. The First Option is the Agency Fund Approval. It is set up so that any requisition line charged to an Agency Fund Code must go to an individual specified for Agency Fund Approvals. Agency funds are used to account for resources held by an institution as custodian or fiscal agent for individual students, faculty, staff members, or other organizations. Agency Fund Codes include 60000, 61000, and 62000.

If your institution chooses to employ this approval stage, there may be multiple Agency Fund Approvers. Each Agency Fund Approver will have the role BOR_AGENCY_FUND_APPR. The institution will determine whether all amount approvers must approve the requisition or if only one from the group of multiple approvers has to approve it. If an agency fund code is not used on a requisition line, the system bypasses this approval stage.

The Next Option is the Tech Fee approval. Any requisition that has fund code 16000 would route to an approver with the role BOR_TECH_FEE_APPR role.

The last Fund Approval Option is the Grant Approval. This is available if your institution wants to route requisitions that have Fund Code 20000 to a user with the role BOR_GRANT_APPR role. This individual/s could be different that the individual on the project chartfield.

Stage 3: Amount Approval

The Amount Approval stage is also an optional one. This stage is for all requisitions that were built from the Georgia*FIRST* Marketplace and has a monetary amount of $10,000 or more. Again, your institution may set up multiple approvers to serve as the Amount Approver. Each Amount Approver will have the

role BOR_CAT_AMOUNT_APPR. The institution will determine whether all amount approvers must approve the requisition or if only one from the group of multiple approvers has to approve it. The institution also does not have to use the $10,000 threshold and can edit this if needed.

If the requisition was not generated from the Georgia*FIRST* Marketplace, it will bypass this approval stage (this can be changed by the institution). If the requisition is below the set threshold and was generated from the Georgia*FIRST* Marketplace, it will also bypass this approval stage.

Stage 4: Item-Type Based Approvals

In Approval Stage 4, approvals are based upon the type of item being requested. Within this stage, there are seven potential approval paths. Each path is optional for the institutions.

- **Stage 4, Path 1: Asset Approval**
  If the item on a Requisition line is an asset and charged to an Asset Account, it will be routed to the person set up as the Asset Approver. The accounts included in this path are 743200, 744200, and 800000 through 899999.

  An Asset Approver must have the role "BOR_ASSET_APPR." If your institution chooses to use the Asset Approver path, there can be multiple asset approvers. The institution will determine whether all asset approvers must approve the requisition or if only one from the group of multiple approvers has to approve it. In addition, institutions may identify additional account codes for asset approval, and they may add monetary amount criteria (i.e., item charged to Account 743200 and is greater than $5,000.).

- **Stage 4, Path 2: Audio Visual Approver**
  This is an optional approval path and is for any item on a requisition line that contains an NIGP code related to Audio Visual items or services. NIGP stands for National Institute of Governmental Purchasings Commodity Services Code. The NIGP Code is a coding classification used primarily to classify products and services procured by state and local governments.

  In PeopleSoft, the Category ID is tied into the NIGP Code. In the Georgia*FIRST* Marketplace, the NIGP code is already tied into item. For requisition line items not generated from the Marketplace, the Requester enters the proper Category ID. For those line items that have an NIGP Code related to Audio Visual items and services, the system will route the requisition line to the Audio Visual Approver.

  An Audio Visual Approver must have the role "BOR_AUDIO_VIS_APPR". If your institution chooses to use the Audio Visual (AV) Approver path, there can be multiple AV approvers. The institution will determine whether all AV approvers must approve the requisition or if only one from the group of multiple approvers has to approve it. In addition, institutions may identify additional NIGP codes for audio visual approval, and they may add monetary amount criteria (i.e., item has an NIGP code of 06400 and is greater than $1,000.).

- **Stage 4, Path 3: Chemical Approver**
  This path is also an optional one, and is for any requisition line with an NIGP code associated with chemicals. If the NIGP code for the requisition line is associated with a chemical purchase, the line will route to the Chemical Approver.

  A Chemical Approver must have the role "BOR_CHEMICAL_APPR". If your institution chooses to use the Chemical Approver path, there can be multiple Chemical Approvers. The institution will determine whether all chemical approvers must approve the requisition, or of only one from the group of approvers must approve it. In addition, institutions may identify additional NIGP codes for chemical approval, and they may add monetary amount criteria.

- **Stage 4, Path 4: Facilities Planning and Design Approver**
  This optional path is for any requisition line with an NIGP code associated with the facilities planning and design.

  A Facilities Planning and Design Approver must have the role "BOR_FACILITIES_APPR". If your institution chooses to use the Facilities Planning and Design Approver path, there can be multiple approvers in this path. The institution will determine whether all Facilities Planning and Design approvers must approve the requisition, or if only one from the group of approvers must approve it. In addition, institutions may identify additional NIGP codes for facilities planning and design approval, and they may add monetary amount criteria.

- **Stage 4, Path 5: IT Approver**
  This approval path is for any IT hardware or software approvals, and is also optional. For any requisition line that is for a computer hardware or software purchase or service (based on NIGP Code), the system routes the line to the IT Approver.

  An IT Approver must have the role "BOR_IT_APPR". If your institution chooses to use the IT Approver path, there can be multiple approvers in this path. The institution will determine whether all IT Approvers must approve the requisition, or if only one from the group of approvers must approve it. In addition, institutions may identify additional NIGP codes for IT approval, and they may add monetary amount criteria.

- **Stage 4, Path 6: University Relations Approver**
  The sixth approval path in stage 4 is also optional and is for the University Relations Approver. For any requisition line that relates to media contact, logo use or copyright items (based on NIGP code), the system routes it to the University Relations Approver.

  The University Relations Approver must have the role "BOR_UNIVREL_APPR". If your institution chooses to use the University Relations Approver path, there can be multiple approvers in this path. The institution will determine whether all University Relations Approvers must approve

the requisition, or if only one from the group of approvers must approve it. In addition, institutions may identify additional NIGP codes for University Relations approval, and they may add monetary amount criteria.

- **Stage 4, Path 7: Default NIGP Code – 00000**
  The seventh approval path in stage 4 will route to a Buyer Approver in the event that a Georgia*FIRST* Marketplace Requisition line does not have an NIGP code. If the line item does not have an NIGP code, it will default to the "00000" NIGP code. This requisition line will automatically route to a Buyer Approver for correction.

- **Stage 4, Path 8: Furniture Approver**
  The Furniture Approver must have the role "BOR_FURNITURE_APPR". If your institution chooses to use the Furniture Approver path, there can be multiple approvers in this path. The institution will determine whether all Furniture Approvers must approve the requisition, or if only one from the group of approvers must approve it. In addition, institutions may identify additional NIGP codes for Furniture approval, and they may add monetary amount criteria.

- **Stage 4, Path 9: Human Resource Approver**
  The Human Resource Approver must have the role "BOR_HUMAN_RES_APPR". If your institution chooses to use the Human Resource Approver path, there can be multiple approvers in this path. The institution will determine whether all Human Resource Approvers must approve the requisition, or if only one from the group of approvers must approve it. In addition, institutions may identify additional NIGP codes for Human Resource approval, and they may add monetary amount criteria.

- **Stage 4, Path 10: Pharmaceutical Drug Approver**
  The Pharmaceutical Drug Approver must have the role "BOR_PHARM_DRUG_APPR". If your institution chooses to use the Pharmaceutical Drug Approver path, there can be multiple approvers in this path. The institution will determine whether all Pharmaceutical Drug Approvers must approve the requisition, or if only one from the group of approvers must approve it. In addition, institutions may identify additional NIGP codes for Pharmaceutical Drug approval, and they may add monetary amount criteria.

- **Stage 4, Path 11: Budget Reference Approver**
  Any requisition line where the budget reference does not equal the fiscal year will route to a Budget Reference Approver. This approver must have the BOR_EP_BUD_REF_APPR security role.

Stage 5: Buyer Approval

In Approval Stage 5, the system will route all special request requisitions (those requisitions not built from the Georgia*FIRST* Marketplace) to the person designated to give buyer approval. This stage is primarily used for Special Request Requisitions since they are not built from contract-approved catalogs. The Buyer Approver can then ensure the line item meets all procurement policies.

Institutions may choose to have multiple Buyer Approvers. In addition, the Institution can choose whether all Buyer Approvers must approve the requisition or if only one needs to act on it. Finally, the institution may choose to inactivate this stage or include it for all requisitions. This user will need the BOR_BUYER_APPR role.

Approval Time Limits

Within the system, there are built-in time limits that an approver has to act on the requisition. This ensures that ePro requisitions do not sit around waiting for an approver for an indefinite amount of time.

When a requisition is submitted for approval, the system sends it to the first approver's Worklist, within PeopleSoft Financials. The Worklist is a queue which holds items waiting for approval. Once an approver works a transaction, it is removed from their Worklist.

Once the requisition hits an Approver's Worklist, that approver has a predetermined amount of days to either approve or deny it, before they get a reminder notification from the system. If the requisition sits in an Approver's Worklist past those days without being approved or denied, the system removes the requisition from that Approver's Worklist, routes it to the ePro Administrator, and the ePro Administrator reassigns the transaction to another approver. After the Approver has approved the requisition, the system automatically moves it onto the next Approver's Worklist. If an Approver denies a requisition, the system returns it to the Requester. Denied requisition lines can be edited and resubmitted for approval.

If an approver will be out of the office for an extended period of time and will be unable to work the requisitions in their Worklist, they have the ability to assign an alternate to serve in their place. This way, their Worklist does not build up while they are out of the office, and requisition approval is not delayed.

Each institution is able to customize the number of days as to when the system will send reminder emails and escalates a requisition.

ePro Administrators must also be set up in the system with the correct security roles. This enables the ePro Admin to set up eProcurement components, including:

- Approver Setup
- Requester Setup
- Reassigning Worklist Items
- Assignment of Alternate Users

The ePro Admin is also responsible for working with the Security Administrator to understand the necessary user security needs relative to security roles, role actions, and routing controls.

ePro Admin Security Roles

Role Name	Purpose
BOR PeopleSoft User	Basic PeopleSoft User access

BOR_EP_ADMINXX	Enables the ePro Admin to manage ePro Workflow; the "XX" is the institution's first two digits in their SetID
BOR_EP_CONFIG_SETUP	Enables the ePro Admin to configure the system for eProcurement
BOR_EP_REASSIGN	Enables the ePro Admin to reassign requisitions that are routed to them due to escalation or Workflow errors

ePro Approver Setup

All ePro Approvers must also be setup with specific security roles. In addition, depending on the type of approver they are, they will need to have a specific security role to match their approver type. For example, Department and Project approvers simply need the basic security roles for an approver. Special Item Category approvers need the basic security roles, along with their specialized approver role (i.e., BOR_IT_APPR for your institution's IT approvers).

Basic Approver Security Roles

Role Name	Purpose
BOR PeopleSoft User	Basic PeopleSoft User access
BOR_AD_HOC_APPROVE	Enables the Approver to insert additional approvals into the Workflow when necessary
BOR_EP_REQ_APPROVE	Enables the Approver to approve/deny requisitions
BOR_EP_MAINT_REQ or BOR_EP_MAINT_REQ_SCI	Enables the Requester to edit and track requisitions in the system. If your institution is implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ_SCI. If your institution is not implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ.

Special Item Approver Security Roles

In addition to the security roles in each section above, there are certain users that may need role action type roles. The following two roles already contain role actions.

The **BOR_ASSET_APPR** security role contains the role action of "Can Change Distrib" and "Can Change Schedule." This allows the approver to change any field on the requisition distribution or schedule without restarting the approval process on requisitions that are not fully approved.

The **BOR_BUYER_APPR** security role contains the role action of "Can Change All." This allows the approver to change any field on the requisition, including quantity and price, without restarting the approval process on requisitions that are not fully approved.

If any other approver needs a role action, you can assign these role actions the individual users. These role actions are also added under the Distribution User Profile > User Roles tab.

Role Name	Purpose
BOR_EP_RA_CHANGEALL	Allows the Approver to update any portion of the requisition

	without restarting Workflow on requisitions that are not fully approved. If the Requisition has been approved and the approver makes a change, the requisition will re-route back through Workflow.
BOR_EP_RA_CHANGEDISTRIB	Allows the Approver to update the distribution of the requisition without restarting Workflow on requisitions that are not fully approved. If the Requisition has been approved, and the approver makes a change, the requisition will re-route back through Workflow.
BOR_EP_RA_CHANGEHDR	Allows the Approver to update the header of the requisition without restarting Workflow on requisitions that are no fully approved. If the Requisition has been approved and the Approver makes a change, the Requisition will re-route back through Workflow.
BOR_EP_RA_CHANGELINE	Allows the Approver to update the line of the requisition without restarting workflow on requisitions that are not fully approved. If the Requisition has been approved and the approver makes a change, the requisition will re-route back through Workflow.
BOR_EP_RA_CHANGESCHED	Allows the approver to update the schedule of the requisition without restarting Workflow on requisitions that are not fully approved. If the Requisition has been approved and the approver makes a change, the requisition will re-route back through Workflow.

Without any of the above role action roles assigned, if an approver updates information on the requisition, such as Chartfield information, the requisition will have to be re-routed back through the approval levels.

For your Department and Project Managers, in addition to setting up their security roles and user preferences, you also need to setup the Department and Project Chartfields with the correct manager User ID.

Department Manager ID

In the Department Chartfield, you need to indicate who the Department Manager is. This field is what Workflow uses for requisitions. When a requisition is charged to a particular department, Workflow is designed to route that requisition to the manager listed on the Chartfield definition.

When updating the Department Chartfield, you need to make sure that the Department's status is "**Active**." Also, you need to be in "**Correct History**" mode. Once you complete the Manager ID field, the Manager Name field should populate as well, once you tab out of the field.

How To: Update a Department Manager ID

1. In the menu, select **Set Up Financials/Supply Chain**.
2. Select **Common Definitions**.
3. Select **Design Chartfields**.
4. Select **Define Values**.
5. Select **Chartfield Values**.
6. Select **Department**.
7. On the **Find an Existing Value** page, enter/select the **Department ID** in the **Department** field.
8. Click the **Search** button.
9. Select the **Department** you want to update.
10. Ensure the Department status is **Active**.
11. Click the **Correct History** button.
12. Select the **Manager ID** look up icon.
13. Enter the last name of the Department Manager in the **Last Name** field.
14. Click the **Look Up** button.
15. Select the correct **User ID** for the Department Manager.
16. Click the **Save** button.
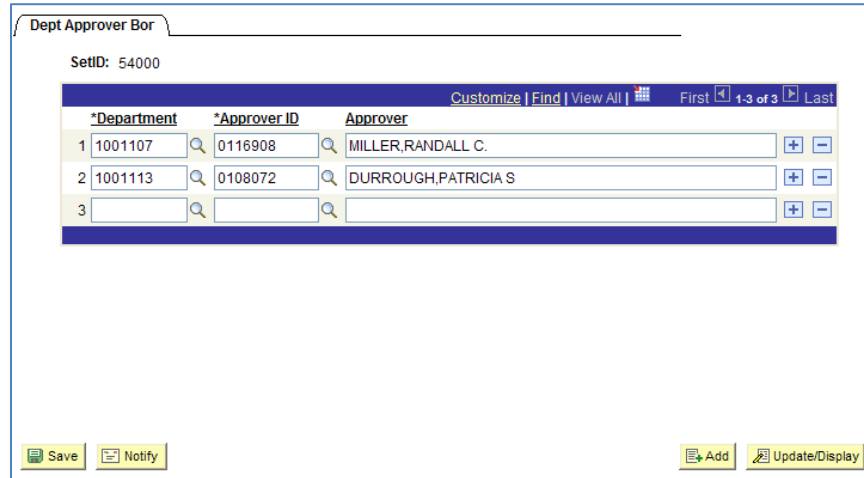
Additional Department Managers

The way Workflow is initially setup, there is only one User ID that you can specify for your Department Manager. If your institution wishes to have multiple department approvers, you can use the **Department Approver** page to specify additional Department managers. These additional Department Managers must also have their security roles and user preferences completed for them.

Important Note: Before using this page for the first time, contact ITS to make a change to your institution's Workflow configuration.

On the **Department Approver** page, you can add multiple approvers for multiple departments. The first time you add multiple approvers, you need to select the Add a New Value tab and add the value using your institution's SetID. After adding your institution the first time, you can add additional approvers through the Find an Existing Value tab (using your SetID).

For each additional approver, you first need to specify the department. Then, you select the User ID of the additional approver. To add additional approvers, you can select the Add a New Row button, and continue to add the additional approvers for the necessary departments.
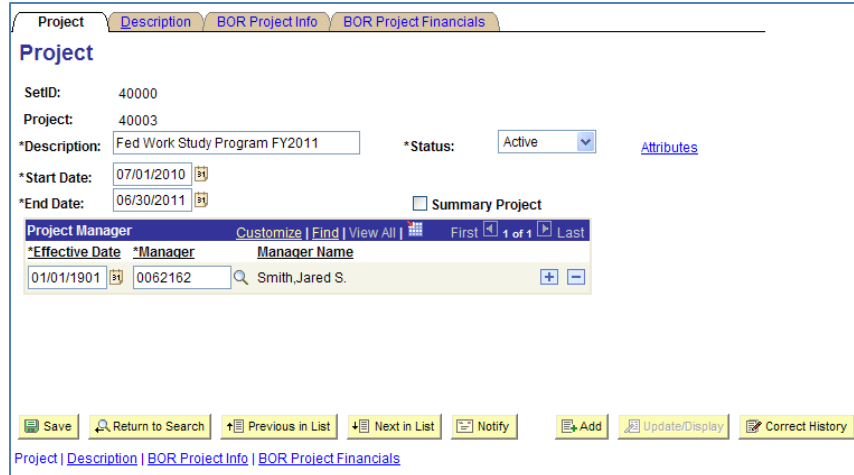
How To: Update Additional Department Managers

1. In the menu, select **Set Up Financials/Supply Chain**.
2. Select **Common Definitions**.
3. Select **Design Chartfields**.
4. Select **Define Values**.
5. Select **Department Approver**.
6. If this is the first time you are adding an additional Department Manager for your institution, select the **Add a New Value** tab. If this is not the first time, select the **Find an Existing Value** tab.
7. Enter/select your institution's **SetID** and click **Add** or **Search**.
8. On a blank row, enter/select the **Department ID** for the Department you want to add an additional approver for.
9. Enter/select the additional Approver's **UserID** in the Approver ID field. **Tab** out of the field to populate the Approver field.
10. To insert additional approvers, select the **Add a New Row** button and repeat steps 8 & 9.
11. Click the **Save** button.

Project Manager ID

In the Project Chartfield, you need to indicate who the Project Manager is. This field is what Workflow uses for requisitions. When a requisition is charged to a particular project, Workflow is designed to route that requisition to the manager listed on the Chartfield definition.

When updating the Project Chartfield, you need to make sure that the Project's Status is "Active." Also, you need to be in "Correct History" mode. Once you complete the Manager Id field, the Manager Name should populate as well, once you tab out of the field.

How To: Update a Project Manager ID

1. In the menu, select **Set Up Financials/Supply Chain**.
2. Select **Common Definitions**.
3. Select **Design Chartfields**.
4. Select **Define Values**.
5. Select **Chartfield Values**.
6. Select **Project**.
7. On the **Find an Existing Value** page, enter/select the **Project ID** in the **Project** field.
8. Click the **Search** button.
9. Select the **Project** you want to update.
10. Ensure the Project status is **Active**.
11. Click the **Correct History** button.
12. Select the **Manager ID** look up icon.
13. Enter the last name of the Project Manager in the **Last Name** field.
14. Click the **Look Up** button.
15. Select the correct **User ID** for the Project Manager.
16. Click the **Save** button.

Purchasing

The Purchasing module encompasses Purchase Orders, Suppliers, Receiving etc. In this module, we will also cover Buyer setup and configuration. Purchasing in 9.2 is now configured with Workflow using the approval process instead of route controls as was delivered in 8.9. We will cover delivered Purchasing workflow in this section as well.

Buyer Setup

Buyers are individuals who in addition to creating their own requisitions, process requisitions from others and perform purchasing-related maintenance tasks. They are also responsible for sourcing requisitions into purchase orders, processing purchasing transactions, running purchasing-related reports, and maintaining Purchasing-related configuration.

Buyer Security Roles

Role Name	Purpose
BOR PeopleSoft User	Basic PeopleSoft User access
BOR_AD_HOC_APPROVE	Enables the Buyer to insert additional approvals into the Workflow when necessary
BOR_EP_REQUESTER	Enables the Buyer to create their own requisitions
BOR_EP_BUYER_CENTER	Enables the Buyer to access the Buyer Center in order to expedite requisitions
BOR_EP_INQUIRY	Enables the Buyer to run inquiries on requisitions
BOR_EP_PROCESSES	Enables the Buyer to run requisition processes
BOR_EP_REQ_APPROVE	Enables the Buyer the ability to approve requisitions that are assigned to him/her
BOR_PO_REQ_WORKBENCH	Enables the Buyer to use the Workbenches for requisitions
BOR_PO_INQUIRY	Enables the Buyer to run inquiries on purchase orders
BOR_PO_MAINTAIN	Enables the Buyer to perform maintenance on existing POs

BOR_PO_PROCESS	Enables the Buyer to run purchasing processes
BOR_PO_REPORTS	Enables the Buyer to run purchasing reports
BOR_PO_REQ_PROCESS	Enables the Buyer to process requisitions thru Purchasing
BOR_PO_SETUP_CONFIG	Enables the Buyer to configure the system for purchasing
BOR_PO_VENDORS_MAINT	Enables the Buyer to add or maintain suppliers in the system
BOR_EP_MAINT_REQ and BOR_EP_MAINT_REQ_SCI	Enables the Requester to edit/track requisitions in the system. If your institution is implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ_SCI. If your institution is not implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ.
BOR_BUYER_APPR	Enables the Buyer to approve requisitions, update the requisitions, and not restart Workflow
BOR_CAT_Requester	Enables the Buyer to shop and create requisitions in the Georgia*FIRST* Marketplace
BOR_PO_APPROVE	Enables the Buyer to approve Purchase Orders.
BOR_PO_BUYER_APPR	Enables Purchase order workflow to route purchase orders to this buyer.

Buyer Setup

Much like a Requester must be set up in the system, you must also set up your Buyers in the system after you have added their Security roles. After setting up a user as a Buyer, you will then be able to add user preferences.

How To: Set Up a Buyer

1. In the menu, select **Set Up Financials/Supply Chain**.
2. Select **Product Related**.
3. Select **Procurement Options**.

4. Select **Purchasing**.
5. Select **Buyer Setup**.
6. Select the **Add a New Value** tab.
7. Enter the **buyer's User ID** in the **Buyer** field.
8. Click the **Add** button.
9. Ensure the status is set to **Active**.
10. In the **Department** SetID field, enter/select your institution's SetID.
11. If the Buyer only processes transactions for one department, you can enter/select that department in the Department field. However, if the Buyer processes transactions for multiple departments, leave this field blank.
12. In the **ShipTo SetID** field, enter/select your institution's **SetID**.
13. In the **ShipTo** field, enter/select this Buyer's default **Ship To location**.
14. In the **Location SetID** field, enter/select your institution's **SetID**.
15. In the **Location** field, enter/select this Buyer's primary **location**.
16. In the **PO Origin SetID** field, enter/select **SHARE**.
17. In the **Origin** field, enter/select **ONL**.
18. If desired, enter a phone and fax number.
19. Set the **Default PO Status** to **Pending Approval/Approved**.
20. Click the **Save** button.

Note: If the Buyer will also be creating Requisitions, they must be set up on the Requester Setup Page also. See ePro section above.

Receiving can be configured to do Not receive, optional or required. Users can take advantage of desktop receiving or use the traditional way of central receiving. The user role for Receiving through Purchasing is BOR_PO_RECEIVING. If a user wants to use desktop receiving, they must have the BOR_PO_RECV_EPRO role.

Vendors went to Suppliers in 9.2 and with the upgrade, ITS reduced the number of roles associated with Supplier activity and controlled it more using user preferences. Now there are only two user roles, BOR_PO_VENDORS_APPROVE and BOR_PO_VENDORS_MAINT. Security administrators can control what actions the user takes on the supplier, by user preferences. For instance, if you want a user to be able to modify an exisiting supplier, but not add a supplier, they would get the BOR_PO_VENDORS_MAINT role, but not the add user preference. See more detail in the user preferences section above.

In 9.2, Purchasing workflow changed from using route controls to using the Approval Framework. BOR_PO_BUD_REF_APPR role - This is approval role for Purchase Orders with Budget Reference differences. BOR_PO_ASSET_APPR role - This is approval role for Purchase Orders with Asset Issues. BOR_PO_ADMINXX (first two digits of institution id) -This role is for escalations or routing issues. Keep in mind that these three roles above are used only to route transactions to users. They do not contain page access. An approver will also have to have the BOR_PO_APPROVE role to approve a purchase

order at any of the above levels. This role gives them the page access needed to get to the purchase order to approve it. See Workflow Stage Docs in Appendix B.

Activity 7:

Login **to F92PLAY.gafirst.usg.edu** with your fprod user id and password.

Create a New **Buyer User id**, with the roles listed above in this section.

Navigate to **Product Related, Procurement Options, Purchasing, Buyer Setup** and set them up as a buyer for your business unit.

Then Navigate to **User Preferences** and add their user id under the buyer box **on Procurement User Preferences** an give them full authority for all buyers as well as the approval User preference.

Commitment Control

Control enables you to control expenditures actively against predefined, authorized budgets. In particular, Commitment Control enables you to:

- Create and maintain control budgets.

- Check actual transactions (such as actual expenditures and revenues) against control budgets.

- Check imminent future financial obligations (pre-encumbrances and encumbrances) against control budgets.

- Check recognized revenue against revenue estimate budgets.

When you set up control budgets, you associate them with a particular General Ledger business unit. You also define the kinds of transactions you are to check against your control budgets. Once your budgets are established, you check these transactions against your budgets, the passing or failing of the transactions depending on the remaining available budget amount and the degree of budgetary control you set up for your budgets.

Depending on how you set up Commitment Control security, users can adjust a transaction that fails budget checking or adjust the budgets that the transaction failed against and budget-check the transaction again. Also, if you grant users the authority, users can override budget checking and allow a transaction to exceed the budget.

Also with 9.2, ITS implemented an optional Workflow for Commitment Control Budget Journals. Institutions wishing to implement this workflow would need to give their approvers the BOR_KK_BUD_APPR role. Also, someone at the institution would need the BOR_KK_ADMINXX role. (first two digits of institution id) -This role is for escalations or routing issues.

With the upgrade to 9.2, ITS renamed several roles to make them more intuitive. The Commitment Control Budget Security rules are defined in this section. To get to them, you need the BOR_KK_SETUP

role. Once the rules are established on a user id, the request build process has to be run, in order for the changes to take effect, and the BOR_KK_PROCESSES role contains access to this process.

Commitment Control, then select Define Budget Security, then select Assign Rule to User ID, then select Assign Commitment Control Security Rule to User ID. ** A user must be tied to an employee id to be selected on this page. Below are the available rules. They are broken out by module. Budget Date Override by Module, Budget Override by Module, Bypass Budget, and the two new ones with 9.2 are BUD_ENTRY(enter budget journals) and BUD_XFER(enter budget transfers only). If a user needs to be able to enter both Budget Journals and budget transfers, they would need BOTH security rules.

Security Rule	Security Rule Attribute	Regular/Dynamic Rule	Description
BUDG_DT_AP	Super User	Regular	Upgrade rule for Budget Date security
BUDG_DT_AR	Super User	Regular	Upgrade rule for Budget Date security
BUDG_DT_BI	Super User	Regular	Upgrade rule for Budget Date security
BUDG_DT_EX	Super User	Regular	Budget Date Expenses
BUDG_DT_GL	Super User	Regular	Upgrade rule for Budget Date security
BUDG_DT_PO	Super User	Regular	Upgrade rule for Budget Date security
BUDG_DT_RQ	Super User	Regular	Upgrade rule for Budget Date security
BUD_ENTRY	Super User	Regular	Restrict budget entry to a limit set of users
BUD_XFER	Super User	Regular	Restrict budget transfers to a limit set of users
BYPASS_BD	Super User	Regular	BYPASS BUDGET
OVRD_AP	Super User	Regular	Upgrade rule for Budget Override Security
OVRD_AR	Super User	Regular	Upgrade rule for Budget Override Security
OVRD_BU	Super User	Regular	Upgrade rule for Budget Override Security
OVRD_EX	Super User	Regular	Override Expenses
OVRD_GL	Super User	Regular	Upgrade rule for Budget Override Security
OVRD_PO	Super User	Regular	Upgrade rule for Budget Override Security
OVRD_RQ	Super User	Regular	Upgrade rule for Budget Override Security

Activity 8:

Login to F92PLAY.gafirst.usg.edu with your fprod user id and password.

Use the Buyer User id you created above. **** Use Activity 1 user id instead

Navigate to Commitment Control, Define budget Security, assign rule to user id:

Give them the BUDG_DT_PO, BUDG_DT_RQ, OVRD_PO and OVRD_RQ rules.

Then you must run the _____ process.

General Ledger

The **General Ledger** is the heart of an organization's financial system as it is the central repository for accounting activity. Organizations record their business activity through journal entries (or through

subsystem accounting entries, such as Payables), which are posted to the general ledger using a collection of accounts, departments and so on. This collection of accounts is often referred to as a chart of accounts, which enables companies to classify financial (and statistical) data that is used for analyzing and reporting worth and profitability.

Journal entries for actual transactions are made in a double entry system, in accordance with Generally Accepted Accounting Principles (GAAP), where debits equal credits.

The true test of a general ledger system is in the way it accepts and processes these journal entries. PeopleSoft General Ledger provides journal entry formats that enable you to enter any type of transaction quickly and easily without losing the control you need to ensure accuracy.

PeopleSoft General Ledger also includes other aspects, such as allocating shared assets and expenses, maintaining budgets, and reporting.

In 9.2, ITS updated Workflow for General Ledger Journals, so that it could take advantage of the new approval process instead of using route controls.   Institutions would need to give their approvers the BOR_GL_JRNL_APPR role. Also, someone at the institution would need the BOR_GL_ADMINXX role. (first two digits of institution id) -This role is for escalations or routing issues.

If your General Ledger Users want to take advantage of the new dashboard/workcenter features, they will need the BOR_GL_DASHBOARD role, the BOR_GL_WORKCENTER role and the BOR_WORKCENTER_USER role.

Other General Ledger considerations includes User preferences as mentioned in the User Preference Section. Don't forget to check user's commitment control rules for GL. If your user needs to override a Budget Date or a Budget Exception error on a Journal, they will need OVRD_GL and/or BUDG_DT_GL commitment control rules. It is located under Commitment Control, Define Budget Security, Assign rule to a User. See Commitment Control Section above. And, don't forget to run the request build process after assigning the rules to the user, or the change will not take effect. (IF you forget to run the request build process, the BORBATCH process that runs every night will run it for you.)

The general ledger module contains security for Year ends processes and reports, TIGA Processing, Chartfield Configuration, and journal entry/processing.

Accounts Receivable

PeopleSoft Receivables enables you to:

 • Enter and track all of your receivables.

• Receive and apply payments.

• Manage outstanding receivables enabling your organization to collect money quickly

Currently only USO is using this module. There are seven security roles for this module, and a few user preferences, but no workflow options as delivered by ITS.

Budget Prep

Each year, the USG institutions complete the development of their proposed budgets for the upcoming fiscal year. This process includes the budgeting of personal services, fringe benefits, and non-personal services. The process should conclude with the reconciliation of the budget to the final allocation by the Regents and the preparation of summary schedules identified by the Regents. This reconciliation process should utilize queries and reports in the financial system.

The Budget Prep Module is used to develop this budget by extracting all budget related information from the PS Financials module. It then loads personal Services information from the ADP EV5 data file (epoh009.txt). Within the Budget Prep Module itself, users can manipulate the data. And when finished, Budget Prep exports the new budget information back to ADP and PeopleSoft Financials.

There are 6 different security roles for Budget Prep. They all Start with BOR_BP, and include inquiry and reporting, processing, setup pages, updates and grants.

Common Remitter/BOR Payroll/Benefits Recon

Common Remitter Module

Common Remitter in PS Financials provides a single source solution for the collection, reconcilement and remittance of Retirement and Tax Sheltered Annunity payroll deductions. The functionality of the Common Remitter reporting provides data required for monthly, quarterly and annual reporting required for Retirement and Tax Sheltered Annunities for all Board of Regents approved providers. The process is a joint effort of the individual Business Units, Shared Services and Information Technology Services**.**

For Common Remitter, the user role needed is BOR_CR_USER.

BOR Payroll Module

BOR Payroll in PS Financials house the functionality for users further process payroll data from the source payroll system. Processes include but not limited to TIGA reporting of salaries, Year End payroll accurals, Payroll Interfaces for payroll actuals, encumbrances, pay distribution codes, project and department, zero personal services and a data purge process. The online reporting functionality provides an array of online queries readily available for institutional reference and reconcilement.

For BOR Payroll: Only the following roles should be used for role assignment. The Security Administrator should only assign roles for General Ledger (GL) based upon the employee's job duties and audit consideration for separation of duties.

Role Name	Description	Comments
BOR PeopleSoft User	FN Base PeopleSoft User	**Each user MUST have a base**
BOR PeopleSoft User-no exp	BOR PeopleSoft User-no exp	**Each user MUST have a base**
BOR PeopleSoft User –No Tauth	Base role without travel	**Each user MUST have a base**
BOR_ADP_PAYROLL_FYE_REPORT	ADP Payroll Year End Reporting	**This role allows access to the BOR Payroll data for FYE reports**
BOR_GL_FN_UTILITY	Utility Processes	**This role allows users to run the 3rd Party Purge process.**
BOR_GL_JOURNAL_ENTRY BOR_GL_JOURNAL_PROCESSING	Process Jrnls-Maintain	**This role limits users to the Edit, Submit and Post processes. This role is necessary for users performing journal entry.**
BOR_GL_JRNL_APPR	Journal Approval	**This role allows users to approve journals submitted and will appear in the approvers Workflow list. The approver role may also Post journals after approving the journal entry.**
BOR_GL_JOURNAL_GENERATION	Journal Generator Process	**This role allows users to journal generate GL entries.**
BOR_GL_PAY_INTERFACE	Payroll GL Budget Validation	**This role allows users to complete Payroll interface and budget validations**
BOR_GL_PROCESSING	BOR GL Processing	**This role allows access to the BOR Payroll Processes and Inquiry related menus**
BOR_GL_TIGA_PROCESSING	Tiga Processing	**This role allows users to process data for the Transparency in Government Act.**
BOR_QRY_SENSDATA	Query Sensitive Data	**This role allows access to employee sensitive data included in queries and reports.**

Benefit Reconciliation Module

Benefit Reconciliation in PS Financials includes the creation of accounting entries, reconcilement tools and reporting data for active and retired employees with benefits. The Benefit Reconciliation module also provides tools for monitoring cobra participants and employees on leave of absence. The functionality of Benefits Reconciliation serves as a source for monthly, quarterly and annual reporting.

For Benefits Recon: Only the following roles should be used for role assignment. The Security Administrator should only assign roles for General Ledger (GL) based upon the employee's job duties and audit consideration for separation of duties.

Role Name	Description	Comments
BOR PeopleSoft User	FN Base PeopleSoft User	**Each user MUST have a base**
BOR PeopleSoft User-no exp	BOR PeopleSoft User-no exp	**Each user MUST have a base**
BOR PeopleSoft User –No Tauth	Base role without travel auths	**Each user MUST have a base**
BOR_ADP_PAYROLL_ADJ	Payroll Adjustments	**This role allows users to enter Payroll Adjustment journal**
BOR_ADP_RET_BEN_ACCTG	Retirement Benefits Accounting	**This role allows access to the users to run the retirement Benefit accounting processes**
BOR_ADP_SUPP_PDR	Supplemental PDR	**This role allows users to run SUPPDR accounting processes**
BOR_GL_ADP_REPORT	Benefit Payment/Accrual Recon	**This role allows users to run Reconcilement processes and Reports**
BOR_GL_JOURNAL_ENTRY BOR_GL_JOURNAL_PROCESSING	Process Jrnls-Maintain	**This role limits users to the Edit, Submit and Post processes. This role is necessary for users performing journal entry.**
BOR_GL_JRNL_APPR	Journal Approval	**This role allows users to Approve journals submitted and will appear in the approvers Workflow list. The approver role may also Post journals after approving the journal entry.**
BOR_GL_JOURNAL_GENERATION	Journal Generator Process	**This role allows users to journal generate GL entries.**
BOR_GL_PAY_INTERFACE	Payroll GL Budget Validation	**This role allows users to complete Payroll interface and budget Validations**
BOR_Reconciliation_User	BOR Reconciliation User	**This role allows access to the BOR Reconciliation Processes and Inquiry related menus.**
BOR_QRY_SENSDATA	Query Sensitive Data	**This role allows access to employee sensitive data included in queries and reports.**

Reminder, each individual may have different job duties. The above is meant for recommendation only. Adjust security to meet the individual's job responsibility without introducing segregation of duties issues.

Workflow Management

Many of the daily tasks that you perform are part of larger tasks that involve several steps and several people working together.

For example, when you enter an invoice, you are initiating an approval and payment process: someone else reviews and approves it, and a third person submits payment to the vendor. The term *workflow* refers to this larger process.

Workflow approval enables transactions that are initiated by End Users, to be routed through the system to pre-defined Approvers. Each of the Approvers are assigned to a specific workflow approval level. As the transaction is passed through each workflow approval level, the Approver is responsible for verifying the information on the transaction.

The actions available to an approver through AF include approve, deny, hold and push pack. Transactions can be approved at the header level, line level, or a combination of the two. All required approvers must approve the transaction to make the status approved. A denied transaction sends the transaction back to the user who submitted it into workflow. For example, if a requisition is denied, it will be sent back to the requester.

Putting a transaction on hold gives the approver time to gather additional information before making the choice to approve or deny and gives others visibility into why a transaction is taking longer than anticipated to flow through workflow. Push back functionality allows the approver to send the transaction back to the prior approver for additional review. For example, if the approver learned of additional information that they believe the first approver was unaware of, they could send the transaction back.

Example of approval level
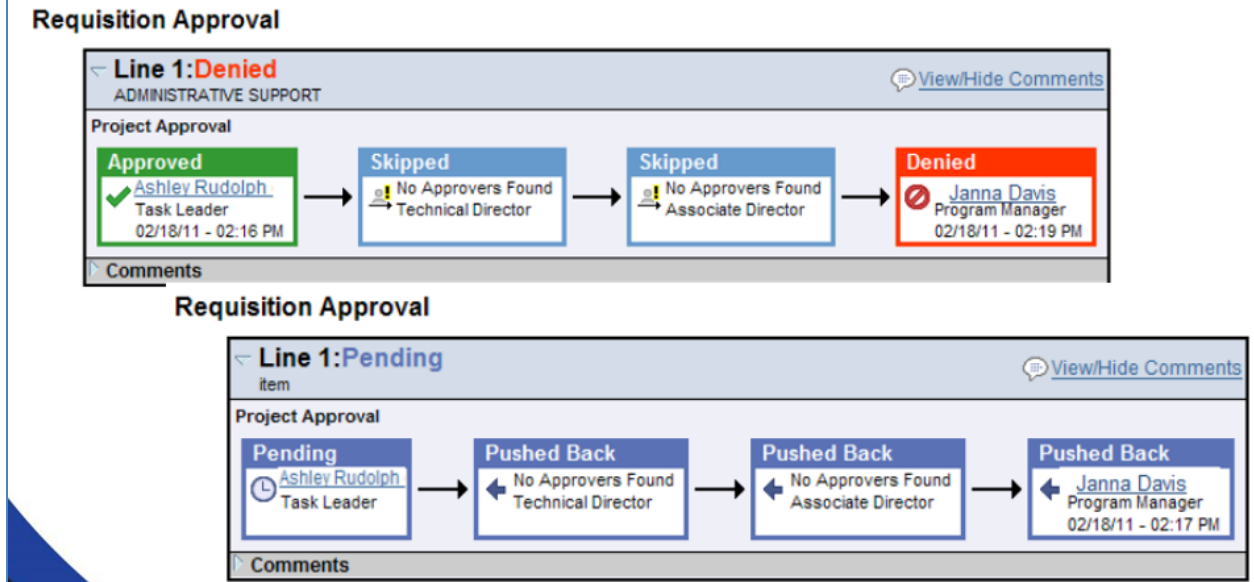
Workflow Admin

Each Institution needs one or more Workflow Administrators. They are responsible for Routing Management and Transaction Rerouting. Transactions missing approver assignments or transactions that have escalated due to no approvals will need to be redirected to the appropriate approvers by the administrator. Escalation and Notification Days by configured by Module and can be institution specific.

Each institution must determine the amount of days for workflow to notify the approver that they have not approved the transaction, and the number of days before it escalates the transaction to the Workflow Admin.

Approval Roles vs. Routing Roles

This was discussed in the above section covering roles, however it is important to mention it here again as well. There are many types of roles. When It comes to workflow and approvals, approvers will need several different type of roles. An Approval role, i.e. BOR_EP_REQ_APPROVE, contains the pages in the system where the approver would go to approve the transaction. However, workflow needs to know who to route the transactions to. There are several ways to configure this. One way to route a transaction is by role. This role, i.e. BOR_ASSET_APPR, has no page access, no permissions. It is only used by workflow, for routing purposes. Other ways to route transactions is by query, by sql, by employee id and for expenses, by user id.

Security Administration

Security administration is distributed out to each institution, and it is their responsibility to administer it, update it and maintain it. This is done through role grant and the distributed user profiles. Since ITS creates the roles and permissions, each institutional security administrator has to have a security role that allows them access to the delivered roles. This role is BOR_LOCAL_SEC_ADMIN. This role contains all the delivered roles that are not institution specific. In addition, for institution specific roles such as BOR_EP_ADMINXX, BOR_PO_ADMINXX, etc, the administrator also needs BOR_LOCAL_SEC_ADMINXX where the XX is the first two digits of the institution id.

The core job functions of the security administrator at the campus level include, but are not limited to:
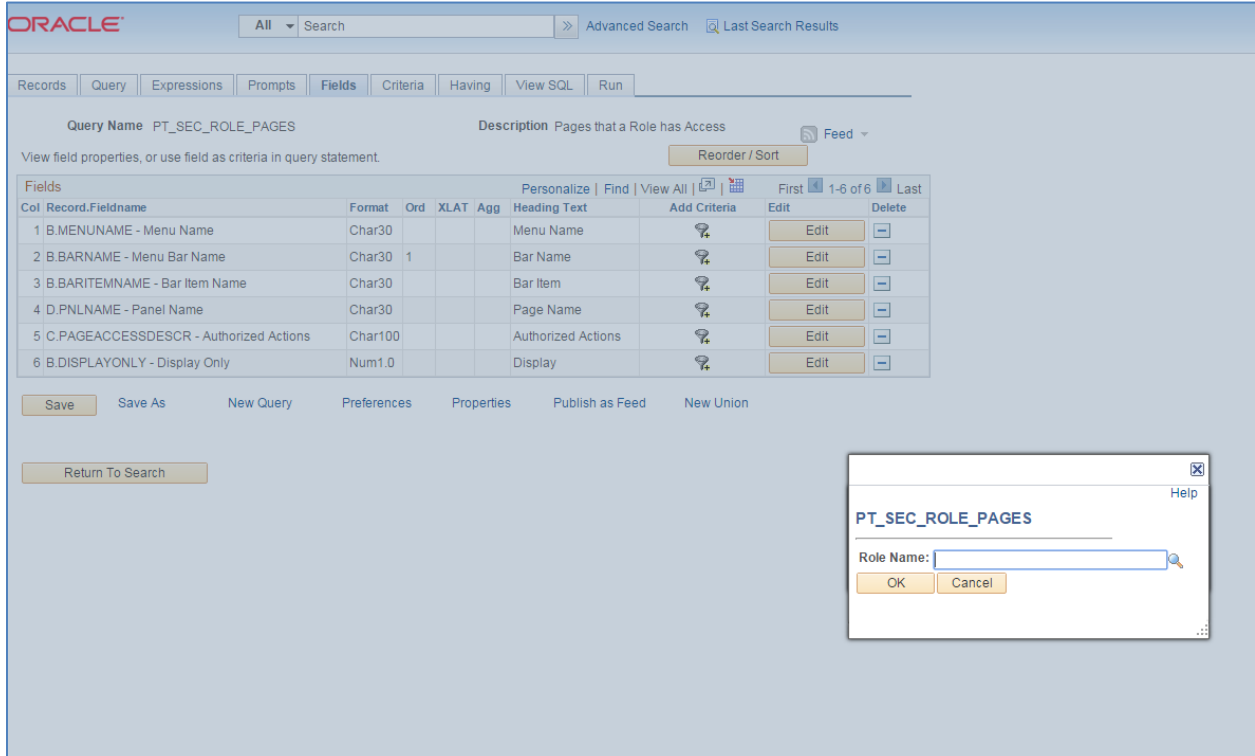
- User Profile Management

    – Core Security Roles Management

    – EMPLID Management

    – Email Address Management

    – Password Reset

    – Account Lock Out / Reset

    – Commitment Control Security

    – User Preferences

    – Approval Setup

- Security Monitoring (will be covered more in the IT Audit section below)

    – New Users

    – Terminated Users

    – Position Changes

Determining Access

One of the most difficult tasks for the security administrators is determining what access and what level of access an end user needs. This can vary by institution. There are hundreds of roles, and many other different aspects of security, so what is the best way for each administrator to determine access. Let's talk about a few different Tools that can be used to determine first of all, what access a role has, and second of all, what access is needed by individual.

Tools and Queries

There are a few tools and queries that can be used to help identify what access a role contains. Let's begin by talking about the PT_SEC_ROLE_PAGES. This query is run by role.

Role Name = BOR_AP_INQUIRY

View All | Rerun Query | Download to Excel | Download to XML

	Menu Name	Bar Name	Bar Item	Page Name	Authorized Actions	Display
1	CREATE_PAYMENTS	INQUIRE	MTRC_AP_PYCYCL	MTRC_AP_PYCYCL	Update/Display	0
2	CREATE_PAYMENTS	INQUIRE	PYCYCL_DATA_INQ	PYCYCL_DATA_INQ	Update/Display	0
3	CREATE_PAYMENTS	INQUIRE	PYCYCL_DATA_SUM	PYCYCL_DATA_SUM	Update/Display	0
4	CREATE_PAYMENTS	INQUIRE	PYMNT_INQ_SRCH	PYMNT_INQ_SRCH	Update/Display	0
5	CREATE_PAYMENTS	INQUIRE	PYMNT_VCHR_DETAIL	PYMNT_VCHR_DET_SEC	Update/Display	0
6	CREATE_PAYMENTS	INQUIRE	REPLACED_PAYMENTS	PYMNT_RPLCD	Update/Display	0
7	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_GL_DRILL	AP_GL_DRILL	Update/Display	0
8	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_INQ_SEARCH	AP_INQ_SEARCH_DEFN	Update/Display	0
9	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_EXCPTN	AP_MTCH_WB_EXCPTN	Update/Display	0
10	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_EXCPTN	AP_WB_HEADER_EXPTN	Update/Display	0
11	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_MOVRD	AP_MTCH_WB_MOVRD	Update/Display	0
12	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_OVRD	AP_MTCH_WB_OVRD	Update/Display	0
13	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_SUCCESS	AP_MTCH_WB_SUCCESS	Add Update/Display	0
14	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_SEARCH_CRIT	AP_SRCH_CRIT_DEFN	Add Update/Display	0
15	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_VCHR_INQ	AP_VOUCHER_INQUIRY	Update/Display	0
16	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_VCHR_MTCH_INQ	AP_VCHR_MATCH_INQ	Add Update/Display	0
17	ENTER_VOUCHER_INFORMATION	INQUIRE	DOC_TOL_EXCPT	DOC_TOL_EXCPT	Update/Display	0
18	ENTER_VOUCHER_INFORMATION	INQUIRE	DOC_TOL_OVR_LOG	DOC_TOL_OVR_LOG	Update/Display	0
19	ENTER_VOUCHER_INFORMATION	INQUIRE	PO_INQUIRY	PO_INQUIRY	Update/Display	0
20	ENTER_VOUCHER_INFORMATION	INQUIRE	VCHR_ACCTG_UNBAL	VCHR_ACCTG_UNBAL	Update/Display	0
21	ENTER_VOUCHER_INFORMATION	INQUIRE	VCHR_LINE_DSP	AP_VCHR_LN_DET_DSP	Update/Display	0
22	ENTER_VOUCHER_INFORMATION	INQUIRE	VCHR_PYMNT_INQ	VCHR_PYMNT_INQ	Update/Display	0
23	ENTER_VOUCHER_INFORMATION	INQUIRE	VOUCHER_ACCOUNTING_ENTRIES	VCHR_ACTG_ENTRIES	Update/Display	0
24	ENTER_VOUCHER_INFORMATION	INQUIRE	VOUCHER_EDIT_ERROR_DETAIL	VCHR_BATCHERR_PG	Update/Display	0
25	MANAGE_COMMITMENT_CONTROL	INQUIRE	KK_XCP_AP1	KK_XCP_HDR_AP1	Update/Display	0

It returns menu names, down to page names. Sometimes this is still hard to distinguish what the Page actually is.

So let's look at BOR_PORTAL_PERMISSIONS:

Records | Query | Expressions | Prompts | Fields | Criteria | Having | View SQL | **Run**

Role Name = BOR_AP_INQUIRY

View All | Rerun Query | Download to Excel | Download to XML   First ◄ 1-100 of 210 ► Last

	Role Name	PortlObjNm	PortlLabel	Menu Name	Bar Name	Bar Item	Panel Item	Component
1	BOR_AP_INQUIRY	EP_F_PYCYCL_DATA_INQ_GBL	Detail Data	CREATE_PAYMENTS	INQUIRE	PYCYCL_DATA_INQ	PYCYCL_DATA_INQ	PYCYCL_DATA_INQ
2	BOR_AP_INQUIRY	EP_F_PYCYCL_DATA_SUM_GBL	Summary Data	CREATE_PAYMENTS	INQUIRE	PYCYCL_DATA_SUM	PYCYCL_DATA_SUM	PYCYCL_DATA_SUM
3	BOR_AP_INQUIRY	EP_PYMNT_VCHR_DET_GBL	Payment Voucher Detail	CREATE_PAYMENTS	INQUIRE	PYMNT_VCHR_DETAIL	PYMNT_VCHR_DET_SEC	PYMNT_VCHR_DET
4	BOR_AP_INQUIRY	EP_PYMNT_INQ_SRCH_GBL	Payment	CREATE_PAYMENTS	INQUIRE	PYMNT_INQ_SRCH	PYMNT_INQ_SRCH	PYMNT_INQ_SRCH
5	BOR_AP_INQUIRY	EP_PYMNT_RPLCD_GBL	Replaced Payments	CREATE_PAYMENTS	INQUIRE	REPLACED_PAYMENTS	REPLACED_PAYMENTS	PYMNT_RPLCD
6	BOR_AP_INQUIRY	EP_MTRC_AP_PYCYCL_GBL	Summary Metric	CREATE_PAYMENTS	INQUIRE	MTRC_AP_PYCYCL	MTRC_AP_PYCYCL	MTRC_AP_PYCYCL
7	BOR_AP_INQUIRY	EP_AP_GL_DRILL_GBL	Journal Drill Down	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_GL_DRILL	AP_GL_DRILL	AP_GL_DRILL
8	BOR_AP_INQUIRY	EP_VCHR_PYMNT_INQ_GBL	Voucher Payments	ENTER_VOUCHER_INFORMATION	INQUIRE	VCHR_PYMNT_INQ	VCHR_PYMNT_INQ	VCHR_PYMNT_INQ
9	BOR_AP_INQUIRY	EP_AP_MTCH_WB_EXCPTN	Match Workbench Exception	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_EXCPTN	AP_MTCH_WB_EXCPTN	AP_MTCH_WB_EXCPTN
10	BOR_AP_INQUIRY	EP_AP_MTCH_WB_EXCPTN	Match Workbench Exception	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_EXCPTN	AP_WB_HEADER_EXPTN	AP_MTCH_WB_EXCPTN
11	BOR_AP_INQUIRY	EP_AP_MTCH_WB_MOVRD	Matched Overridden	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_MOVRD	AP_MTCH_WB_MOVRD	AP_MTCH_WB_MOVRD
12	BOR_AP_INQUIRY	EP_AP_MTCH_WB_OVRD	Match Workbench Overridden	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_OVRD	AP_MTCH_WB_OVRD	AP_MTCH_WB_OVRD
13	BOR_AP_INQUIRY	EP_AP_MTCH_WB_SUCCESS	Match Workbench Success	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_SUCCESS	AP_MTCH_WB_SUCCESS	AP_MTCH_WB_SUCCESS
14	BOR_AP_INQUIRY	EP_AP_SRCH_CRIT_GBL	AP Search Criteria	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_SEARCH_CRIT	AP_SRCH_CRIT_DEFN	AP_SRCH_CRIT
15	BOR_AP_INQUIRY	EP_AP_VCHR_INQ_GBL	Voucher	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_VCHR_INQ	AP_VOUCHER_INQUIRY	AP_VCHR_INQ
16	BOR_AP_INQUIRY	EP_AP_VCHR_MATCH_INQ	Supplier Match Metrics	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_VCHR_MTCH_INQ	AP_VCHR_MATCH_INQ	AP_VCHR_MATCH_INQ
17	BOR_AP_INQUIRY	EP_DOC_TOL_EXCPT_GBL	Document Tolerance Exceptions	ENTER_VOUCHER_INFORMATION	INQUIRE	DOC_TOL_EXCPT	DOC_TOL_EXCPT	DOC_TOL_EXCPT
18	BOR_AP_INQUIRY	EP_DOC_TOL_OVR_LOG	Document Tolerance Override	ENTER_VOUCHER_INFORMATION	INQUIRE	DOC_TOL_OVR_LOG	DOC_TOL_OVR_LOG	DOC_TOL_OVR_LOG
19	BOR_AP_INQUIRY	EP_GRP_AP_CTL_GBL	Group Information	ENTER_VOUCHER_INFORMATION	USE	GROUP_INFORMATION	VOUCHERING_OPTIONS_1	GRP_AP_CTL
20	BOR_AP_INQUIRY	EP_GRP_AP_CTL_GBL	Group Information	ENTER_VOUCHER_INFORMATION	USE	GROUP_INFORMATION	TOTAL_AND_ASSIGNMENT_ENTRY	GRP_AP_CTL
21	BOR_AP_INQUIRY	EP_GRP_AP_CTL_GBL	Group Information	ENTER_VOUCHER_INFORMATION	USE	GROUP_INFORMATION	TAX_OPTIONS	GRP_AP_CTL
22	BOR_AP_INQUIRY	EP_GRP_AP_CTL_GBL	Group Information	ENTER_VOUCHER_INFORMATION	USE	GROUP_INFORMATION	ACCOUNTING_OPTIONS	GRP_AP_CTL
23	BOR_AP_INQUIRY	EP_GRP_AP_CTL_GBL	Group Information	ENTER_VOUCHER_INFORMATION	USE	GROUP_INFORMATION	VOUCHERS	GRP_AP_CTL
24	BOR_AP_INQUIRY	EP_PO_INQUIRY_COM_GBL	Purchase	ENTER_VOUCHER_INFORMATION	INQUIRE	PO_INQUIRY	PO_INQUIRY	PO_INQUIRY_COM

As you can see above it contains the Portal Label which is much more intuitive.

These two queries are helpful if you want to see by a specific role. This query could be modified to remove the role prompt, and add run for all delivered roles.

Another tool that can be used is the Security Matrix for 9.2 that is on our website:

CLASSID	MENUNAME	BARNAME	BARITEMNAME	PNLNAME	PAGEACCESSDESCR	DISPLA
BOR_AP_INQUIRY	AP_CRTE_PMNTS_INQ	CREATE_PAYMENTS	INQUIRE	MTRC_AP_PYCYCL	MTRC_AP_PYCYCL	Update/Display	0
BOR_AP_INQUIRY	AP_CRTE_PMNTS_INQ	CREATE_PAYMENTS	INQUIRE	PYCYCL_DATA_INQ	PYCYCL_DATA_INQ	Update/Display	0
BOR_AP_INQUIRY	AP_CRTE_PMNTS_INQ	CREATE_PAYMENTS	INQUIRE	PYCYCL_DATA_SUM	PYCYCL_DATA_SUM	Update/Display	0
BOR_AP_INQUIRY	AP_CRTE_PMNTS_INQ	CREATE_PAYMENTS	INQUIRE	PYMNT_INQ_SRCH	PYMNT_INQ_SRCH	Update/Display	0
BOR_AP_INQUIRY	AP_CRTE_PMNTS_INQ	CREATE_PAYMENTS	INQUIRE	PYMNT_VCHR_DETAIL	PYMNT_VCHR_DET_SEC	Update/Display	0
BOR_AP_INQUIRY	AP_CRTE_PMNTS_INQ	CREATE_PAYMENTS	INQUIRE	REPLACED_PAYMENTS	PYMNT_RPLCD	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_GL_DRILL	AP_GL_DRILL	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_INQ_SEARCH	AP_INQ_SEARCH_DEFN	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_EXCPTN	AP_MTCH_WB_EXCPTN	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_EXCPTN	AP_WB_HEADER_EXPTN	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_MOVRD	AP_MTCH_WB_MOVRD	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_OVRD	AP_MTCH_WB_OVRD	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_MTCH_WB_SUCCESS	AP_MTCH_WB_SUCCESS	Add Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_SEARCH_CRIT	AP_SRCH_CRIT_DEFN	Add Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_VCHR_INQ	AP_VOUCHER_INQUIRY	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	AP_VCHR_MTCH_INQ	AP_VCHR_MATCH_INQ	Add Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	DOC_TOL_EXCPT	DOC_TOL_EXCPT	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	DOC_TOL_OVR_LOG	DOC_TOL_OVR_LOG	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	PO_INQUIRY	PO_INQUIRY	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	VCHR_ACCTG_UNBAL	VCHR_ACCTG_UNBAL	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	VCHR_LINE_DSP	AP_VCHR_LN_DET_DSP	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	VCHR_PYMNT_INQ	VCHR_PYMNT_INQ	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	VOUCHER_ACCOUNTING_ENTRIES	VCHR_ACTG_ENTRIES	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	INQUIRE	VOUCHER_EDIT_ERROR_DETAIL	VCHR_BATCHERR_PG	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	UNMATCH_WRK	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_CORRECTION	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_ERRORSMMRY_PG	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_EXPRESS1	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_LINE_MISC_CHG	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_LINE_PO_WRK	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_LINE_RECV_WRK	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_LOOKUP_MTCH	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_LOOKUP_MTCH2	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_MAIN2_WRK	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_PAYMENT_PNL	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_RECV_MTCH	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_REG_WRK_LC	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_STATUS_IA	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_SUMMARY_PG	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_TEMPLATE	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_TERMS_EXP	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_VNDR_INFO	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_WTHD_ERR	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VCHR_WTHD_EXP	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VNDR_LOOKUP_WRK	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VNDR_LOOKUP_WRK1	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	ENTER_VOUCHER_INFORMATION	USE	EXPRESS_VOUCHER	VOUCHER_WRK_MTCH	Update/Display	1
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	PROCUREMENT_ANALYSIS	INQUIRE	PO_DOC_STATUS	PRCR_DOCSTAT_INQ	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	PROCUREMENT_ANALYSIS	INQUIRE	PO_DOC_STATUS	PRCR_DS_PO_WRK	Update/Display	0
BOR_AP_INQUIRY	AP_ENTER_VCHR_INFO_INQ	PROCUREMENT_ANALYSIS	INQUIRE	VOU_DOCSTAT_INQ	PRCR_DOCSTAT_VCHR	Update/Display	0
BOR_AP_INQUIRY	AP_MNG_COMMIT_CNTRL_INQ	MANAGE_COMMITMENT_CONTROL	INQUIRE	KK_XCP_AP1	KK_XCP_HDR_AP1	Update/Display	0

Also, as part of fit gap, there were spreadsheets by module, that was sent out that contained business processes by module and what 9.2 security role was associated with those business processes:

Business process	Current 8.9 Role(s)	Fit Gap Recommended Role	9.2 Role	Comments
AP.050.020 Viewing and Correcting Document Tolerance Exceptions	BOR_AP_INQUIRY	AP Inquiry	BOR_AP_INQUIRY	
AP.060.010 Reviewing Voucher Information	BOR_AP_INQUIRY	AP inquiry	BOR_AP_INQUIRY	
AP.060.020 Reviewing Posted Accounting Entries	BOR_AP_INQUIRY	AP inquiry	BOR_AP_INQUIRY	
AP.060.040 Reviewing Journal Detail for a GL Journal	BOR_AP_INQUIRY	AP inquiry	BOR_AP_INQUIRY	
AP.060.050 Reviewing Voucher Document Status	BOR_AP_INQUIRY	AP inquiry	BOR_AP_INQUIRY	
AP.060.060 Performing Payment Inquiries	BOR_AP_INQUIRY	AP inquiry	BOR_AP_INQUIRY	
AP.060.070 Reviewing Vendor Aging	BOR_AP_INQUIRY	AP inquiry	BOR_AP_INQUIRY	
AP.060.080 Reviewing Scheduled Payments on Hold	BOR_AP_INQUIRY	AP inquiry	BOR_AP_INQUIRY	
AP.060.090 Reviewing Scheduled Payment Information	BOR_AP_INQUIRY	AP inquiry	BOR_AP_INQUIRY	
AP.060.100 Reviewing Current Vendor Balances	BOR_AP_INQUIRY	AP inquiry	BOR_AP_INQUIRY	
AP.050.030 - View and Correct Voucher Build Errors	BOR_AP_INQUIRY, BOR_AP_VOUCHER_ENTRY, BOR_AP_QUICK_INV, BOR_AP_VOUCHER_BUILD	AP Inquiry/Voucher Entry	BOR_AP_INQUIRY, BOR_AP_VOUCHER_ENTRY	
AP.020.506 Pay Cycle Approval	BOR_AP_PAYCYCLE_APPROVE	Payment Approval	BOR_AP_PAYCYCLE_APPROVE	
AP.070.005 APS8001 Voucher Activity Report	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.010 APY0000 List of Voucher Origins	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.015 APY0011 Business Unit Options	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.020 APY1010 Voucher Register	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.025 APY1011 Control Group Register	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.030 APY1020 Posted Voucher Listing	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.035 APY1090 Match Exception Report	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.045 APY1400 Summary AP/GL Open Liability Act Recon	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.050 APY1405 Detail AP/GL Open Liability Account Re	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.055 APY1406 Payables Open Liability Report	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.060 APY1408 Vendor Liability Aging Data Report	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.065 APY1410 AP/GL Journal Reconciliation Report	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.070 APY1420 AP/GL Account Reconciliation Report	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.075 BORRY002 Payment History by Vendor	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.080 APY2001 Detailed (Summary) Check Register	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.085 APY2004 Detail (Summary) Payment History by Bank	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.090 APY2030 Trial Payment Register	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.095 APY2040 Payment Forecast	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	
AP.070.100 APY2050 Payment Hist by Pymt Method (Dtl or Summary)	BOR_AP_REPORTS	AP Reports	BOR_AP_REPORTS	

Activity 9:

You have a request to add security to a user and this user needs to be able to enter a voucher.

 What role should you give them? _____

Are there any other considerations you need to look at for this user? If so list them here:

_____

You have another request for a user to be able to Run depreciation on an asset.

What role is required? _____

 Are there any other considerations you need to look at for this user? If so list them here:

_____

Institution-Specific Job Aids and Forms

As discuss before, one of the best ways to determine what access your employees need, is to create custom security job aids by job functions. I have included ITS's sample ones in Appendix A, however, not every institution is the same, or is the same size, so job functions will vary across institutions.   Look for common job titles at your institution between various departments. Then if the job duties are the same, or even maybe have a few exceptions, document the security for that job duty and note the exception roles and preferences. Then as new hires come along and are placed in those job functions, you will have the security assignments documented.

For instance, some institutions have a directory on their campus website. This directory lists each department and some of them provide names and job titles. So for instance, let's say your Budget Office has a Director, Assistant Director, and a Budget Analyst. Look at the job functions for each and determine what security requirements are needed and document them. It may be that the Director and Assistant Director need the same security, so only one job aid would be needed. If there is only a few roles, different, you could use the same job aid and note the differences. I would expect that the Budget Analyst would not need near as much security, therefore I would expect to see a different job aid.

Another example would be the Purchasing Department. For instance, if you have a Director, a senior buyer, a Buyer, and a Purchasing Staff, you could divide these up into different job aids.

The director probably needs the most supervisory access, so that may be one job aid. The senior buyer and the buyer most likely would be the same job aid and the Staff member would need even less

security, so they would be a separate job aid. This will help with Auditing purposes, documentation and ease of administration.

IT Audit

The security process for new hires and terminations should be handled on an "as needed" basis, as personnel are hired or terminated. Steps should be put in place to ensure that 1) accounts are being locked in a timely manner, 2) accounts are being setup with the appropriate access for new hires, and 3) the appropriate authorization has been provided and documented.

Each campus may have its own business process for handling each of these procedures; however, the procedures should be documented and followed. Procedural guidelines for setting up and terminating accounts are outlined below.

New Hires

1) Determine the level of access the individual needs and complete a security request form.
2) If the account is setup manually, set a generic password and set it to expire upon login.
3) Have the security request form authorized by two individuals, 1) the person requesting the user have access and 2) the security administrator.
4) Have the user sign the security request form.
5) Or you can have the user self-register or create his or her account manually.
6) Ensure that there is no segregation of duties issue.
7) Ensure you setup all roles, user preferences, budget security, etc.

Terminated Users

1) Terminations should be reviewed often, at least monthly, and users who have terminated should have their user account locked and base role removed.
2) Remove any workflow related roles.
3) Change the ID Type on the ID page to None instead of employee. Place the employee id on the General tab under user id alias field and attach the user id beside it. EMPLID-USERID.
4) Update the user's security request form to a "terminated" status and document the appropriate signatures.
5) If the user was a requester/buyer for ePro or Purchasing, go to his or her requester/buyer setup and inactivate it (only after all requisitions and purchase orders are complete that this person was responsible for).
6) For Approvers, go to the user profile > workflow tab and uncheck the worklist/email user checkbox. If the person was an expenses approver, remove them from the approver assignments pages. If the person was an ePro approver for a department or project, remove their employee id from the chartfield setup page.

7) If the person had budget security, remove the commitment control security rules and run the request build process.

Terminated User Query

Navigation: Reporting Tools > Query > Query Manager > BOR_SEC_TERMINATED_USERS

This query will return users in the PeopleSoft Financials system that have a user id that is not locked and has a termination row in the Job record.

	A	B	C	D	E	F	G	H	I
1	User	Description	ID	Status	Action	ACTN DATE	Unit	Short Descr	
2	testuser	last name, first name	0033XXX	T	TER	5/18/2011	98000	Unlocked	
3	sampleuser	last name, first name	0159XXX	T	TER	5/5/2011	98000	Unlocked	
4									

ITS strongly recommends that security administrators query PSOPRDEFN to ensure that the user is not a multi-campus user and that the termination row in PS_JOB is for their campus.

Also, query PS_JOB to ensure that the user is truly terminated. If so, the security administrators will need to lock the account and remove the base role. This query is meant to be a secondary tool for identifying terminated users. The primary tool would be the source HR system.

Activity 10:

Login to fplay using your prod user name and password.

Go to the Query Manager under Reporting Tools and run the BOR_TERMINATED_USERS_QUERY.

Then follow the procedures above if you have any results on the query. Just pick one user.

Current Users

When a user's job function changes, the security administrator will need to update the user's security request form, get authorization from the user's manager, and change his or her access within the PeopleSoft Financials system.

Security administrators are responsible for unlocking user accounts and resetting passwords if they expire.

Documentation and Approvals

Whether your institution requires a printed copy of a security request form, or you have an electronic system to track security requests and approvals, you must periodically review the requests and recertify the users. The main message here is that you cannot have a verbal request for security access with no backup documentation. It must have a signature or electronic approval that can be audited.

Monitoring

ITS recommends that every year, at least once a year, all user accounts that are setup at your institution are reviewed. The accounts should be reviewed for:

- level of access (too much or not enough),
- type of access (have they changed job functions), and
- need of access (do they still need access).

The person who reviews the security request forms should maintain signed documentation that the user accounts were reviewed.   These forms should be stored on top of the security request form on file for audit purposes or electronically.

This should include things such as Segregation of Duties review, User preferences review, budget security reviews.

Segregation of Duties Query

Navigation: Reporting Tools > Query > Query Manager > SEGREGATE_DUTY_BOR

This query is based on a Segregation of Duties (SOD) spreadsheet provided by the auditors.   It is based off of Process/Functions and role names that may be considered a segregation of duties issue.

If a user appears on this query, it does not necessarily mean they are in violation. However, further research should be completed by the security administrator on the campus to ensure it is not a violation and annotate the research for the auditors. If it is a violation, the security administrators should work with the Business Office to determine what access to remove from the user.

Process	COSO	Procedure/Function	Grp	Create Requisition 1	Approve Requisition 2	Create PO 3	Approve PO 4	Create Voucher 5	Approve Voucher 6	Cut Check 7	Add/Edit Vendor 8	Approve Vendor 9	Bank Reconciliation 10	Enter JE 11	Approve JE 12	Cust 13
Purchasing	R	Create Requisition	1		X		*		*	X	X	X	X		*	
	A	Approve Requisition	2	X		*		*		X	X	X	X	*		
	R	Create PO	3		*		X		*	X	X	X	X		*	
	A	Approve PO	4	*		X		*		X	X	X	X	*		
	R	Create Voucher	5		*		*		X	X	X	X	X		*	
	A	Approve Voucher	6	*		*		X		X	X	X	X	*		
	C	Cut Check	7	X	X	X	X	X	X		X	X	X	X	X	
	A	Add/Edit Vendor	8	X	X	X	X	X	X	X		X				
	A	Approve Vendor	9	X	X	X	X	X	X	X	X					
Reconciliation	RX	Bank Reconciliation	10	X	X	X	X	X	X	X				*	X	X
Journal Entry	R	Enter JE	11		*		*		*	X			*		X	X
	A	Approve JE	12	*		*		*		X			X	X		X

Activity 11:

Login to fplay using your prod user name and password.

Go to the Query Manager under Reporting Tools and run the SEGREGATE_DUTY_BOR query.

Choose Create Requisition.

Make note of user.

- User preference Report is located at Set Up Financials/Supply Chain > Common Definitions >User Preferences > User Preferences Report

It can be run by an individual user or by all users

User Preferences Report

Run Control ID post Report Manager Process Monitor [Run]
Language [English ▼]

Report Request Parameters

☐ Asset Management ☐ General Ledger ☐ Order Management ☐ Purchasing
☐ IT Asset Management ☐ Inventory ☐ Payables ☐ Receivables
☐ Billing ☐ Manufacturing ☐ Project Costing ☐ Maintenance Management

☑ Report on All Products
☑ Report on All Users

[Save] [Return to Search] [Previous in List] [Next in List] [Notify] [Add] [Update/Display]

Activity 12:

Login to fplay using your prod user name and password.

Go to the User Preferences Report and run it for ALL Products and for user id noted in activity 11.

- The Commitment Control Security report is located at: BOR Menus > BOR Utilities > BOR Security > Commitment Control Security

This query will provide you a list of users and their associated commitment control security rules.

Activity 13:

Login to fplay using your prod user name and password. Go to the Commitment Control Security Report and run it for your institution.

The BOR_SEC_USER_ROLE_PLIST_PAGE query or the BOR_SEC_USER_ROLES query can be used to show what roles a user id has access to.

Institution Audit Checklist

ITS recommends that a binder be established and a copy of this checklist placed in the front for reference by the auditors. Complete each item as needed and record the actual date of completion. There are several categories, and within each category, there could be several tasks. These tasks will be listed out in the procedures that will be distributed as part of this packet. For example, within account maintenance, there may be changes in a user's job function that would require the security

administrator to make a security change in the system as well as get an updated and signed security request form. Password resets and lockouts would also fall under the account maintenance category.

Not only does an institution need to keep a copy of the checklist, but it is recommended that all associated policies and procedures that correspond to the checklist be kept in a binder. Any documentation that is associated to a change that is made in the system should be kept in the binder, divided by months, so that this binder can be handed directly to the audit staff. Keep all security request forms, changes, updates and annual review forms in a binder to ensure compliance.

Category	Description of Change/Update	Frequency	Completion Date Range	Completion Date
Account Setup/Termination		As Needed		
Account Maintenance		As Needed		
User Acceptance Testing		As Needed		
Model Change Request		As Needed		
Terminated User Query		Monthly	End of Month	
Segregation of Duties Query		Monthly	End of Month	
User Access Query		Quarterly	March/ June/ September/ December	
Annual User Account Audit		Yearly	March	

Frequently Asked Questions

Q. After a security administrator assigned budget security to a user, that user still didn't have budget security access in the system. Why?

A. The security administrator forgot to run the request build process.

Q. I provided my user with access to the match workbench however the user still cannot unmatch vouchers.

A. It is a process group issue under user preferences. Ensure they have the Matching process groups.

Q. What is this error message? "No origin was found on you operator profile."

A. This error message is typically found when trying to enter a voucher. Go to the user preferences for the user and go to the payables link and enter ONL in the origin field.

Q. I'm trying to enter a user id on the Expenses Approver Assignments page and I am receiving the error message that this person is a multi campus user, however I know they are not.

A. Alot of times the issue is not with the person you are trying to enter. Sort the page by Employee ID and if there is a userid that doesn't have an associated employee id, this is your issue. If it is truly a multi campus user issue, contact ITS.

Q. My ePro approver can't approve the transaction that is in their worklist; They are receiving the error message stating you are not authorized, however I gave them the approver role.

A. The issue is with user preferences, they need the Approve user preference under requisition authorizations.

Q. I have a new person that I want to be a Security Administrator. What do i need to do?

A. Create the user id and assign all necessary roles. Enter a ticket with ITS to have them provide the local security administration roles.

Q. I can't add Commitment Control Security rules to a user. I have tried searching for their user id and adding their user id and it will not come up.

A. The issue is that the User id is not setup as employee. IT must contain an employee id to receive commitment control security.

Q. What role can be given to allow a user to only do password resets?

A. The role name is: BOR_PT_USER_GENERAL This could be given to a helpdesk to have them to the majority of the password resets.

Q. I am resetting a password for a user, however when I click save, I am getting a multi campus user error?

A. Sometimes people define an alternate user and forget to remove it after the date range expires. If this alternate user terminates and moves to another institution, they are the multi campus user. Look on the workflow tab of the user profile and clear out the alternate user id and date range.

Q. I was running a query on roles assigned to my users and a role showed up on the query that I can't see on the users profile?

A. This is mostly likely a role that existed in version 8.9 that is no longer available. Unfortunately you have to submit a ticket to ITS to remove the role.

Q. I have a user that cannot get to the report manger to retrieve their reports? Please advise.

A. The issue is that they are missing the BOR_FN_ADMIN_REPORTING role.

Q. User cannot pull up items from their worklist.

A. User has: "Use standard layout mode" enabled under personalization options, default is "Accessibility features off". Have use turn it back to "Accessibility features off"

Q. User is trying to post a budget journal and is getting the Security Error under Budget Header Status.

A. If you are receiving the Budget Security Error when creating a budget journal, your security administrator has not assigned you the BUD_ENTRY and/or BUD_XFER commitment control security rule; It is located under Commitment Control, Define Budget Security, Assign Rule to User id;. Once they do, they will need to run the request build process that is in the same menu structure.You will need to reenter the budget journal.

APPENDIX A

Job Aids By Job Function

All Job Aids are located at: http://www.usg.edu/gafirst-fin/documentation/job_aids/category/security
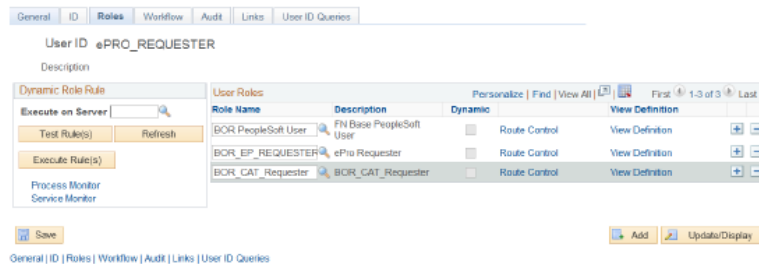
Here is a sample:

ePro REQUESTER
9.2 SECURITY ROLES & USER PREFERENCES

SECURITY ROLES

1

Navigation:

PeopleTools > Security > User Profile > Distributed User Profile > Add a New Value > User Roles Tab

ePro Requester users enter requisitions in the ePro module. They can also insert ad hoc approvers.

ROLES:
BOR_EP_MAINT_REQ
BOR_EP_REQUESTER
BOR PeopleSoft User

If user is a GeorgiaFirst Marketplace Requester, also add these Roles:
BOR_CAT_Requester
BOR_EP_MAINT_REQ_SCI

If the user needs to have their access cutoff at year end, then user the following roles instead:

BOR_EP_MAINT_REQ_YE_CUTOFF
BOR_EP_REQUESTER_YE_CUTOFF
BOR_EP_MAINT_REQ_SCI_YE_CUTOFF

PeopleSoft 9.2 — ePro REQUESTER 9.2 SECURITY ROLES & USER PREFERENCES

USER PREFERENCES

2

Navigation:
Set Up Financials & Supply Chain > Common Definitions > User Preferences > Define User Preferences > Overall Preferences

USER PREFERENCES

3

Navigation:
Set Up Financials & Supply Chain > Product Related > Procurement Options > Purchasing > Requester Setup > Add a New Value

Default Requisition Status should be set to Pending Approval.

The GL Unit must be defined in the Chartfields section. Always leave the account field under defaults blank. This will default into the requisition from the NIGP code.

In the catalog information section, select the Default checkbox and enter SHARE for the SetID. Enter either NIGP_TREE or NIGP_SHORT_TREE for catalog ID.

PeopleSoft 9.2 | ePro REQUESTER 9.2 SECURITY ROLES & USER PREFERENCES

USER PREFERENCES
4

Navigation:
Set Up Financials & Supply Chain > Common Definitions > User Preferences > Define User Preferences > Procurement

USER PREFERENCES
5

Navigation:
Set Up Financials & Supply Chain > Common Definitions > User Preferences > Define User Preferences > Procurement > Requisition Authorizations hyperlink

Select 'Full Auth for All Requesters' if user should have authority for all requesters. Do not specify individual Requester Id's in the 'Requesters User Authorization' section if Full Authority is granted.

If the user should not have authority for all do not select the option above. Instead, enter the Requester ID for each requester that the user should have authority for in the 'Requesters User Authorization' section. Also, select the applicable box(es) to grant authority to the user for all applicable actions (Add, Update, etc).

Note: Reopen is a new option in 9.2. Only grant if user should have authority to reopen Requisitions.

Appendix B:

Workflow

Stages of Approvals

Stage 1 - Asset Approval

Approval Process Definition
- In this stage, vouchers will be routed to the Asset approver if the profile id is blank and the account is an asset account.
- Vouchers will also be routed if the profile id is populated and the account is not an asset account.
- Vouchers will also be routed if the account is in the 743% range and greater than 3000.00 and the profile id is blank.
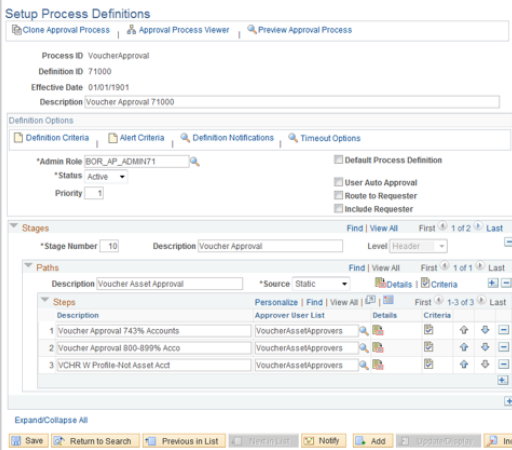- If there is no user at the institution with the correct asset approval role, it will route to the Accounts Payable Admin on campus. The Accounts Payable Admin on Campus must be identified and assigned the BOR_AP_ADMINXX role (the XX is the first two digits of the setid).

Workflow

Stages of Approvals

These transactions will route to an approver with the BOR_VOUCHER_ASSET_APPR role.

Institution Customization Options
- This approval level is optional.
- Institutions may choose to route all transactions with Asset Accounts even if the profile id is populated to ensure the profile id is correct.
- Institutions can determine if they want all the asset approvers to approve the Voucher or if only one has to approve it for those with multiple asset approvers.

ITS has to be notified of which option is selected, so that workflow can be configured appropriately.

Stage 2 - Budget Ref Approvals

Budget Ref Approval Process Definition
- In this stage, purchase orders will be routed to an approver on campus if the budget reference on the Voucher is different from the budget reference on the Purchase Order if it was sourced from a PO; Or

- In this stage, Vouchers will be routed to an approver on campus if the budget reference on the Voucher doesn't match the accounting date and it was not sourced from a Purchase Order.

Stages of Approvals

Setup Process Definitions

Clone Approval Process | Approval Process Viewer | Preview Approval Process

Process ID VoucherApproval
Definition ID 71000
Effective Date 01/01/1901
Description Voucher Approval 71000

Definition Options
Definition Criteria | Alert Criteria | Definition Notifications | Timeout Options

*Admin Role BOR_AP_ADMIN71   ☐ Default Process Definition
*Status Active   ☐ User Auto Approval
Priority 1   ☐ Route to Requester
                                         ☐ Include Requester

Stages   Find | View All   First ◁ 2 of 2 ▷ Last
*Stage Number 20   Description Voucher Budget Reference Appr   Level Header

Paths   Find | View All   First ◁ 1 of 1 ▷ Last
Description Voucher Budget Reference Appr   *Source Static   Details | Criteria

Steps   Personalize | Find | View All | ⤓ | 🖾   First ◁ 1 of 1 ▷ Last
Description   Approver User List   Details   Criteria
1 Voucher Budget Reference Appr   VoucherBudRefApprovers

Expand/Collapse All

Save | Return to Search | Previous in List | Next in List | Notify | Add | Update/Display | Include History | Correct History

These transactions will route to an approver with the BOR_VOUCHER_BUD_REF_APPR.

Institution Customization Options

➢ Institutions may inactivate this Stage.

➢ Institutions can determine if they want all the budget ref approvers to approve the Voucher or if only one has to approve it for those with multiple budget ref approvers.

Stages of Approvals

Checklist

1) Determine Stages that your campus would like to enable.

   Activate   Inactivate
   a. Stage 1 – Asset Approval   ☐   ☐
   b. Stage 2 – Budget Ref Approval   ☐   ☐

2) Within Each Stage, Determine if there are institution specific criteria needed, such as how many approvers have to approve, or if all assets should route, etc…

3) Determine who on campus will be the Accounts payable admin for workflow issues. This person(s) will need to be granted the BOR_AP_ADMINXX role (XX is first two digits of your setid) to their user id.

4) Determine approvers for each stage and grant them the approval roles.

5) Determine the amount of days to remind the approvers that they haven't approved it yet and how many days before it reassigns to the admin.