**UNIVERSITY SYSTEM OF GEORGIA**
Information Technology Services

User's Guide
for
Security Administrators

PeopleSoft 9.2

Georgia*FIRST*

(This page is intentionally left blank for printing purposes.)

# TABLE OF CONTENTS

# Introduction: PeopleSoft Security Basics

**Security Design Strategy** *(Optional)*

Before we focus on security, we will begin with an overview of the PeopleSoft Financials security design philosophy. The three components of this system are **Users**, **Roles**, and **Permission Lists**.
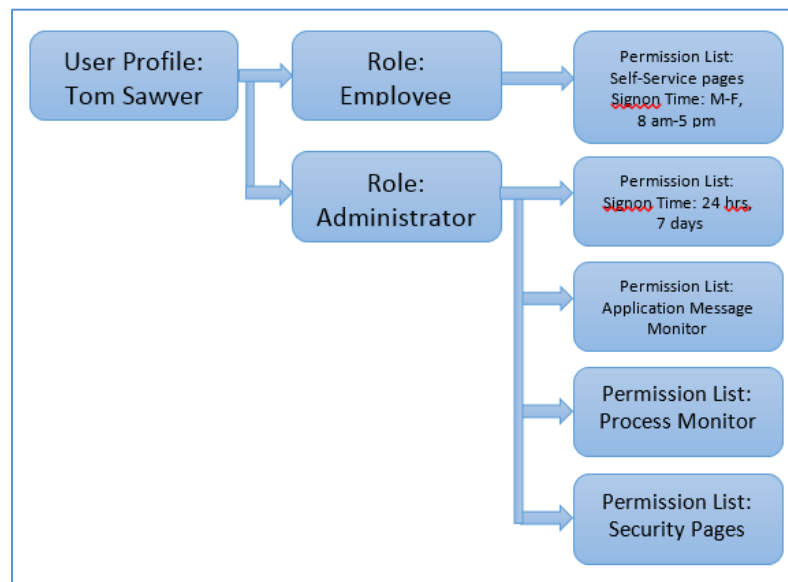


User Profiles, i.e., the user, refers to any employee set up to use the system. Each user is assigned one or more roles. These roles, sometimes called Model Roles because we deliver most roles to schools rather than allowing them to create their own, then determine which business processes a particular user is allowed to perform. The business processes are contained in Permission Lists (see chart above).

Roles are "granular," which means that each role is based upon a specific business process. Therefore, access needed to complete a business process is mapped into corresponding role/roles. For example, if you assign a user the Voucher Entry role, that user automatically has access to Add Vouchers.

Some business processes require only one role to complete. More complex business processes, such as running a pay cycle under Accounts Payable, 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 institutions to administer the delivered roles to their individual users through a distributed user profile. We will cover this more in the security administration area of this document.

## Dynamic Roles

To make role assignment faster and more efficient, the Georgia*FIRST* model utilizes the dynamic roles functionality within PeopleSoft. Dynamic roles allow administrators to assign roles based on preset permissions.

Roles can be assigned dynamically using several different methods. One method is by creating a query that says, If a user has access to role X, then automatically give them role XX as well. In addition, if a user has access to page X, then role X can also be assigned. The benefit of creating a dynamic role is that, when role X is removed, role XX is also removed. Queries, PeopleCode, or Directories can be used to assign dynamic roles.

Currently, ITS has only one Dynamic Role: the **BOR_EX_APPROVAL** role. Any user who is on the Expenses Approver Assignments page automatically gets this role. As a result, they also receive permission to approve expense transactions. Upon termination, the user should be removed from the Expenses Approver Assignments page. The Dynamic Role will automatically be removed from their user profile.

## Permission Lists

Permission Lists, building blocks of end-user security authorizations, control what a user can and cannot access. A user inherits permissions through the role or roles the security administrator assigns to them. In the chart above, notice that 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 assigned.

A Permission List may contain any number of the following permissions: sign-on times, page permissions, component interface permissions, web libraries, and so on. Although a permission list may contain one or more

permissions, the smaller the number of permissions within a particular permission list, the more flexible and scalable that permission list is.

**Please note:** 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.

All permission lists start with the module, i.e., GL for General Ledger, and are then followed by the name of the permission list. For example, GL_PAY_INTERFACE is a General ledger permission list. Tools version 8.4+ allows you the naming length of 30 characters for a permission list.

There are two tables that contain information on permission lists:

- PSCLASSDEFN - Permissions Lists Definition
- PSAUTHITEM - Authorized Menu Item

## Workflow Roles

When enabled, some delivered business processes provide for the routing of work through an automated process called workflow. For example, when an Accounts Payable clerk enters a voucher, and an Accounts Payable manager needs to approve it, the system will automatically route the transaction to the manager using 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 provide only this function. They will be different from other roles in that they are shell roles, with no page access.

# Chapter 1: Security Administration

System security involves protecting financial data against modification, loss, theft, and unauthorized disclosure. To ensure the safety of data, Georgia*FIRST* has a security framework with several key areas of control, such as data access, password management, user account management, authorization management, and audit logs.

Security administration is distributed to each institution, and it is that institution's responsibility to administer, update, and maintain it. This is done through role grant and distributed user profiles. Since ITS creates the roles and permissions, each institutional security administrator must have a security role that allows access to the delivered roles. This role is BOR_LOCAL_SEC_ADMIN and 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 (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
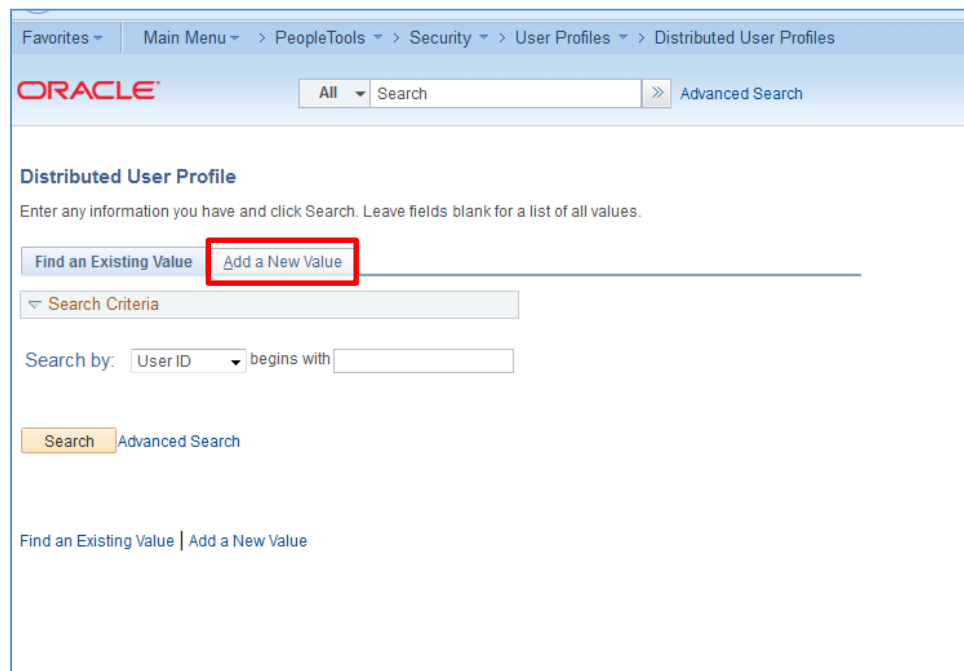
# Chapter 2: Managing User Security

User Profiles define individual PeopleSoft users. You begin the security process by defining User Profiles and then linking each User to roles. Normally, a User Profile is linked to at least one role in order for it to be a valid profile; however, it is possible to have a User Profile with no Roles if, for example, a user who is not allowed access to the PeopleSoft application needs to receive workflow-generated emails. As we explained in the Introduction, the majority of permissions (values) that make up a user profile are inherited from the linked roles.

**User Profiles**
The first thing you must do to set up a User Profile is create a User ID by entering appropriate values, such as user password, work email (.edu) address, employee ID, and so on. To set up a User Profile, follow the navigation:

*PeopleTools > Security > User Profiles > Distributed User Profiles.*



There are three ways to manually create a new User Profile. First, you can click on the "Add a New Value" tab and add a User ID. The User ID should be unique and not contain white space or any of the following special

characters: ; : & , < > \ / " [ ] ( ). People Tools version 8.5+ allows you the naming length of up to 30 characters. (Some institutions prefer that the User ID not be tied to the user's name. Check your institution to see if they have a preferred style for User IDs.) Click the **Add** button.
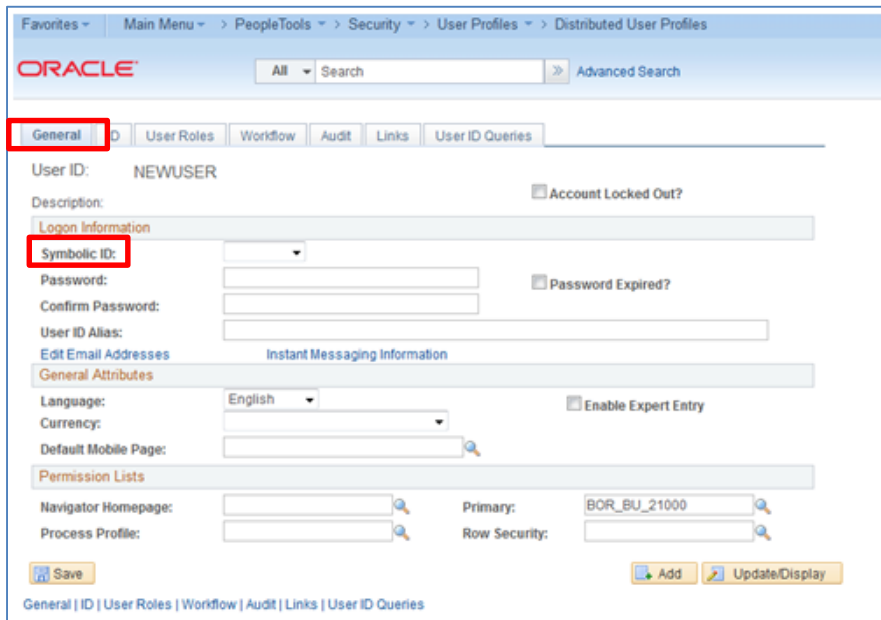


The second way to create a new Profile is to use the **Copy User Profile** feature to duplicate a similar profile. The benefit of using this method is that, if you have a core user with 50 roles and hire another user who needs the same 50 roles to replace them, you either have to manually add the 50 roles or do the **Copy User Profile**, which copies the roles. To copy a User Profile, follow the navigation: *PeopleTools > Security > User Profiles >* **Copy User Profile.** The name of your new profile will need to be different from the one you are about to copy.

**Please note:** The third way to create a User Profile is to have the user self-register. This method is explained on page 24.

**General Tab**

Now that you have created a new User ID, you can enter the user's values into fields located under the "General" tab.



1. Start by entering the **Symbolic ID**. Click the down arrow and select the system default (SYSADM1). (Users who will only be authenticating through a Directory will not need a **Symbolic ID** for access into the system.)

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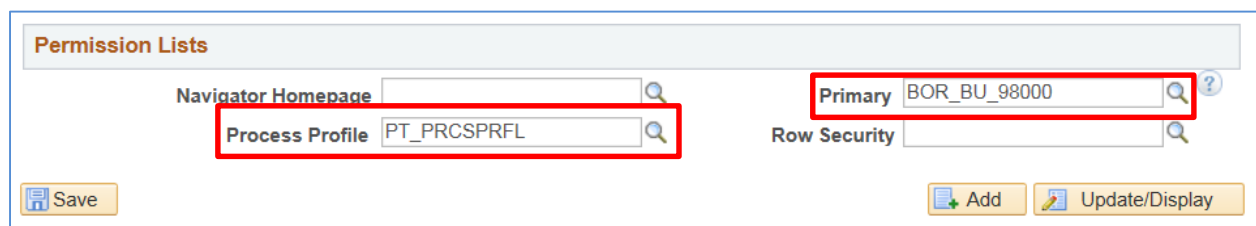


When a password is entered, the system will automatically make the password longer and return dots, then save the profile.



---

The only other fields that may be required on the "General" tab are the **Process Profile** and **Primary** fields in the **Permission Lists** portion of the page.

**Permission Lists**

The **Process Profile** can control which processes a user is allowed to run. In the Georgia*FIRST* model, processes are not grouped into different process groups. If a user has security to a page, he or she can run the process because all processes have been consolidated into one group. To add a process, type **PT_PRCSPRFL** into the Process Profile.

**Please note:** This is the only instance where a permission list is attached directly to the User Profile.
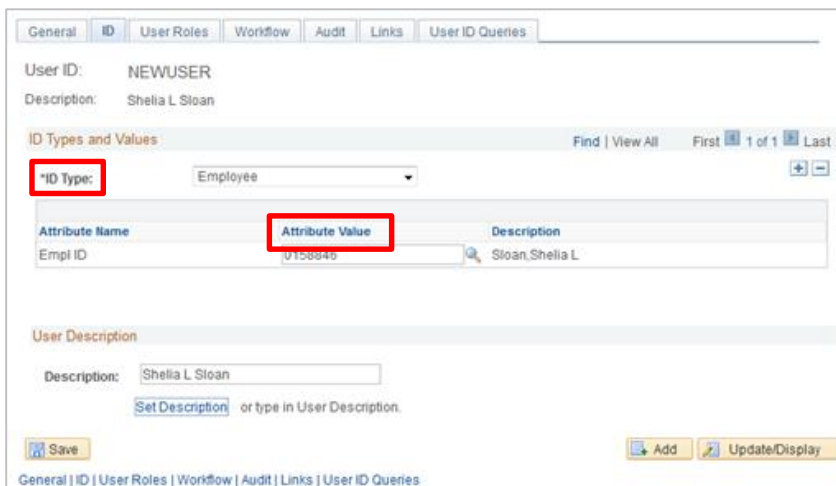


The **Primary** permission list is what controls which institution's data the user can access, update, and inquire on. For example if a university's Business Unit is XXXXX, the user's primary permission list is BOR_BU_XXXXX. This list enforces row level security and allows users to see data only from their institution. To give permission for a Primary level,

1. Click on the **Search** symbol beside the Primary key field.
2. Click the number that corresponds to your organization.
3. Click **Add.**

If the local security administrator creates the profile manually, the process profile defaults from the local security administrator's profile.

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**.

| General | ID | User Roles | Workflow | Audit | Links | User ID Queries |

User ID:        NEWUSER
Description:    Shelia L Sloan

ID Types and Values                                    Find | View All      First ◄ 1 of 1 ► Last

*ID Type:          Employee                    ▼                                              ➕ ➖

| Attribute Name | Attribute Value | Description |
| Empl ID | 0158846 🔍 | Sloan,Shelia L |
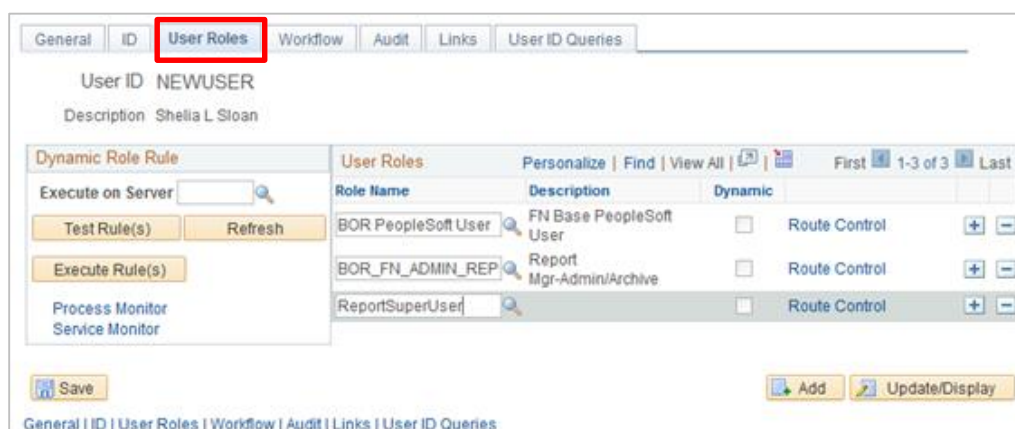
User Description

Description:    Shelia L Sloan

Set Description  or type in User Description.

🖫 Save                                                    ➕ Add    ⧉ Update/Display

General | ID | User Roles | Workflow | Audit | Links | User ID Queries

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

**User Roles Tab**

| General | ID | User Roles | Workflow | Audit | Links | User ID Queries |

User ID  NEWUSER
Description  Shelia L Sloan

Dynamic Role Rule

Execute on Server  [        ] 🔍

[ Test Rule(s) ]   [ Refresh ]

[ Execute Rule(s) ]

Process Monitor
Service Monitor

User Roles                Personalize | Find | View All | ⧉ | 📇       First ◄ 1-3 of 3 ► Last

| Role Name | Description | Dynamic | | | |
| BOR PeopleSoft User 🔍 | FN Base PeopleSoft User | ☐ | Route Control | ➕ | ➖ |
| BOR_FN_ADMIN_REP 🔍 | Report Mgr-Admin/Archive | ☐ | Route Control | ➕ | ➖ |
| ReportSuperUser 🔍 | | ☐ | Route Control | ➕ | ➖ |

🖫 Save                                                    ➕ Add    ⧉ Update/Display

General | ID | User Roles | Workflow | Audit | Links | User ID Queries

Use the **User Roles** tab to attach the functional and system roles you need to complete the profile definition.
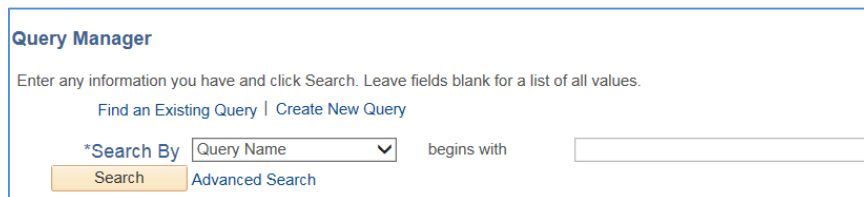
The business processes you are trying to complete determine what roles you need. For example, if the business process is "Enter a PO Voucher", then you look up the role associated with that process, such as BOR_AP_VOUCHER_ENTRY. Because all roles are not intuitive, you may need to consult Job Aids on the Georgia*First* website (http://www.usg.edu/gafirst-fin/documentation/job_aids/category/security). Once the appropriate roles are attached, click the **Save** button to complete your profile.

**Determining Access**

One of the most difficult tasks for security administrators is determining what access and what level of access an end user needs. This can vary by institution because of the hundreds of roles and other aspects of security. We will address a few of the tools and queries that can be used to determine what access a role has and what access an individual needs.

The first one is PT_SEC_ROLE_PAGES, which is run by role. To reach Query Manager, follow the navigation: **Reporting Tools > Query > Query Manager.**

**Query Manager**

Enter any information you have and click Search. Leave fields blank for a list of all values.

Find an Existing Query | Create New Query

*Search By [Query Name ⌄] begins with [                    ]

[Search]  Advanced Search

Enter your Query Name and click on Search.
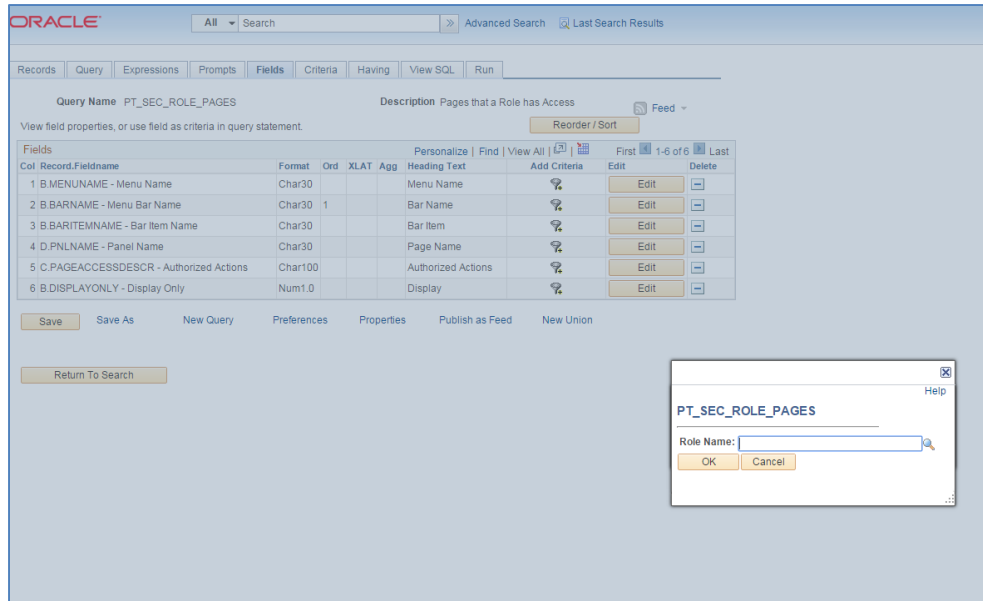
Click run and enter your search criteria. Select OK.

**Role Name = BOR_AP_INQUIRY**

View All | Rerun Query | Download to Excel | Download to XML — First ◄ 1-100 of 104 ► Last

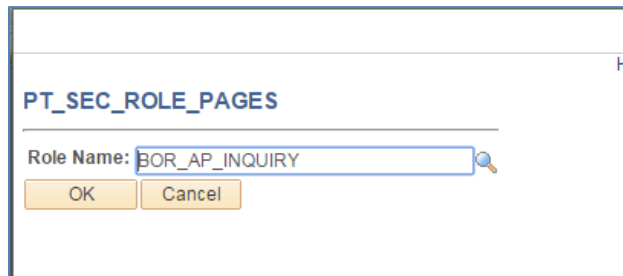| | Menu Name | Bar Name | Bar Item | Page Name | Authorized Actions | Display |
|---|---|---|---|---|---|---|
| 1 | CREATE_PAYMENTS | INQUIRE | MTRC_AP_PYCYCL | MTRC_AP_PYCYCL | Update/Display | 0 |
| 2 | CREATE_PAYMENTS | INQUIRE | PYCYCL_DATA_INQ | PYCYCL_DATA_INQ | Update/Display | 0 |
| 3 | CREATE_PAYMENTS | 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 |

The query results return menu names down to page names. Because distinguishing what the Page actually is may be difficult, you need to run the BOR_PORTAL_PERMISSIONS query:

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

Query Name  BOR_PORTAL_PERMISSIONS  Description  Portal permissions

Working on selection  Top Level of Query

Feed ▾
Subquery/Union Navigation

View field properties, or use field as criteria in query statement.

Reorder / Sort

**Fields**

Personalize | Find | View All | 🗗 | 🖩   First ◄ 1-8 of 8 ► Last

| Col | Record.Fieldname | Format | Ord | XLAT | Agg | Heading Text | Add Criteria | Edit | Delete |
|-----|------------------|--------|-----|------|-----|--------------|--------------|------|--------|
| 1 | A.ROLENAME - Role Name | Char30 | | | | Role Name | 🔍 | Edit | − |
| 2 | D.PORTAL_OBJNAME - Portal Object Name | Char30 | | | | PortlObjNm | 🔍 | Edit | − |
| 3 | E.PORTAL_LABEL - Portal Label | Char30 | | | | PortlLabel | 🔍 | Edit | − |
| 4 | B.MENUNAME - Menu Name | Char30 | 1 | | | Menu Name | 🔍 | Edit | − |
| 5 | B.BARNAME - Menu Bar Name | Char30 | | | | Bar Name | 🔍 | Edit | − |
| 6 | B.BARITEMNAME - Bar Item Name | Char30 | | | | Bar Item | 🔍 | Edit | − |
| 7 | B.PNLITEMNAME - Panel Item Name | Char30 | | | | Panel Item | 🔍 | Edit | − |
| 8 | C.PNLGRPNAME - Component Name | Char18 | | | | Component | 🔍 | Edit | − |

Save | Save As | New Query | Preferences | Properties | Publish as Feed | New Union

Return To Search

⊠
Help

**BOR_PORTAL_PERMISSIONS**

Role Name: BOR_AP_INQUIRY   🔍

OK | Cancel

---

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, the query results contain the Portal Label, which is sometimes much more intuitive than the page name itself. These two queries are helpful if you want to see what access a specific role contains. This query could be modified to remove the prompt for the Role Name field. Removing the prompt would allow you to run the query for all delivered roles.

Security Matrix for 9.2, a list of all delivered BOR roles, and spreadsheets broken out by business processes and roles are available on the Georgia*FIRST* website.

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| | CLASSID | MENUNAME | BARNAME | BARITEMNAME | PNLNAME | PAGEACCESSDESCR | | DISPLA |
| 1 | BOR_AP_INQUIRY | AP_CRTE_PMNTS_INQ | CREATE_PAYMENTS | INQUIRE | MTRC_AP_PYCYCL | MTRC_AP_PYCYCL | Update/Display | 0 |
| 2 | BOR_AP_INQUIRY | AP_CRTE_PMNTS_INQ | CREATE_PAYMENTS | INQUIRE | PYCYCL_DATA_INQ | PYCYCL_DATA_INQ | Update/Display | 0 |
| 3 | BOR_AP_INQUIRY | AP_CRTE_PMNTS_INQ | CREATE_PAYMENTS | INQUIRE | PYCYCL_DATA_SUM | PYCYCL_DATA_SUM | Update/Display | 0 |
| 4 | BOR_AP_INQUIRY | AP_CRTE_PMNTS_INQ | CREATE_PAYMENTS | INQUIRE | PYMNT_INQ_SRCH | PYMNT_INQ_SRCH | Update/Display | 0 |
| 5 | BOR_AP_INQUIRY | AP_CRTE_PMNTS_INQ | CREATE_PAYMENTS | INQUIRE | PYMNT_VCHR_DETAIL | PYMNT_VCHR_DET_SEC | Update/Display | 0 |
| 6 | BOR_AP_INQUIRY | AP_CRTE_PMNTS_INQ | CREATE_PAYMENTS | INQUIRE | REPLACED_PAYMENTS | PYMNT_RPLCD | Update/Display | 0 |
| 7 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | AP_GL_DRILL | AP_GL_DRILL | Update/Display | 0 |
| 8 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | AP_INQ_SEARCH | AP_INQ_SEARCH_DEFN | Update/Display | 0 |
| 9 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | AP_MTCH_WB_EXCPTN | AP_MTCH_WB_EXCPTN | Update/Display | 0 |
| 0 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | AP_MTCH_WB_EXCPTN | AP_WB_HEADER_EXPTN | Update/Display | 0 |
| 1 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | AP_MTCH_WB_MOVRD | AP_MTCH_WB_MOVRD | Update/Display | 0 |
| 2 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | AP_MTCH_WB_OVRD | AP_MTCH_WB_OVRD | Update/Display | 0 |
| 3 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | AP_MTCH_WB_SUCCESS | AP_MTCH_WB_SUCCESS | Add Update/Display | 0 |
| 4 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | AP_SEARCH_CRIT | AP_SRCH_CRIT_DEFN | Add Update/Display | 0 |
| 5 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | AP_VCHR_INQ | AP_VOUCHER_INQUIRY | Update/Display | 0 |
| 6 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | AP_VCHR_MTCH_INQ | AP_VCHR_MATCH_INQ | Add Update/Display | 0 |
| 7 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | DOC_TOL_EXCPT | DOC_TOL_EXCPT | Update/Display | 0 |
| 8 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | DOC_TOL_OVR_LOG | DOC_TOL_OVR_LOG | Update/Display | 0 |
| 9 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | PO_INQUIRY | PO_INQUIRY | Update/Display | 0 |
| 0 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | VCHR_ACCTG_UNBAL | VCHR_ACCTG_UNBAL | Update/Display | 0 |
| 1 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | VCHR_LINE_DSP | AP_VCHR_LN_DET_DSP | Update/Display | 0 |
| 2 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | VCHR_PYMNT_INQ | VCHR_PYMNT_INQ | Update/Display | 0 |
| 3 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | VOUCHER_ACCOUNTING_ENTRIES | VCHR_ACTG_ENTRIES | Update/Display | 0 |
| 4 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | INQUIRE | VOUCHER_EDIT_ERROR_DETAIL | VCHR_BATCHERR_PG | Update/Display | 0 |
| 5 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | UNMATCH_WRK | Update/Display | 1 |
| 6 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_CORRECTION | Update/Display | 1 |
| 7 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_ERRORSMMRY_PG | Update/Display | 1 |
| 8 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_EXPRESS1 | Update/Display | 1 |
| 9 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_LINE_MISC_CHG | Update/Display | 1 |
| 0 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_LINE_PO_WRK | Update/Display | 1 |
| 1 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_LINE_RECV_WRK | Update/Display | 1 |
| 2 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_LOOKUP_MTCH | Update/Display | 1 |
| 3 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_LOOKUP_MTCH2 | Update/Display | 1 |
| 4 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_MAIN2_WRK | Update/Display | 1 |
| 5 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_PAYMENT_PNL | Update/Display | 1 |
| 6 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_RECV_MTCH | Update/Display | 1 |
| 7 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_REG_WRK_LC | Update/Display | 1 |
| 8 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_STATUS_IA | Update/Display | 1 |
| 9 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_SUMMARY_PG | Update/Display | 1 |
| 0 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_TEMPLATE | Update/Display | 1 |
| 1 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_TERMS_EXP | Update/Display | 1 |
| 2 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_VNDR_INFO | Update/Display | 1 |
| 3 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_WTHD_ERR | Update/Display | 1 |
| 4 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VCHR_WTHD_EXP | Update/Display | 1 |
| 5 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VNDR_LOOKUP_WRK | Update/Display | 1 |
| 6 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VNDR_LOOKUP_WRK1 | Update/Display | 1 |
| 7 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | ENTER_VOUCHER_INFORMATION | USE | EXPRESS_VOUCHER | VOUCHER_WRK_MTCH | Update/Display | 1 |
| 8 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | PROCUREMENT_ANALYSIS | INQUIRE | PO_DOC_STATUS | PRCR_DOCSTAT_INQ | Update/Display | 0 |
| 9 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | PROCUREMENT_ANALYSIS | INQUIRE | PO_DOC_STATUS | PRCR_DS_PO_WRK | Update/Display | 0 |
| 0 | BOR_AP_INQUIRY | AP_ENTER_VCHR_INFO_INQ | PROCUREMENT_ANALYSIS | INQUIRE | VOU_DOCSTAT_INQ | PRCR_DOCSTAT_VCHR | Update/Display | 0 |
| 1 | BOR_AP_INQUIRY | AP_MNG_COMMIT_CNTRL_INQ | MANAGE_COMMITMENT_CONTROL | INQUIRE | KK_XCP_AP1 | KK_XCP_HDR_AP1 | Update/Display | 0 |

| 1 | Business process | 9.2 Role |
|---|---|---|
| 2 | AP.020.503 Locating Pay Cycle files in Report Manager | BOR PeopleSoft User |
| 3 | AP.020.140 Uploading Vouchers from MS Excel | BOR PeopleSoft User; Query Access |
| 4 | AP.080.012 1099 Withholding Report Control Information | BOR_AP_1099_PRC |
| 5 | AP.080.020 1099 Posting Withholding Transactions | BOR_AP_1099_PRC |
| 6 | AP.080.030 1099 Withholding Invoice Line Update | BOR_AP_1099_PRC |
| 7 | AP.080.040 1099 Withholding Vendor Updates | BOR_AP_1099_PRC |
| 8 | AP.080.050 1099 Running Withholding Update Process | BOR_AP_1099_PRC |
| 9 | AP.080.090 1099 Adjusting Withholding Manually | BOR_AP_1099_PRC |
| 10 | AP.080.110 1099 Generating Withholding Reports | BOR_AP_1099_PRC |
| 11 | AP.080.120 1099 Running Withholding Sent File Process | BOR_AP_1099_PRC |
| 12 | AP.080.100 1099 Running Withholding Report Post | BOR_AP_1099_PRC |
| 13 | AP.080.060 1099 Reviewing Vendor Balances by Class | BOR_AP_1099_RPTS |
| 14 | AP.080.070 1099 Reviewing Vouchers by Vendor | BOR_AP_1099_RPTS |
| 15 | AP.080.080 1099 Reviewing Payments to Withholding Vendors | BOR_AP_1099_RPTS |
| 16 | AP.070.040 Running 1099-MISC Copy B Report (APY1099) | BOR_AP_1099_RPTS |
| 17 | AP.070.115 APY3012 Vendor WH Balances Control Report | BOR_AP_1099_RPTS |
| 18 | AP.070.170 APY7010 Withholding Rules Report | BOR_AP_1099_RPTS |
| 19 | AP.070.175 APY7020 Withholding Types Report | BOR_AP_1099_RPTS |
| 20 | AP.070.180 APY7030 Withholding Entities Report | BOR_AP_1099_RPTS |
| 21 | AP.070.195 APY8056 1099 Withholding to Send Detail Report | BOR_AP_1099_RPTS |
| 22 | AP.070.200 APY9010 Withholding Mismatch Report | BOR_AP_1099_RPTS |
| 23 | AP.070.300 BORRY010 1099 Reportable Transactions Report | BOR_AP_1099_RPTS |
| 24 | AP.020.210 Deleting Control Groups | BOR_AP_CNTRL_GRPS_MAINT |
| 25 | AP.020.200 Creating and Using Control Groups | BOR_AP_CNTRL_GRPS_MAINT |
| 26 | AP.020.540 Canceling a Payment | BOR_AP_CRTE_PMNTS_MAINT |
| 27 | AP.020.550 Processing Escheated Payment | BOR_AP_CRTE_PMNTS_MAINT |
| 28 | AP.030.050 - Posting Payments | BOR_AP_CRTE_PMNTS_MAINT |
| 29 | AP.020.500 Payment Selection Criteria | BOR_AP_CRTE_PMNTS_PRC |
| 30 | AP.020.501 Running Check Pay Cycles | BOR_AP_CRTE_PMNTS_PRC |
| 31 | AP.020.502 Running EFT or ACH Pay Cycles | BOR_AP_CRTE_PMNTS_PRC |
| 32 | AP.020.510 Restarting a Pay Cycle (re-create buttons) | BOR_AP_CRTE_PMNTS_PRC |
| 33 | BK.010.070 Updating AP Pay Cycles for new Disbursement Bank | BOR_AP_CRTE_PMNTS_PRC |
| 34 | AP.040.030 Generating the Positive Payment File | BOR_AP_CRTE_PMNTS_PRC |
| 35 | AP.020.505 Reviewing Payments Selected and Exceptions & Alerts | BOR_AP_CRTE_PMNTS_PRC and BOR_AP_INQUIRY |

**Activity 1:**

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

1. What role should you give them? _____

2. 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.

3. What role is required? _____

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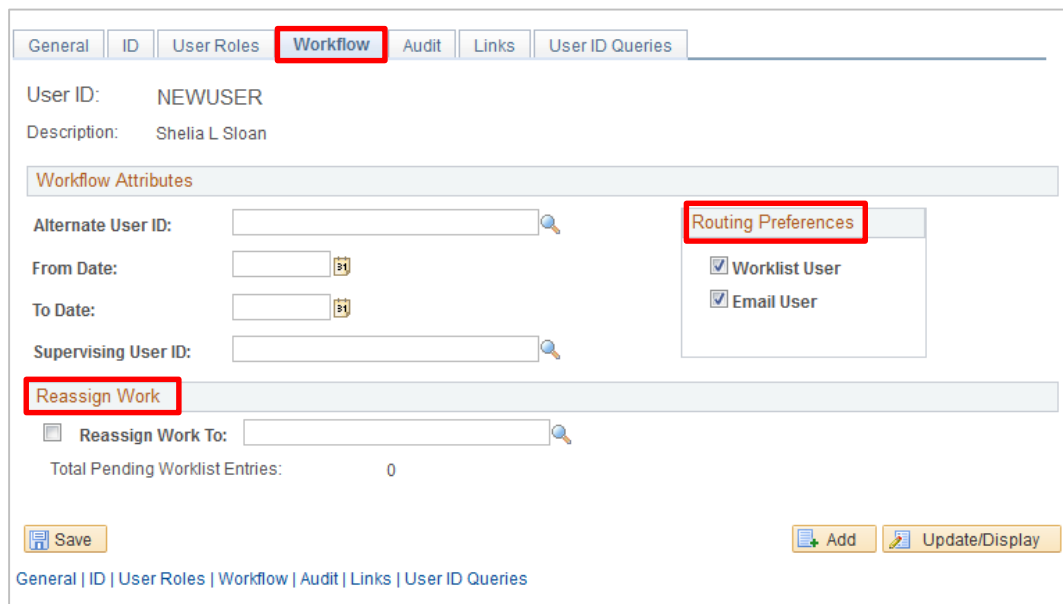
   _____

**Institution-Specific Job Aids and Forms**

As discussed before, one of the best ways to determine what access your employees need is to create custom security job aids by job functions. The Georgia*FIRST* website has sample job aids (http://www.usg.edu/gafirst-fin/documentation/job_aids/category/security); however, job functions will vary across institutions. Look for common job titles between various departments at your institution. Then if the job duties are the same, or even have only a few exceptions, document the security for that job duty and note the exception roles and preferences. 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 that lists each department and may also include names and job titles. If your Budget Office has a Director, Assistant Director, and Budget Analyst, for example, you could 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 only a few roles differ, you could use the same job aid and note the differences. The Budget Analyst would not need as much security, however, so I would expect to see a different job aid for that role.

Another example might involve the Purchasing Department. If you have a director, a senior buyer, a buyer, and a purchasing staff, you should divide these into different job aids. The director probably needs the most supervisory access, so that may be one job aid. Because the senior buyer and buyer need less security, they should probably be on the same job aid, and the Staff member, who needs even less security, should be on a separate job aid. This will help with Auditing purposes, documentation and ease of administration.

**Workflow Tab**



1. 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.

2. The **Email User** checkbox allows end users to receive system notifications via work email (.edu). These notifications will be sent to the email address on the user's General Tab. This box is selected by default, and I suggest leaving it checked for active employees.

3. The **Workflow Attributes** section allows a user to have an alternate approver defined. If a user defined as an approver is going to be out of the office for a predefined time, you can redirect approvals to a specified User ID for a date range. The **Reassign Work To** section allows the security administrator to reassign ALL transactions in this individual's worklist to a new approver. To redirect approvals, search for new approver and click on the **User ID**. Then click **SAVE**.

**Please Note:** This will reassign EVERYTHING. If this person is an ePro Approver and a General Ledger Approver, it will send all Requisition and Journal approvals to the person you identify. It cannot separate them out. If the

General Ledger transactions need to go to a different approver than the ePro transactions, use the Monitor Worklist page to reassign these transactions individually.

One other point to consider is that, reassigning work can cause issues if the date range expires. If the person 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 is changed. In addition, the system may continue 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.
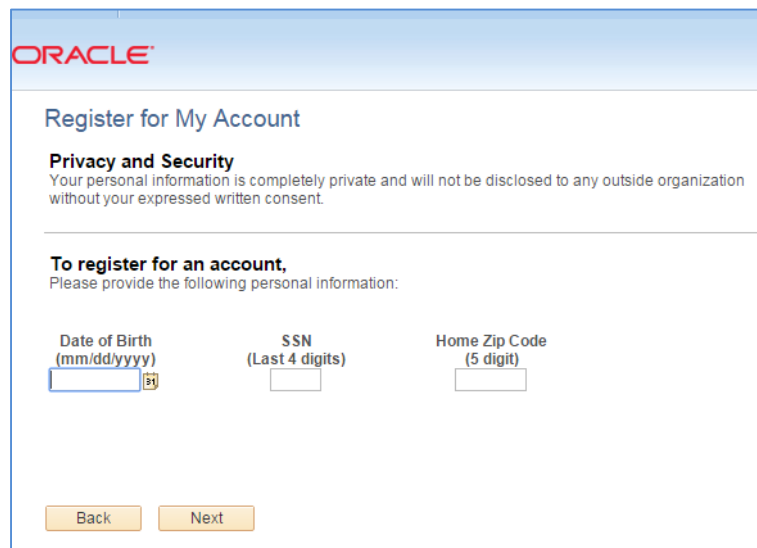
### Self-Registration

The third way to manually create a new User Profile is self-registration. For institutions at which many employees travel and, therefore, use travel and expenses, users may self-register so that they receive a user ID and basic rights to file an expense report. For large schools that have thousands of employees who travel, having users self-register saves you the time it takes to create multiple accounts. However, if the user needs other module functionality, then you must add the additional roles.

1. Login to the self-service site at fprod-selfservice.gafirst.usg.edu.

2. Click on **Register for My Account**.

3.  Fill in the required fields on the next screen:



4.  The system will display the job row for the employee who is self-registering. They need to click the box beside the active job row and select next. At this point, the user can create his or her own User ID and setup a 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, it assigns the basic expenses access required to create and print expense transactions. No security form is required for self-registered individuals until they need additional roles. At that point, approvals and documentation are required.
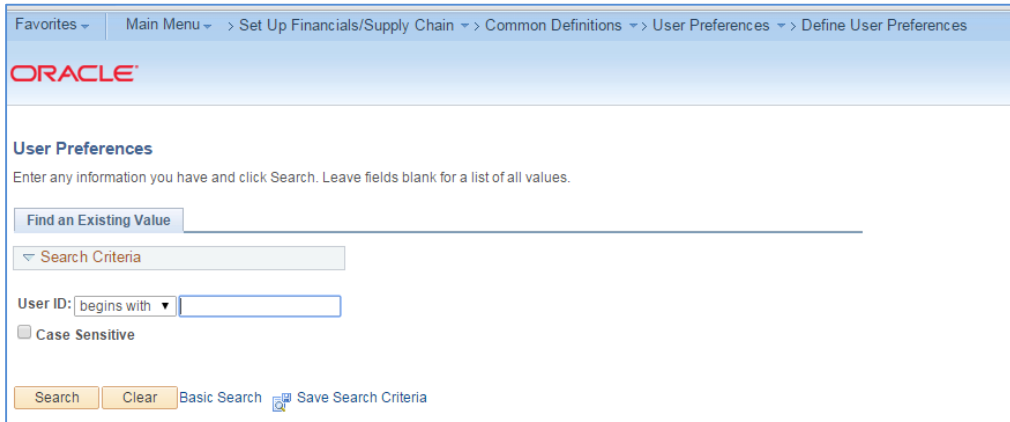
---

**Activity 2:**

1.  Login to FPLAY with your User ID and password that you use in current production.
2.  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.
3.  Save the user profile and write down the user name/password you created.

---

# Chapter 3: Managing 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. Institution security administrators and designates are responsible for setting up correct user preferences, which determine which actions the user can take.

To set up a user preference, follow the navigation: *Setup Financials/Supply Chain > Common Definitions > User Preferences > Define User Preferences*.
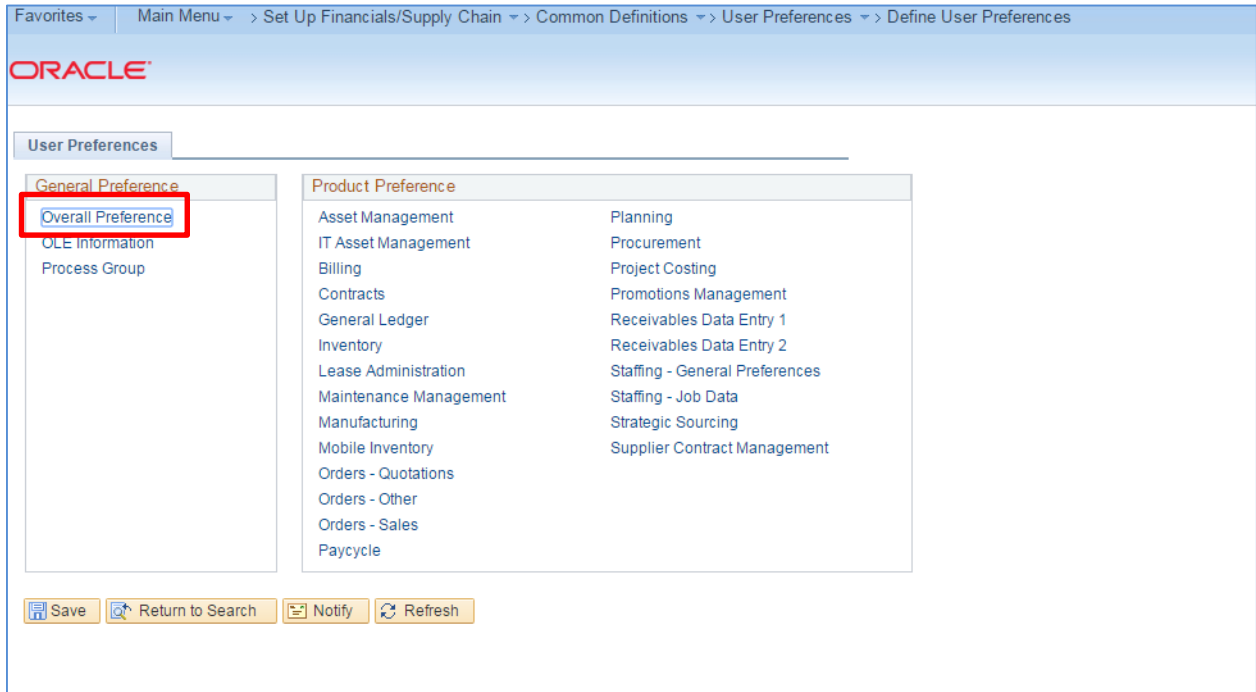


1.  Enter the **User ID**
2.  Click the **Search** Button.
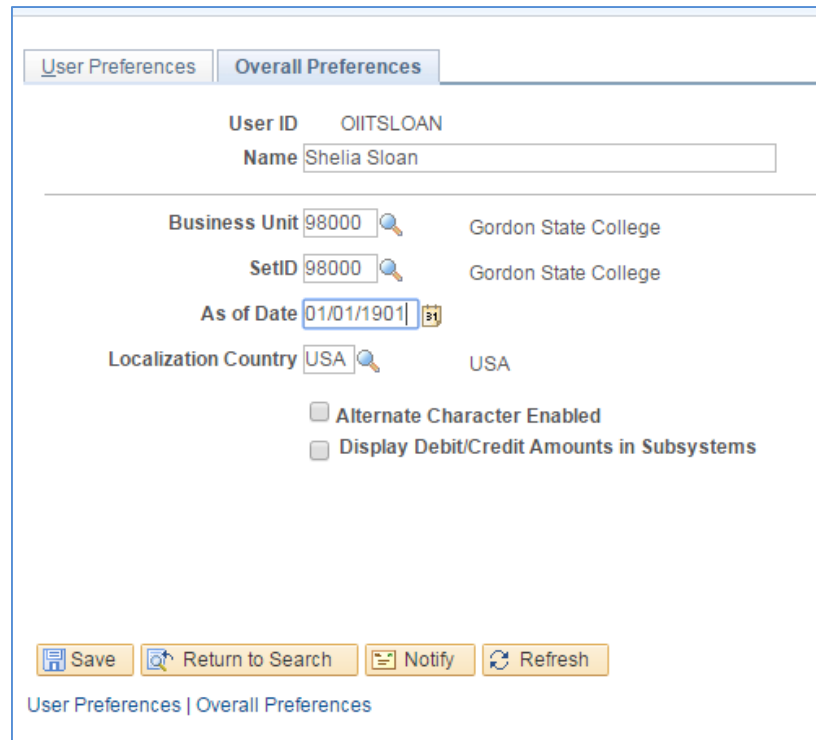3.  Click on the user's name.

**General Preference**

General user preferences provide certain user access that is cross modular rather than being tied to a specific module. As a result, administrators need to assign these user preferences at the beginning of reviewing user preferences for a particular user.

The first General Preference, the Overall Preference, is the business unit/setid and is required. Entering this information defaults the business unit on all user transaction pages. For example, in General Ledger, when a user adds a journal entry, the business unit defined here will default on the journal entry so that the user does not have to enter their institution ID for each transaction.



To set up the user's Overall Preferences, click on **Overall Preference** link in the left-hand bar.

1. Enter the **User ID** and **Name** fields default.

2. Enter the default **Business Unit**

3. Enter the default **SetID** field.

4. **As of Date** displays the default date for the Combo Edit process.

5. Enter "**USA"** in the **Localization Country** field**.**

6. **Do not** select **Alternate Character Enabled** to activate alternate description buttons or links. Georgia*FIRST* does not use this feature.

7. **Do not** select **Display Debit/Credit Amounts in Subsystem,** which displays debit and credit amounts of the default business unit on journal entry and inquiry pages. Georgia*FIRST* does not use this feature.

8. Select the **Save** button.

**OLE Information and Process Group**

When you return to the User Preferences tab, you will see two more choices on the left-hand bar. The first one is OLE Information. No setup is required.

The second choice is Process Group. This is set up by Security and controls the on-demand features on transaction pages. For instance, a user who enters a voucher may want to run budget check and voucher post directly on the voucher entry page. This transaction would be controlled and enabled through process groups. The **Allow Processing** checkbox must be selected.

Once you click **Save**, you will see a list of process groups that are enabled for different source transactions within the system. (You can also copy these source transactions from another user.)

Favorites ▾    Main Menu ▾ > Set Up Financials/Supply Chain ▾ > Common Definitions ▾ >

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 | ➕ | ➖ |

For example, if you have a super user who wants to run all voucher processes at once, including Budget Checking, Document Tolerance, Matching, and Voucher Post, assign the VCHR_STM process group in Source Transaction. If the user needs to run these processes on the voucher individually, then assign the Source Transaction of Voucher

individually. You then choose which one you want to run or, if you want to run all of them, you click Post Voucher (PST_VCHR).

The screen shot below shows the screen an Accounts Payable user would see if assigned the VOUCHER process group.
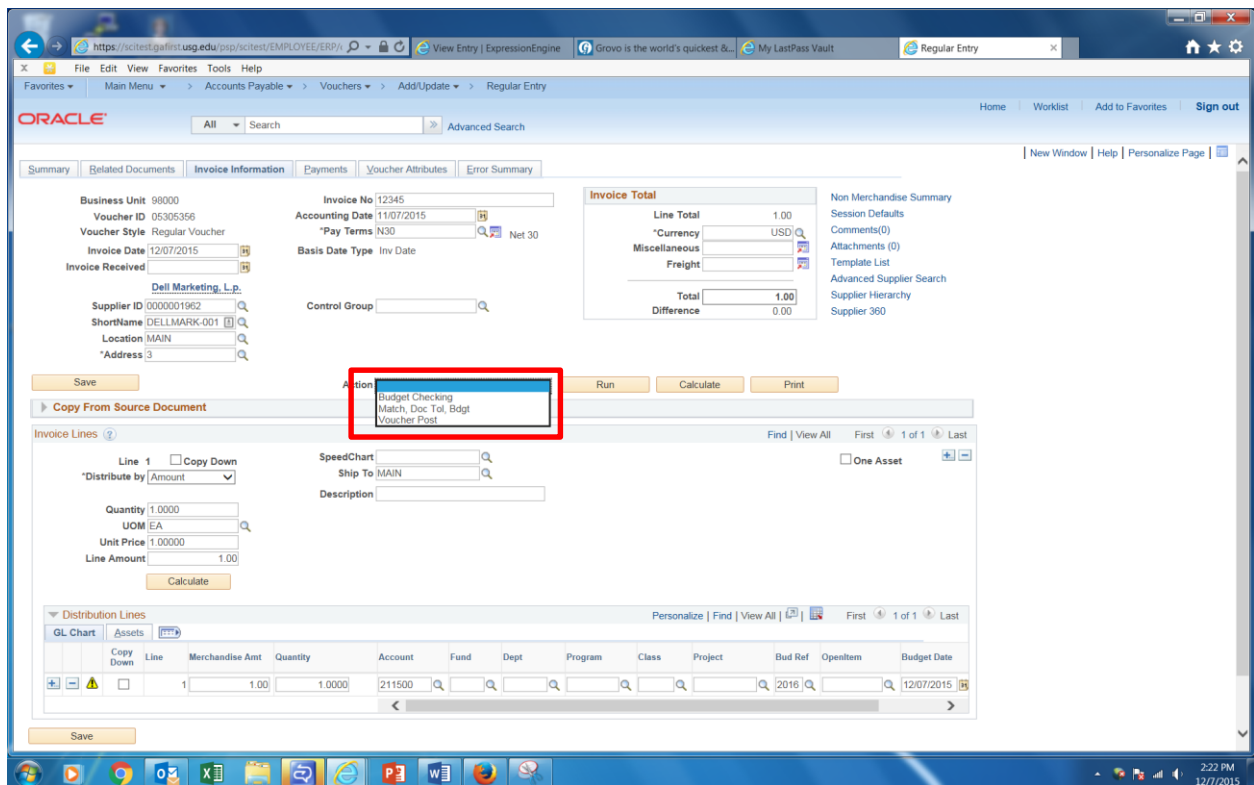


## Asset Management User Preferences

To set User Preferences for the Asset Management module, return to the User Preferences tab and click on Asset Management under Product Preference.

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

ORACLE

**User Preferences**

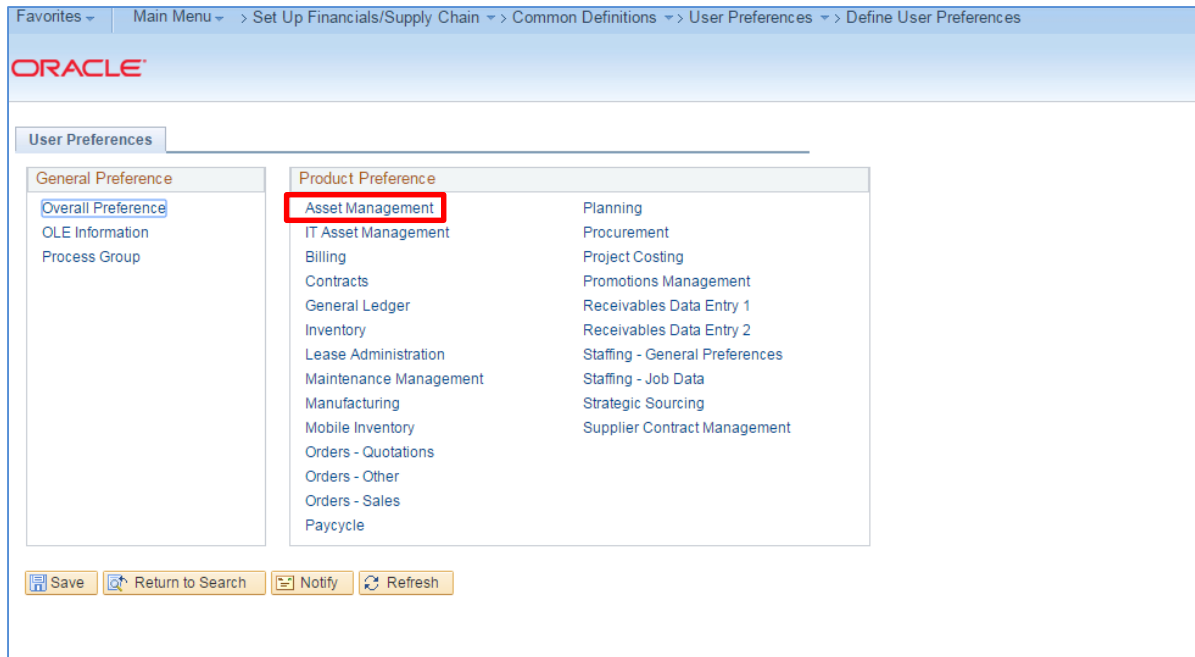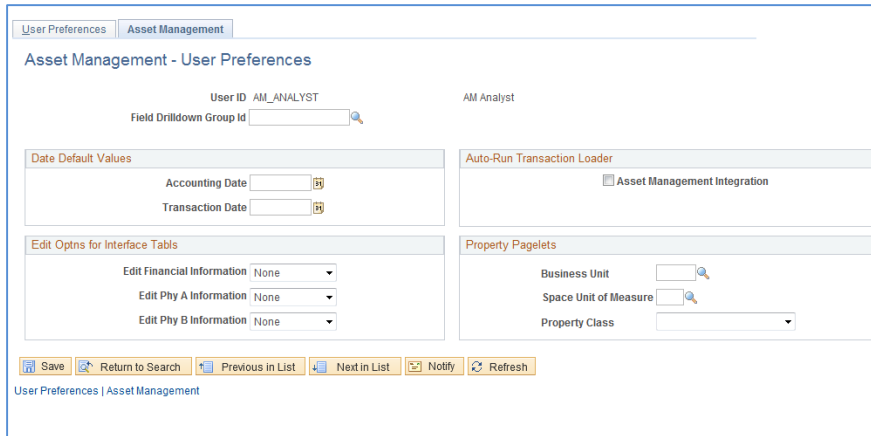| General Preference | Product Preference | |
|---|---|---|
| Overall Preference | Asset Management | Planning |
| OLE Information | IT Asset Management | Procurement |
| Process Group | Billing | Project Costing |
| | Contracts | Promotions Management |
| | General Ledger | Receivables Data Entry 1 |
| | 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

If you are an Asset Management User, you need to make sure that your security administrator has given you the following options:

1. Select a drill-down group to be used by online reporting when filtering data.
2. Supply a **default date** on which you want this transaction distributed to the general ledger. The **accounting date** is validated against the open periods that you establish for Asset Management in the FIN_OPEN_PERIOD table to determine to which period the system posts. (The difference between the transaction date and the accounting date determine whether any prior period depreciation must be calculated. For example, suppose that a computer was acquired and placed in service on 3/16 but was not entered into Asset Management until 8/1. All general ledger periods prior to August are closed. In this case, Asset Management automatically calculated depreciation starting in March and posts it to the general ledger in August.)
3. Click on **Asset Management Integration** to add transactions from Maintenance Management to the transaction loader process.
4. Under **Edit Options for Interface Table**, choose the following information:
   - **Edit Financial Information:**
     - ALL: Select to allow this user to make edits to all financial transaction table entries.
     - Date: Select to allow this user to make edits to transaction and accounting dates on the financial transaction table.
     - None: Select to disallow this user to make edits to any financial transaction table entries.
   - **Edit Phy A Information:**
     - ALL: Select to allow this user to make edits to all physical A table entries.

> ➢ None: Select if this user is not allowed to make any edits to any physical A table entries.
- **Edit Phy B Information:**
  - ➢ ALL: Select to allow this user to make edits to all physical B table entries.
  - ➢ None: Select if this user is not allowed to make any edits to any physical B table entries.

5. Enter the **Business Unit**.
6. Select the **Default Unit of Measure** to access when a user is working with space allocations.
7. Select the **Property Class** to be commonly used by default for this user ID: Site, Building, Floor, Area, or Space.
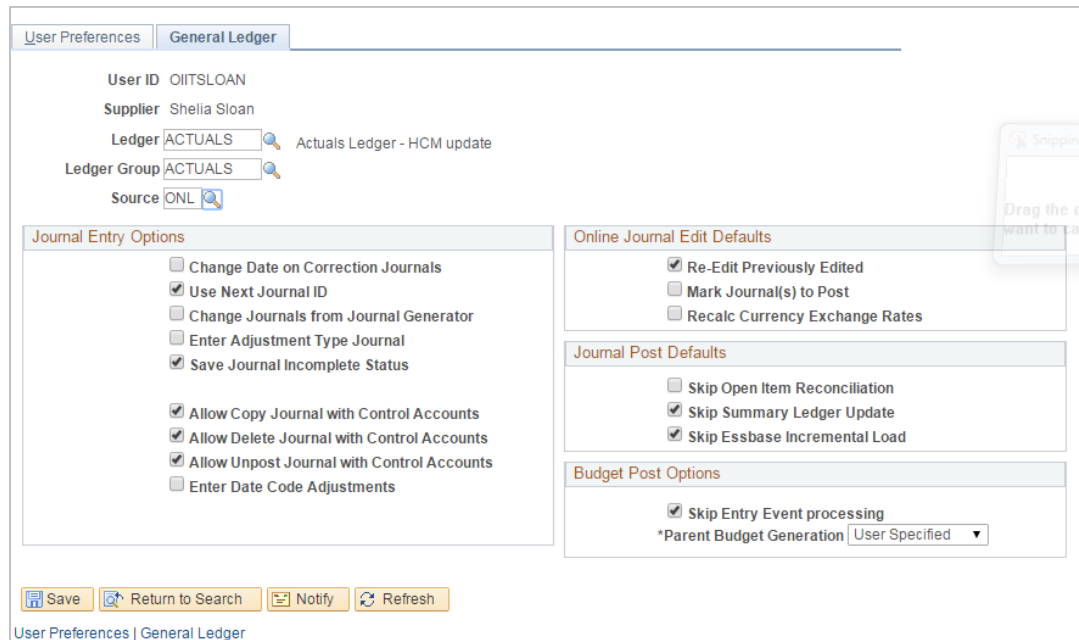8. Click **SAVE**.

**General Ledger User Preferences**

To set User Preferences for the General Ledger module, return to the User Preferences tab and click on General Ledger under Product Preference.



1. The **User ID** and **Name** fields default.

2. Select the "**ACTUALS" Ledger.**

3. Select the "**ACTUALS" Ledger Group**.

4. Select a default **Source** (ONL)

**Journal Entry Options**

1. **Change Date on Correction Journals:** Select to allow the user to change the date on correction journals.

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

3. **Change Journals from Journal Generator:** Select to allow the user to update the ChartField and amounts on the Journal Entry page for a journal created by the Journal Generator process. **Please note:** If Change Journal from Journal Generator is selected, and the ChartField values are changed

and the journal reedited, inconsistencies between the subsystem data and the general ledger data can be created.

4. **Enter Adjustment Type Journal:** Select to allow a user to enter a book code adjustment type journal.

5. **Save Journal Incomplete Status:** 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.

6. **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**

1. **Re-Edit Previously Edited:** Select this button to allow users to reedit journals marked as valid. (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.)

2. **Mark Journal(s) to Post: DO NOT SELCT THIS OPTION** as it bypasses Journal Workflow.

3. **Recalc Currency Exchange Rates:** Not applicable to USG.

**Journal Post Defaults**

1. **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.

2. **Skip Summary Ledger Update:** Select to bypass summary ledger updates for this User ID when posting by clicking the Post Button during Online Journal entry.

3. **Skip Essbase Incremental Load**: Select to bypass the Essbase Incremental Load for a specific user ID during the online journal post process.
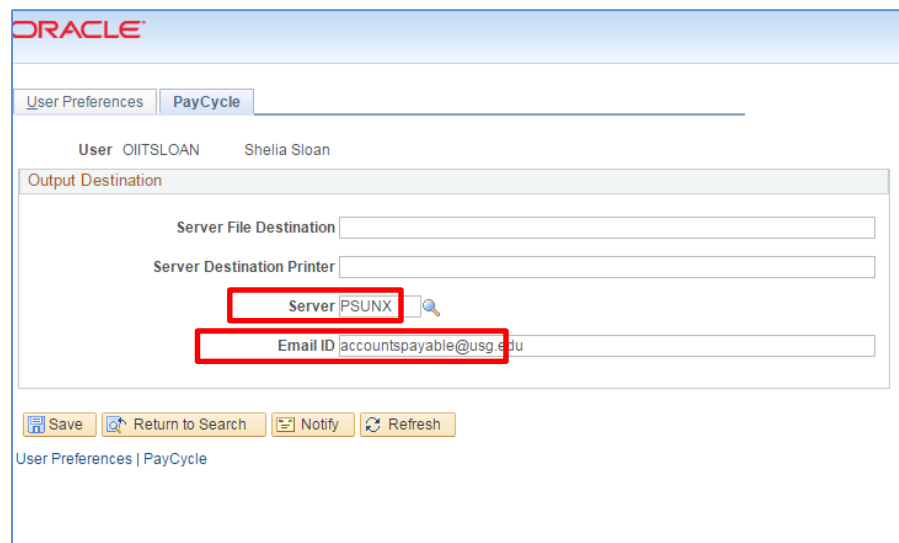
**Budget Post Options**

1. **Skip Entry Event Processing:** Select 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.

2. **Parent Budget Generation:** Select 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 when you never want to 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**

To set User Preferences for PayCycle, return to the User Preferences tab and click on Paycycle under Product Preference.
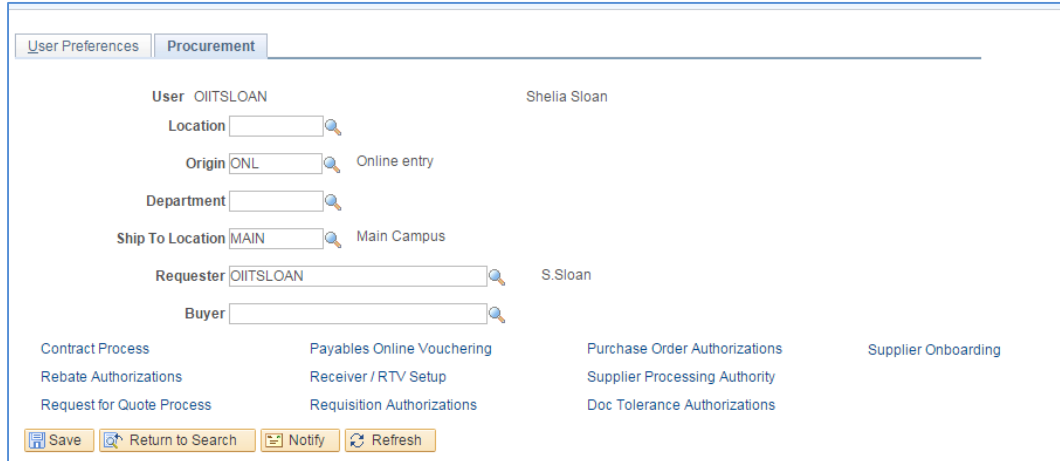


Select the PSUNX server on the user that runs the pay cycle at your institution. The **Email ID** is the From Email account used for the ACH Payment Notifications.

**Procurement**

To work with the Procurement module, return to User Preferences and click on Procurement under Product Preference.

| 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
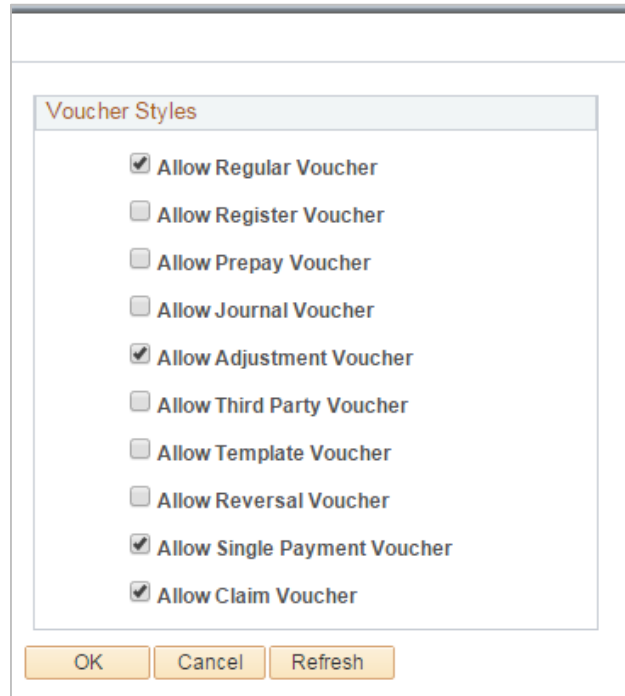
🖫 Save    ⬉ Return to Search    🖺 Notify    🔄 Refresh

1. Enter the **User** and **Name** default.

2. Enter the default **Location** where requested items should be delivered when they are received.

3. Enter the default **Origin**.

4. Enter the **Department** (optional).

5. Enter the **Ship to Location** (optional).

6. Enter the **Requester:** This is Required if the user is a requester.

7. Enter the **Buyer** authorized to enter Purchase Orders (PO's) (optional).

8. Click the **Save** button.

9. Select the **Payables Online Vouchering** link**.**

**Payables Online Vouchering**



1. Enter the **User ID** and **Name** default.

2. **Default Values:** Select a voucher **Origin.**

3. **Operator Voucher Authorities**

   o **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:** Select to enable a user to copy matched and closed POs.

   o **Override Accounting Date Edit:** Select to override the accounting date edit option on the Procurement Control_General Controls page.

   o **Pay Unmatch Amt:** If you select **Pay Unmatched Vouchers,** you can use this field to specify an amount limit.

- o **Security for Voucher Styles:** Click 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
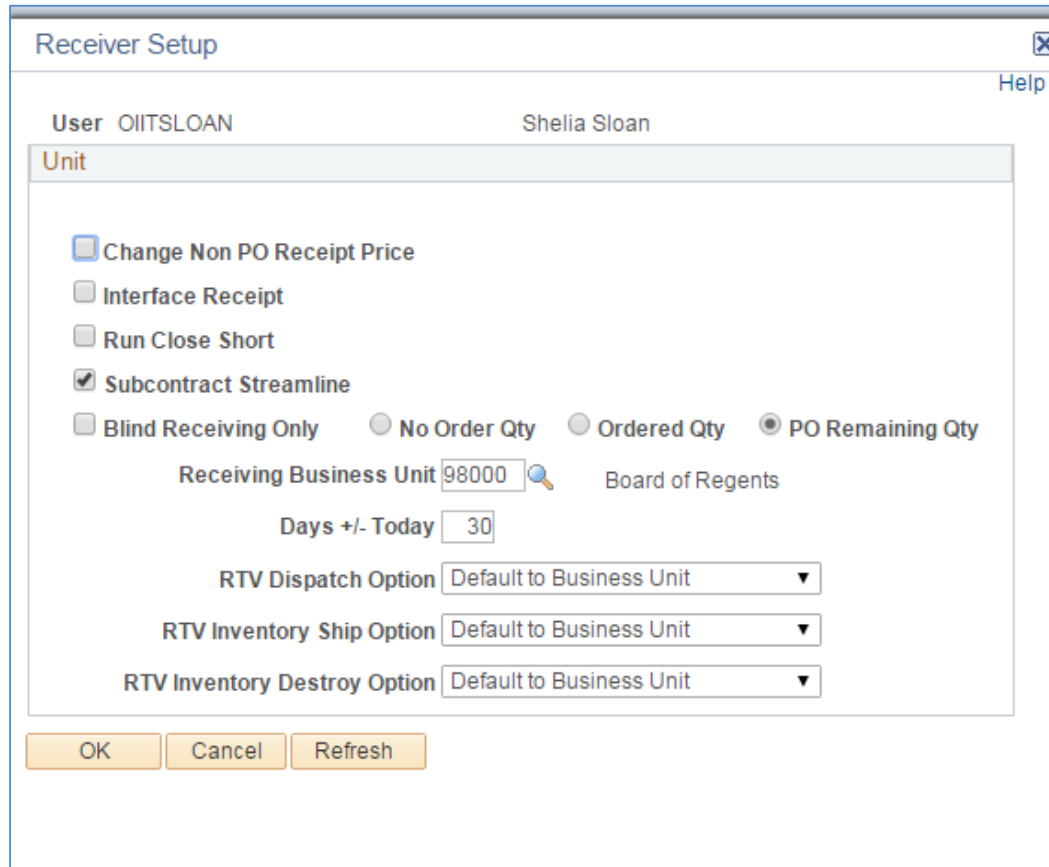
[ OK ]  [ Cancel ]  [ Refresh ]

4. **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:** Select to enable the user to post approved vouchers.

- o **Manually Schedule Payments:** Select to enable the user 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:** Select to enable the user 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:** Select to enable the user 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. (**Please 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.

5. **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.

6. Click **OK.**

7. Select the **Receiver Setup** link.

**Receiver Setup**



1. Enter the **User** and **Name** default.

2. **Change Non PO Receipt Price:** Select to enable the user to change the receipt price for an item on a non-purchase order receipt.

3. **Interface Receipt:** Select to automate the passing of inventory and asset information through the Receiver Interface Push process.

4. **Run Close Short:** Select to call the close short process automatically during the receiver interface push processing.

5. **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.

6. **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.

7. **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.

8. **Ordered Qty:** Select to use the purchase order quantity as the default quantity received.

9. **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.

10. **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.

11. **Return to Vendor (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.

   o 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.

12. **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.

o 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.

  **Please 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.

- *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.

- *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.
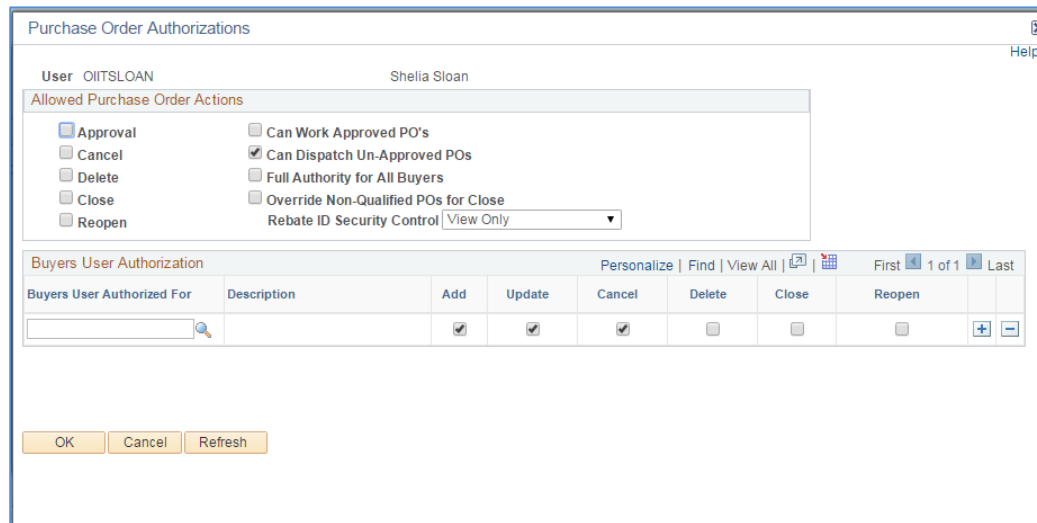
13. **RTV Inventory Destroy Options:** Select the return to vendor destroy option that you want to use as this user's default value for the Inventory Process field on the RTV line. This option is only used by the RTV function when the disposition on the RTV line has a value of Destroy. The system determines 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 the 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.

14. **Select OK**

15. **Select Purchase Order Authorizations** link.

## Purchase Order Authorizations



1. The **User** and **Name** default.

2. **Can Work Approved POs:** Select to change a purchase order that has already been approved or dispatched.

3. **Can Dispatch Un-Approved POs:** Select to enable a user to dispatch purchase orders with a status of pending approval.

4. **Full Authority for All Buyers:** Select to add, update, cancel, and close purchase orders for all buyers

5. **Override Non-Qualified POs for Close:** Select to close unqualified purchase orders.

6. Enter "**View Only**" for the **Rebate ID Security Control.**

7. **Select Approval** if the user is Purchase Order Approver.

## Buyers User Authorization (Optional)

1. Enter **Buyers User Authorized For** the buyers for whom this user can enter purchase orders.

   o Select **"Add"**, **"Update"**, **"Cancel"**, **"Close"** and **"Reopen"** only if the full authority is not selected.

2. Click **OK**

3. Select the **Vendor Processing Authority** link.

**Supplier Processing Authority**
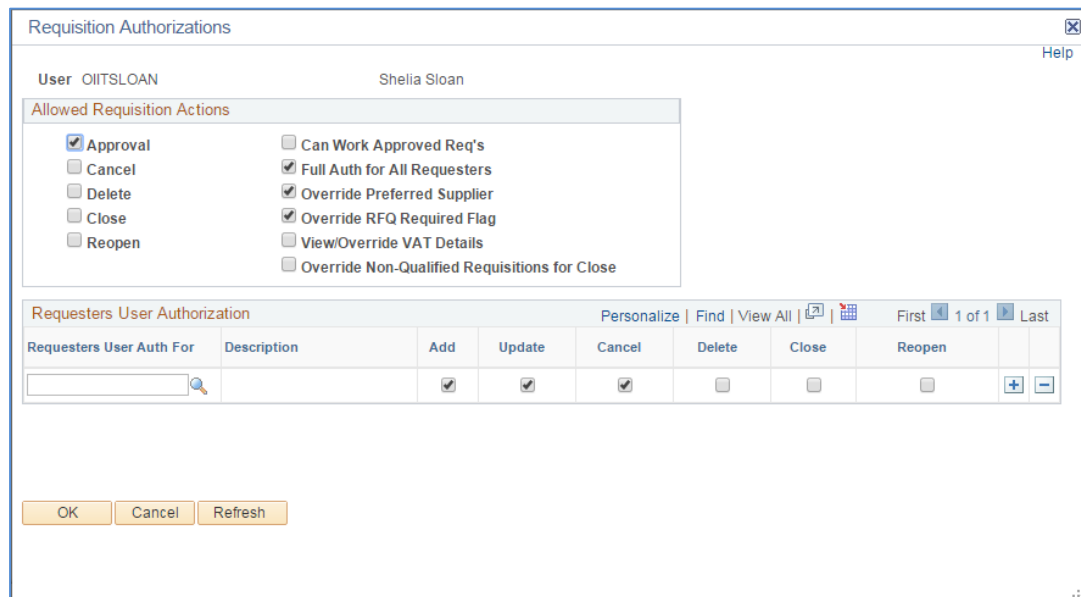


1. The **User** and **Name** default.

2. **Authority to Enter:** Select to allow user to enter a new supplier.

3. **Authority to Approve:** Select to allow user to approve a supplier.

4. **Authority to Inactivate:** Select to allow user to inactivate a supplier.

5. **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.

6. **Supplier Audit Configuration Template**: Select the desired fields to audit and set the Reason flag, which requires Reason Code and comments to be captured.

7. **Supplier Audit Template:** Includes H-Grid (Hierarchical Grid) for Supplier Address, Phone Information, and Supplier Contact Phone fields and 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.

8. Click **OK**.

9. Click the **Doc Tolerance Authorizations link.**

**Document Tolerance Authorizations**
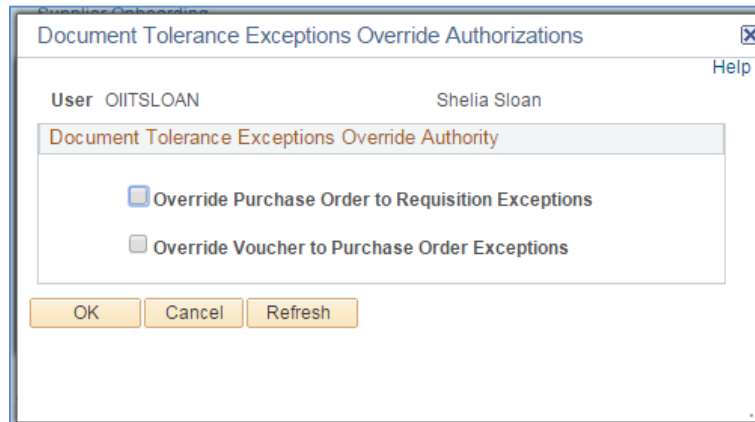


1. **Override Purchase Order to Requisition Exceptions:** Enables you to override document tolerance exceptions that are generated when an encumbrance exceeds the pre-encumbrance during document tolerance checking.

2. **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.

3. **Select OK**

4. Click **the Requisition Authorizations link.**

**Requisition (Req) Authorizations**

1. **Can Work Approved Req's:** Select to enable a user to change a requisition that has already been approved.

2. **Full Auth for All Requesters:** Select to give the user authority to add, update, cancel, delete, and close requisitions for all requesters.

3. **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.

4. **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.

5. **View/Override VAT Details:** Select to view and override VAT details within the requisition component.

6. **Override Non-Qualified Requisitions for Close:** Select to enable a user to close requisitions that are nonqualified for close.

7. **Approval:** Allows a user to Approve Requisitions.

8. **Cancel/Delete/Close/ReOpen:** Allows users to cancel/delete/close or reopen requisitions.

9. **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.

10. **Add/Update/Cancel/Close/Delete/Reopen:** Select to enable the user to add, update, cancel, delete, close, and reopen requisitions for this requester.

11. **Select OK**

12. **Click Save.**

In the previous chapters, you learned to set up users and assign general roles and permissions. In the next chapter, you will learn about workflow.

> **Activity 3:**
>
> 1. Login to FPLAY with your User ID and password from fprod (not the one you created).
>
> 2. Navigate to **Setup Financials Supply Chain > Common Definitions > User Preferences > Define User Preferences**.
>
> 3. Pull up the user ID you created in Activity 2.
>
> 4. Add Overall Preferences and give them Requisition Authorization user preferences.
>
> 5. Give them full authority for all requesters and save.

# Chapter 4: 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 initiate 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 is 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 Approval Framework include approve, deny, hold, and push back. 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. 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
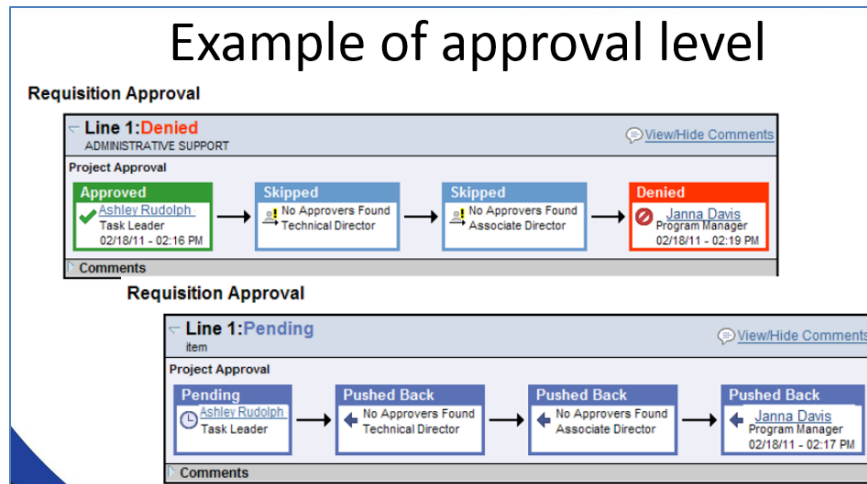
**Workflow Administration**

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 are configured by Module and can be institution specific.

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

**Approval Roles vs. Routing Roles**

We discussed this process in the Introduction; however, it is important to mention it here as well. Because many types of roles exist, approvers will need permission for several different roles to be able to facilitate various types of approvals and workflows. 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 and no permissions. It is used by workflow only for routing purposes. Other ways to route transactions are by query, by SQL, by Employee ID and, for expenses, by User ID.

# Chapter 5: Managing Module Specific Security

Now that you have set up the user and assigned general roles and permissions, you are ready to assign module-specific roles. In this chapter, modules are listed in alphabetical order, except for ePro, which is addressed in Chapter 6.

**Please note:** Since the University System of Georgia has 28 different Business Units, it has to deliver security in a flexible manner. To help institutions segregate duties and define requirements that fit their needs, ITS has created job aids by job function that each institution can use as a guide to create their own version. (They can be downloaded from the Georgia*FIRST* Website: http://www.usg.edu/gafirst-fin/documentation/job_aids/category/security.) The benefit of creating institution-specific job aids is that security administrators can use them to set up user accounts for a specific function without guessing which roles they need each time, segregate duties, and define requirements.

## Accounts Payable

The Accounts Payable module contains voucher security, pay cycle security, 1099 security, workflow security, user preferences, setup and budget, and budget date override security considerations. Tying roles and user preferences to each other provides the full-level access that an end user will need. For example, if you recall in the user preferences section on Procurement/Payables Online Vouchering (Chapter 3), there is a checkbox that says, "Enter Vouchers Only in Groups". 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.

**Please note:** When assigning user roles and security preferences, keep segregation of duties issues in mind. For example, a user should not be able to enter a voucher, approve it, run a pay cycle, and then approve it.

If your institution uses voucher workflow, the following roles will need to be assigned to the appropriate users:
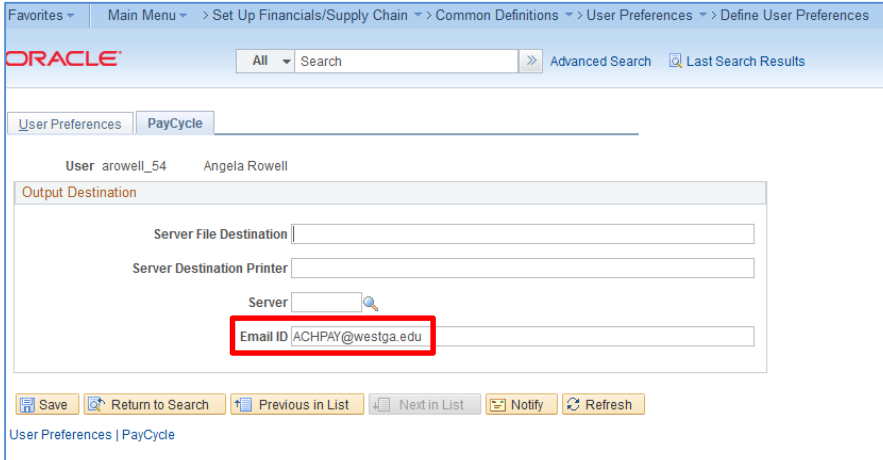
- BOR_VOUCHER_BUD_REF_APPR is the approval role for vouchers with Budget Reference differences.
- BOR_VOUCHER_ASSET_APPR is approval role for vouchers with Asset Issues.
- BOR_AP_ADMINXX (first two digits of institution id) is for escalations or routing issues.

Keep in mind that these three roles 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.

If your institution makes ACH payments and would like all of the "**from email**" addresses to be a generic email address such as accountspayable@XXX.edu, then you must configure a new user preference and setup page. The person who normally runs the pay cycle can enter the generic email address on their user preferences on the screen below. This process must be implemented for only one user.
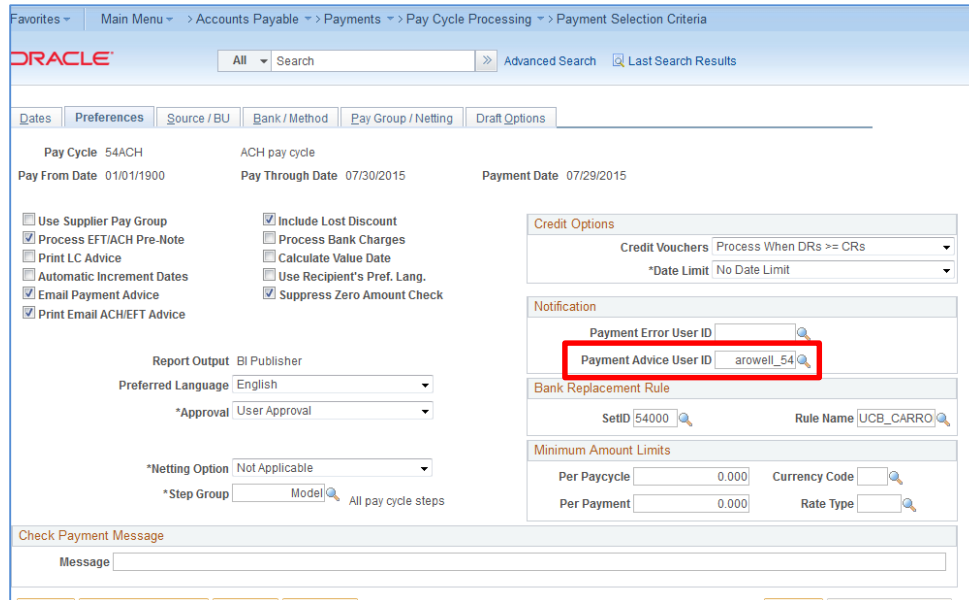
Follow the navigation: **Set Up Financials/Supply Chain > Common Definitions > User Preferences > Define User Preferences.**

1. Click on **PayCycle**.
2. Enter the generic **Email ID**.
3. Click on **Save**.

Now go to the PayCycle Selection Criteria page. Follow the navigation: **Accounts Payable > Payments > Pay Cycle Processing > Payment Selection Criteria**. Enter the same user ID under Payment Advice User ID.



If your Accounts Payables users want to take advantage of the new dashboard/workcenter features, they will need the following roles:

- BOR_AP_DASHBOARD

- BOR_AP_WORKCENTER

- BOR_WORKCENTER_USER role

Other Accounts Payable considerations include the user preferences mentioned in the User Preference Section. These include Process Groups, which allow a user to run budget check, document tolerance, voucher post, and matching directly from the voucher pages, without relying on batch. This also includes Matching process groups that allow a user to override a match exception.

**Please note:** 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. These are located under **Commitment Control > Define Budget Security > Assign Rule to a User**. See Commitment Control Section below. Run the request build process after assigning the rules to the user or the

![Georgia First Financial, Information & Reporting Systems for Tomorrow - A Project of the University System of Georgia]

![PeopleSoft 9.2]

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 4:**

1. Login to FPLAY with your User ID and password from fprod (not the one you created).

2. Navigate to **PeopleTools > Security > User Profiles > Distributed User Profiles**. Create a Payables User ID with the following roles: BOR PeopleSoft User, BOR_FN_ADMIN_REPORTING, ReportSuperUser, BOR_WORKCENTER_USER, BOR_AP_DASHBOARD, BOR_AP_WORKCENTER, and BOR_AP_VOUCHER_ENTRY. Then navigate to user preferences for this user and fill in Overall Preferences and payables preferences. Choose ONL as Origin.

3. Write down User name and password.

---

**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.

**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. Only the following roles should be used for Benefits Reconciliations 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.

| | Description | Comments |
|---|---|---|
| **BOR PeopleSoft User** | FN Base PeopleSoft User | Each user MUST have a base role. |
| **BOR PeopleSoft User-no exp** | BOR PeopleSoft User-no exp | Each user MUST have a base role. |
| **BOR PeopleSoft User –No Tauth** | Base role without travel auths | Each user MUST have a base role. |
| **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. |

**Please note:** 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.

**BOR Payroll Module**

BOR Payroll in PS Financials houses the functionality for users to further process payroll data from the source payroll system. Processes include but are not limited to TIGA reporting of salaries, Year End payroll accruals, 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.

Only the following roles should be used for BOR Payroll 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 role. |
| BOR PeopleSoft User-no exp | BOR PeopleSoft User-no exp | Each user MUST have a base role. |
| BOR PeopleSoft User –No Tauth | Base role without travel auths | Each user MUST have a base role. |
| 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. |

**Budget Preparation (Budget Prep)**

Each year, University System of Georgia 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. Budget Prep then exports the new budget information back to ADP and PeopleSoft Financials. There are six different security roles for Budget Prep. They all begin with BOR_BP and include inquiry and reporting, processing, setup pages, updates and grants.

**Common Remitter**

Common Remitter in PS Financials provides a single-source solution for the collection, reconcilement and remittance of Retirement and Tax Sheltered Annuity payroll deductions. The functionality of the Common Remitter reporting provides data required for monthly, quarterly and annual reporting required for Retirement and Tax Sheltered Annuities 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 is BOR_CR_USER.

**Commitment Control**

Commitment Control enables you to control expenditures 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 institutions set up control budgets, they associate them with a particular General Ledger business unit. They also define the kinds of transactions users check against control budgets. Once their budgets are established, they can check these transactions against their budgets, the passing or failing of the transactions depending on the remaining available budget amount and the degree of budgetary control they set up for their 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, they can override budget checking and allow a transaction to exceed the budget.

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 for the changes to take effect. The BOR_KK_PROCESSES role contains access to this process.

To assign Commitment Control Security Rules to the user, follow the navigation: **Commitment Control > Define Budget Security > Assign Rule to User ID > Assign Commitment Control Security Rule to User ID**.

## Assign Commitment Control Security Rule to User ID

**User ID** OIITSLOAN
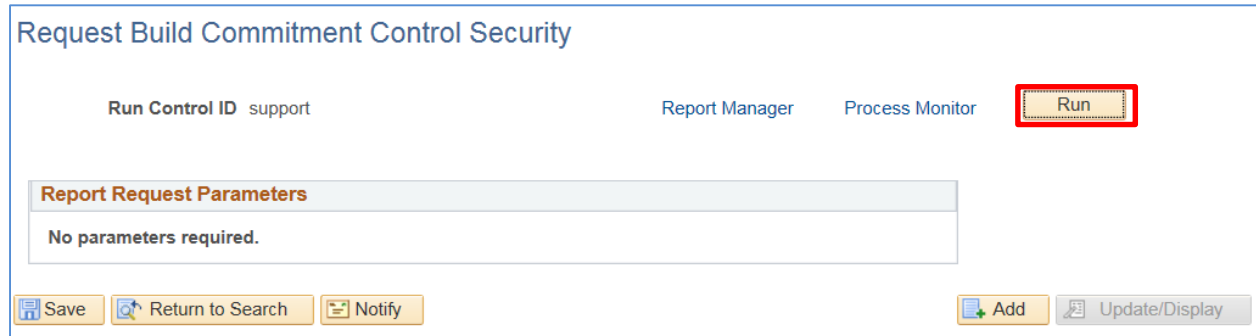
| Security Rules for User | | Personalize \| Find \| View All \| 🗗 \| 🖽 | First ◄ 1-4 of 4 ► Last | | |
|---|---|---|---|---|---|
| **Security Rule** | **Description** | **Attribute** | **Regular/Dynamic** | | |
| BUDG_DT_EX × 🔍 | Budget Date Expenses | Super User | Regular | ➕ | ➖ |
| BUDG_DT_GL 🔍 | Upgrade rule for Budget Date security | Super User | Regular | ➕ | ➖ |
| OVRD_EX 🔍 | Override Expenses | Super User | Regular | ➕ | ➖ |
| OVRD_GL 🔍 | Upgrade rule for Budget Override Security | Super User | Regular | ➕ | ➖ |

💾 Save | 🔍 Return to Search | ✉ Notify | 📥 Add | 📄 Update/Display

**Please note:** A user must be tied to an employee ID to be selected on this page.

Below are the available rules, Budget Date Override, Budget Override, and Bypass Budget broken out by module, as well as two rules that were part of the 9.2 upgrade: BUD_ENTRY (enter budget journals) and BUD_XFER (enter budget transfers only). If a user needs permission to enter both budget Journals and budget transfers, they 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 |

To run the Request Build process, follow the navigation: **Commitment Control > Define Budget Security > Assign Rule to User ID > Request Build**.

**Request Build Commitment Control Security**

|  |  |  |  |  |
|---|---|---|---|---|
| Run Control ID  support |  | Report Manager | Process Monitor | Run |

**Report Request Parameters**

No parameters required.

Save | Return to Search | Notify | Add | Update/Display

ITS has implemented an optional Workflow for Commitment Control Budget Journals. Institutions wishing to implement this workflow need to give their approvers the BOR_KK_BUD_APPR role. In addition, someone at the institution will need the BOR_KK_ADMINXX role (first two digits of institution ID) for escalations or routing issues.

**Activity 5:**
1. Login to FPLAY.gafirst.usg.edu with your fprod User ID and password.
2. Use the Buyer User ID you created above. **** Use Activity 1 User ID instead.
3. Navigate to **Commitment Control > Define budget Security > Assign Rule to User ID**.
4. Give them the BUDG_DT_PO, BUDG_DT_RQ, OVRD_PO and OVRD_RQ rules.
5. Then you must run the _____ process.

**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, which allows travelers to login to the self-service portal from anywhere and complete their expense reports. The Base role of a BOR PeopleSoft User contains expenses access in self-service for expense reports and travel authorizations. (Cash advances 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.

Because this module requires more setup than others, Expenses should have an overall administrator whose role is The BOR_EX_ADMINISTRATION. This individual would maintain default ChartFields and bank accounts for travelers, update delegates, update designates, and potentially maintain approver assignments for workflow.

Expenses uses workflow, although it is setup differently from most modules and lacks flexibility. It does not route via a role, as the other modules do; instead, it routes to the individual who 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 for which 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, he or she is 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 administrator is needed; 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. To get to the Approver Assignment page, follow the navigation: **Setup Financials/Supply Chain > Product Related > Expenses > Management > Approval Setup > Approver Assignments.**

**Approver Assignments**

GL Business Unit 98000

Approver Profile DEPT_MANAGER1

| *User Id | Employee ID | Name | *Department From | *Department To | | |
|---|---|---|---|---|---|---|
| | 0158960 | | 0000000 | 9999999 | + | − |
| | 0158960 | | A000001 | A000088 | + | − |

Personalize | Find | View All | | First 1-2 of 2 Last

Save | Return to Search | Notify | Add | Update/Display

It is important to note that with Expenses and some of the other modules, many employee notifications are sent to the email address listed on the User ID of the employee. Therefore, the Email checkbox on the User Profile, Workflow tab must be selected for the individual to receive notifications.

As with Accounts Payable, you must check user's commitment control rules for Expenses. If your user needs to override a Budget Date or a Budget Exception error on an Expenses Transaction, he or she will need OVRD_EX and/or BUDG_DT_EX commitment control rules, located under **Commitment Control > Define Budget Security > Assign Rule to a User**. Also, don't forget to run the Request Build 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 6:**
> 1. Login to FPLAY-selfservice.gafirst.usg.edu with the User ID you created in Activity 4.
> 2. Navigate to **Employee Self Service > Travel and Expenses Center** and confirm you can see Create Expense Report.

**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. To do this, institutions need to give their approvers the BOR_GL_JRNL_APPR role. Someone at the institution will also need the BOR_GL_ADMINXX role (first two digits of institution ID) for access to escalations or routing issues. If you want to take advantage of the new dashboard/workcenter features, users will need the BOR_GL_DASHBOARD role, the BOR_GL_WORKCENTER role, and the BOR_WORKCENTER_USER role.

Other General Ledger considerations include user preferences, as mentioned in the User Preference Section. Don't forget to check user's commitment control rules for GL. If users need 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. To assign this rule, follow the navigation: **Commitment Control > Define Budget Security > Assign rule to a User**. See Commitment Control Section above.

You must 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 End processes and reports, TIGA Processing, ChartField Configuration, and journal entry/processing.

**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 Roles**

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. The table below contains the 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. <ul><li>If your institution is implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ_SCI.</li><li>If your institution is not implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ.</li></ul> |
| 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**

Just as 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. To do this, follow the navigation: **Set Up Financials/Supply Chain > Product Related > Procurement Options > Purchasing > Buyer Setup.**

**Buyer Setup**

Enter any information you have and click Search. Leave fields blank for a list of all values.

| Find an Existing Value | Add a New Value |

▼ **Search Criteria**

Buyer [begins with ▼] [                    ]
Description [begins with ▼] [                    ]
☐ Case Sensitive

[ Search ]  [ Clear ]   Basic Search 🔍 Save Search Criteria

1. Select the **Add a New Value** tab.

2. Enter the buyer's **User ID** in the **Buyer** field.

3. Click the **Add** button.

| Buyer Setup | Dashboard |

**Buyer Setup**

Buyer OIITPAGE                                    T.Page OIIT          *Status [Active ▼]

Department SetID [73000] 🔍     Department [        ] 🔍      **Default PO Status**
ShipTo SetID [73000] 🔍         Ship To [MAIN] 🔍            ○ Open
Location Set ID [73000] 🔍      Location [        ] 🔍        ⦿ Pending Approval/Approved
PO Origin SetID [SHARE] 🔍      Origin [ONL] 🔍
Phone [                    ]                                   PO Dispatch Signature Location:
Fax [                    ]                                     [                    ]

💾 Save   🔍 Return to Search   📧 Notify                              ➕ Add   📄 Update/Display

Buyer Setup | Dashboard

1. Ensure the status is set to **Active**.

2. In the **Department SetID** field, enter/select your institution's **SetID**.

3. 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.

4.  In the **ShipTo SetID** field, enter/select your institution's **SetID**.

5.  In the **ShipTo** field, enter/select this Buyer's default **Ship to location**.

6.  In the **Location SetID** field, enter/select your institution's **SetID**.

7.  In the **Location** field, enter/select this Buyer's primary **location**.

8.  In the **PO Origin SetID** field, enter/select **SHARE**.

9.  In the **Origin** field, enter/select **ONL**.

10. If desired, enter a phone and fax number.

11. Set the **Default PO Status** to **Pending Approval/Approved**.

12. Click the **Save** button.

**Please note:** If the Buyer will also be creating Requisitions, they must be set up on the Requester Setup Page also. See ePro chapter below.

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 users want to use desktop receiving, they must have the BOR_PO_RECV_EPRO role.

ITS has reduced the number of roles associated with Supplier activity and controlled it with 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 through user preferences. For instance, if you want a user to be able to modify an existing supplier but not add a supplier, they would get the BOR_PO_VENDORS_MAINT role, but not the Add User Preference. See more details in the User Preferences section above.

In 9.2, Purchasing workflow changed from using Route Controls to using the Approval Framework. The approval role for Purchase Orders with Budget Reference differences is BOR_PO_BUD_REF_APPR. The approval role for Purchase Orders with Asset Issues is BOR_PO_ASSET_APPR. The role for escalations or routing issues is BOR_PO_ADMINXX (XX is the first two digits of institution ID). Keep in mind that these three roles 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 documents on the Georgia*FIRST* website.

> **Activity 7:**
>
> 1. Login to **FPLAY.gafirst.usg.edu** with your fprod User ID and password.
>
> 2. Create a new **Buyer User ID**, with the roles listed above in this section.
>
> 3. Navigate to **Product Related, Procurement Options, Purchasing,** and **Buyer Setup** and set them up as a buyer for your business unit.
>
> 4. Then Navigate to **User Preferences** and add their User ID under the buyer box on **Procurement User Preferences**, giving them full authority for all buyers as well as the approval User preference.

# Chapter 6: eProcurement (ePro)

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

**Types of Roles Involved**

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 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 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 or build their own shopping carts.
- **Approvers:** These users are set up to approve ePro requisitions.
- **Buyers:** These users are responsible for ensuring that 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 other 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 occasionally need to work with the ePro Administrator to perform maintenance, such as updating email addresses, on these users. In addition, because Workflow is such a critical piece of eProcurement, the user setup is very important.

**Requester Security Roles**

The first step in ePro is setting up security roles for requesters, users who create ePro requisitions either from Special Request items or from shopping carts in the Georgia*FIRST* Marketplace.

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, also known as 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. <br>• If your institution is implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ_SCI and BOR_EP_MAINT_REQ. <br>• If your institution is not implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ only. |
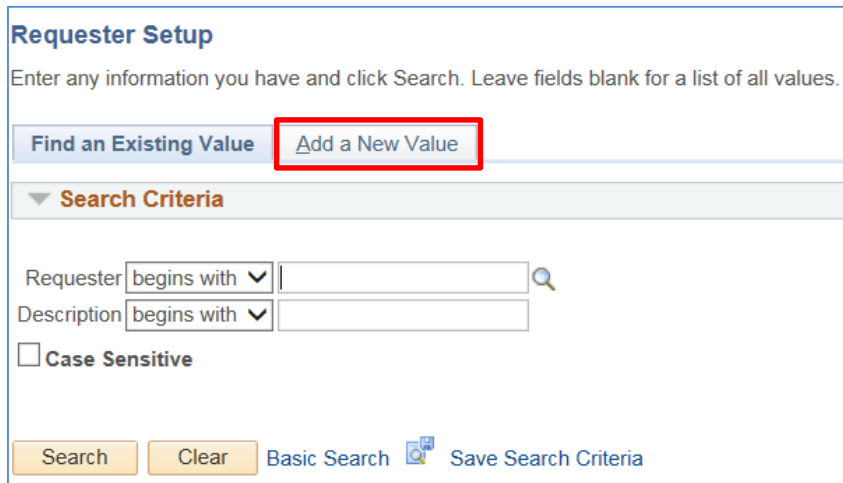
**Please note:** If the requester will also be a Shopper, give them the BOR_CAT_Requester role only. Users should not have multiple "BOR_CAT" roles.

**Please note:** If you want to cut off your requester's access to create requisitions at year end, give them 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 then set up the individual as a Requester. If you have a user who is only a Shopper, he or she will still need the Requester Setup page completed so that the person they assign their carts to can choose them as the requester once the item in their cart is turned into a requisition.

To set up a Requester, follow the navigation: **Set Up Financials/Supply Chain > Product Related > Procurement Options > Purchasing > Requester Setup**.



1. Select the **Add a New Value** tab.

2. Enter the requester's **User ID** in the **Requester** field.

3. Click the **Add** button.

**Requester Setup**

| | | | |
|---|---|---|---|
| Requester | OIITPAGE | T.Page OIIT | *Status Active ▼ |

**Requisition Defaults**

ShipTo SetID 71000 🔍          Ship To CS1115 🔍

*Location SetID 71000 🔍          *Location MAIN 🔍

PO Origin SetID SHARE 🔍          Origin ONL 🔍

Currency USD 🔍 Dollar

Phone _____

Fax _____

☐ Override Auto Item Substitute

☐ Use Only Assigned Catalogs

☐ Consolidate with other Reqs

**Requisition Status**
- ○ Open
- ● Pending Approval

☑ Price Can Be Changed on Order

☐ Defaults Inventory BU

**ChartFields**          Personalize | Find | View All | 🔲 | 🔳

| GL Unit | Account | Fund | Dept | Program | Class | Project | Bud Ref |
|---|---|---|---|---|---|---|---|
| 71000 🔍 | 🔍 | 🔍 | 🔍 | 🔍 | 🔍 | 🔍 | 2016 🔍 |

**Catalog Information**          Personalize | Find | View All | 🔲 | 🔳          First ◀ 1 of 1 ▶ Last

| Default | *SetID | *Catalog ID | Description | |
|---|---|---|---|---|
| ☑ | SHARE 🔍 | NIGP_TREE 🔍 | NIGP CODE TREE | ➕ ➖ |

💾 Save    🔍 Return to Search    📧 Notify          ➕ Add    📝 Update/Display

---

1. Ensure the status is set to **Active**.

2. In the **ShipTo SetID** field, enter your institution's **SetID**.

3. In the **ShipTo** field, enter/select the default **Ship To address** for this Requester.

4. In the **Location SetID** field, enter your institution's **SetID**.

5. In the **Location** field, enter/select the default **Location** for the Requester.

6. In the **PO Origin SetID** field, enter/select **SHARE**.

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

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

9. Enter a phone and fax number if desired.

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

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

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

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

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

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

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

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

18. Leave the Account field blank.

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

---

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

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

22. Leave the Use Only Assigned Catalogs checkbox blank.

23. **Save** the page.

Don't forget to set up user preferences as well. These were defined in an earlier user preference section. You also have buyer set up to complete, but we will cover that in the next section, which is covered in the Purchasing section of the previous chapter.

A critical component of 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?**

When a Requester builds a requisition in ePro, each item on a requisition is placed on its own requisition line. Theoretically, each line in a requisition can be charged to a different set of ChartFields. As a result, each line on a requisition may have different approval paths.

The 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 who 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, such as approvers for assets, Information Technology (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, five approval stages can be used for eProcurement requisitions. Keep in mind that each one has different security workflow roles that control the routing of the transaction. Each approver will still need the BOR_EP_REQ_APPROVE role in addition to the workflow roles, since it contains the page access to allow approval. The approval stages are as follows:

### Stage 1: Department and Project Approval

Each requisition line must be charged to a Department. In addition, they can also 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

There are three approvals in this stage, all of which are optional. These approvals are all based on the Fund Code entered on the transaction.

The first one 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. Each Agency Fund Approver will have the role BOR_AGENCY_FUND_APPR.

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, available to institutions that route requisitions that have Fund Code 20000 to a user with the BOR_GRANT_APPR role. This individual/s can be different from the individual on the project ChartField.

If your institution employs any of these approval stages, then multiple approvers can be set up. The institution will determine whether all approvers must approve the requisition or whether only one from the group of

multiple approvers has to approve it. If the corresponding fund code is not used on a requisition line, the system bypasses this approval stage.

**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 have 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 whether 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 four, approvals are based upon the type of item being requested. Within this stage, there are seven potential approval paths, all optional.

- **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 whether 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 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 the item. For requisition line items not generated from the Marketplace, the Requester enters the proper Category ID. For 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 whether 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, also an optional one, 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 whether only one from the group of approvers must approve it. In addition, institutions may identify additional NIGP codes for chemical approval and 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, it may have multiple approvers in this path. The institution will determine whether all Facilities Planning and Design approvers must approve the requisition or whether 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. The system routes any requisition line for a computer hardware or software purchase or service (based on NIGP Code) to the IT Approver.

  An IT Approver must have the role "BOR_IT_APPR". If your institution chooses to use the IT Approver path, it can have multiple approvers. The institution will determine whether all IT Approvers must approve the requisition or whether 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, also optional, is for the University Relations Approver. The system routes any requisition line that relates to media contact, logo use or copyright items (based on NIGP code) 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, it can assign multiple approvers. The institution will determine whether all University Relations Approvers must approve the requisition or whether 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, which will automatically route the line 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, it can assign multiple approvers. The institution will determine whether all Furniture Approvers must approve the requisition or whether 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, it can assign multiple approvers in this path. The institution will determine whether all Human Resource Approvers must approve the requisition or whether 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, it can assign multiple approvers in this path. The institution will determine whether all Pharmaceutical Drug Approvers must approve the requisition or whether 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 also choose whether all Buyer Approvers must approve the requisition or whether 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**

An approver has built-in deadlines by which he or she must 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 in PeopleSoft Financials. The Worklist is a queue that holds items waiting for approval. Once an approver works a transaction, it is removed from that 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 plans to be out of the office for an extended period of time and, therefore, unable to work requisitions, 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 (see Chapter 3). Each institution is able to customize the number of days as to when the system will send reminder emails and escalate a requisition.

**ePro Administrators**

ePro Administrators must be set up in the system with the correct security roles to enable them 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. The ePro Admin Security Roles are as follows:

| Role Name | Purpose |
|---|---|
| BOR PeopleSoft User | Basic PeopleSoft User access |
| BOR_EP_ADMINXX | Enables the ePro Admin to manage ePro Workflow; "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 be set up 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). The Basic Approver Security Roles are as follows:

| 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. <br> • If your institution is implementing the Georgia*FIRST* Marketplace, use BOR_EP_MAINT_REQ_SCI. <br> • 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 the following to 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 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_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.

In addition to setting up security roles and user preferences for department and project managers, you also need to set up 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**".

When you complete the Manager ID field, the Manager Name field should populate as well, once you tab out of the field. To update a department manager ID, follow the navigation: **Set Up Financials/Supply Chain > Common Definitions > Design ChartFields > Define Values > ChartField Values > Department**.



1. On the **Find an Existing Value** page, enter/select the **Department ID** in the **Department** field.
2. Click the **Search** button.
3. Select the **Department** you want to update.



1. Ensure the Department status is **Active**.
2. Click the **Correct History** button.
3. Select the **Manager ID** look up icon.

4. Enter the last name of the Department Manager in the **Last Name** field.

5. Click the **Look Up** button.

6. Select the correct **User ID** for the Department Manager.

7. Click the **Save** button.

### Additional Department Managers

The way Workflow is initially setup, you can specify only one User ID for your department manager. If your institution wishes to have multiple department approvers, you must 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.

**Please 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 your institution's SetID. After adding your institution for the first time, you can add additional approvers through the **Find an Existing Value** tab (using your SetID).

For each additional approver, you 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 approvers for the necessary departments.
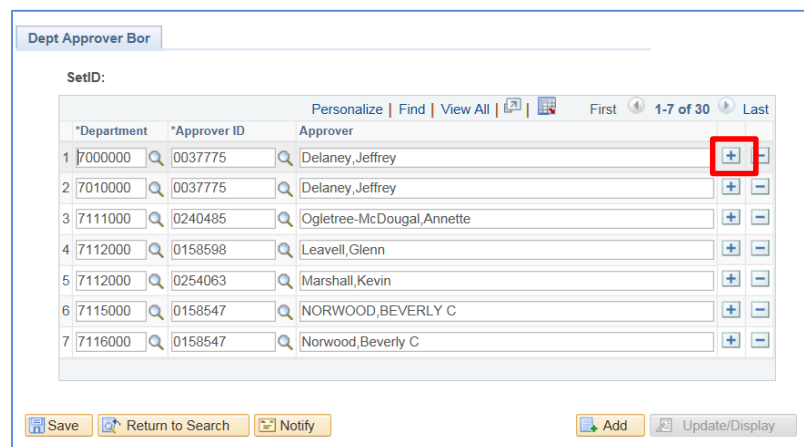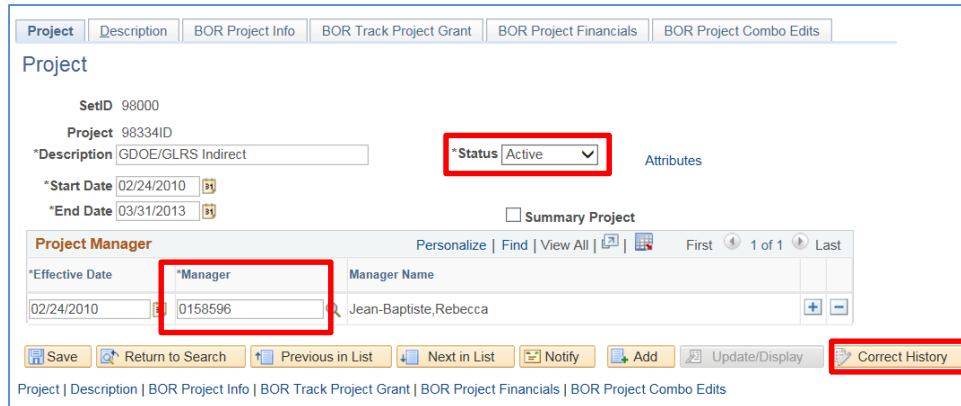
To update additional department managers, follow the navigation: **Set Up Financials/Supply Chain > Common Definitions** > **Design ChartFields > Define Values > Department Approver**.

1. 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.
2. Enter/select your institution's **SetID** and click **Add** or **Search**.
3. On a blank row, enter/select the **Department ID** for the Department you want to add an additional approver for.
4. Enter/select the additional Approver's **UserID** in the Approver ID field. **Tab** out of the field to populate the Approver field.
5. To insert additional approvers, select the **Add a New Row** button and repeat steps 8 & 9.
6. 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". Once you complete the **Manager ID** field, the Manager Name should populate as well, once you tab out of the field. To update a project manager ID, follow the navigation: **Set Up Financials/Supply Chain > Common Definitions >** **Design ChartFields > Define Values > ChartField Values > Project**.

1. On the **Find an Existing Value** page, enter/select the **Project ID** in the **Project** field.

2. Click the **Search** button.

3. Select the **Project** you want to update.

4. Ensure the Project status is **Active**.

5. Click the **Correct History** button.

6. Select the **Manager ID** look up icon.

7. Enter the last name of the Project Manager in the **Last Name** field.

8. Click the **Look Up** button.

9. Select the correct **User ID** for the Project Manager.

10. Click the **Save** button.

---

**Activity 8:**

Login to FPLAY.gafirst.usg.edu with your fprod User ID and password.

Once logged in, use the User ID you created in Activity 1 and do the following:

1. Navigate to **Product Related > Procurement Options > Purchasing > Requester Setup** and set the user up as a requester for your business unit.

2. Then Navigate to User Preferences and add their User ID under the requester box on Procurement User Preferences.

# Chapter 7: Managing Query Security

One of the most important areas of security is PeopleSoft Query (Query) because queries give administrators control over the processes and data to which users have access. Three levels of security exist:

- **Table-level security** is set by using PeopleSoft Query to build SQL queries to specify the records (tables) the user is allowed to access when building and running queries.
- **Row-level security** controls access to individual rows of data stored within application database tables through security views and enables you to specify the data that a particular user is permitted to access.
- **Field-level security** is set using PeopleCode, the proprietary language used in the development of PeopleSoft applications, to restrict access to particular fields or columns within application tables.
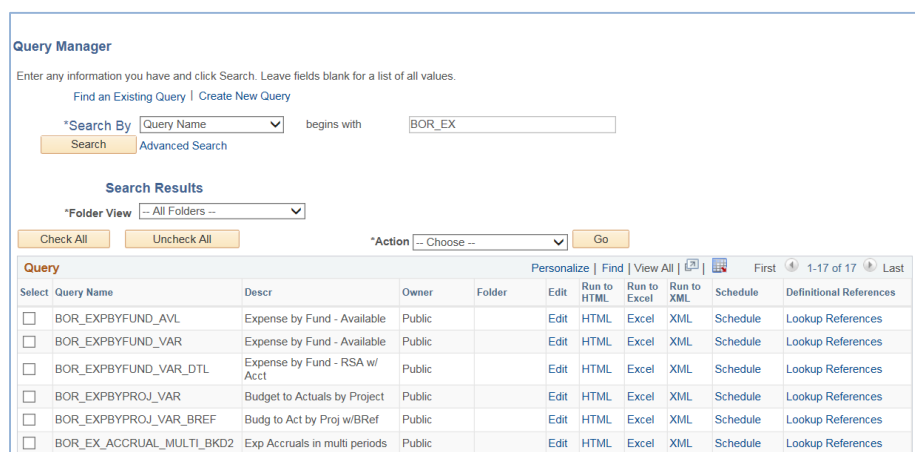
Query helps you build SQL statements to retrieve information from application tables by taking advantage of a user's security settings, row-level security, and primary permission list. The Query Profile defines what features of Query operations the user has. The table below explains the five levels of 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. | BOR_PT_QRY_VIEWER |
| **Level II** | Query Manager-User has the ability to create and run Private queries and run Public queries. The user will only be able to create and run queries on records that they have access to through Access Group security. | BOR_PT_QRY_PRIVATE |
| **Level III** | Query Manager-User has the ability to run only Public queries. The user will only be able to run those Public queries on records that they have access to through Access Group security. | Not applicable to USG |
| **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 | BOR_PT_QRY_PUBLIC |
| **Level V** | Query Manager/Monitor-User has the ability to create and run both Private and Public queries. The user will be able to create and run only queries on records that they have access to through Access Group security. Query monitor allows a user to gather statistics on Query use. | BOR_PT_QRY_ADMIN |

For a user to run a query, they must have authorization to access the records behind the query. Most records are included in the role BOR_PT_QRY_ALLACCGRPS. However, certain records have been broken out into other roles for sensitive data considerations. BOR_QRY_SENSDATA and BOR_PT_BUD_PREP are examples. If a user tries to pull up a query in Query Manager and cannot see it, they probably do not have access to the records in that query. To gain access, the security administrator has to give them access to one of the sensitive data roles.

**Navigation to Query Manager Components**

To perform query operations, follow the navigation: **Reporting Tools > Query > Query Manager.**



Query components will be enabled for the user to match the level of query operations for which they are authorized through the query profile permissions.

**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, if you want users to review personal data for employees in their department but not for people in other departments, you assign access to the PERSONAL_DATA table but enforce row-level security so that users see only 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

![GEORGIA FIRST FINANCIAL, INFORMATION & REPORTING SYSTEMS FOR TOMORROW - A Project of the University System of Georgia]

PeopleSoft 9.2

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 set up for row-level security. For example, to restrict user access to data from their own department, the view would select rows only from the underlying table in which the DEPTID matches the user's DEPTID rows.

**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 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 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.

# Chapter 8: 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 set up 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.

4) Place the employee ID on the General tab under the User ID alias field and attach the User ID beside it.

5) Update the user's security request form to a "terminated" status and document the appropriate signatures.

6) 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 that this person was responsible for are complete).

7) 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.

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

**Terminated User Query**

To run a terminated user query, follow the navigation: **Reporting Tools > Query > Query Manager > BOR_SEC_TERMINATED_USERS**.

This query will return users in the PeopleSoft Financials system that have an unlocked User ID and 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, 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 is the source HR system.

**Activity 9:**

Login to fplay using your prod user name and password.

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

   BOR_TERMINATED_USERS_QUERY.

2. Follow the procedures above if you have any results on the query. Pick only 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 has an electronic system to track security requests and approvals, you must periodically review the requests and recertify 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 at least once a year, all user accounts set up at your institution are reviewed for:

- Level of access (too much or not enough)

- Type of access (have they changed job functions)

- 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 stored electronically and should include items such as segregation of duties review, user preferences review, and budget security reviews.

**Segregation of Duties Query**

To run a segregation of duties query, follow the navigation: **Reporting Tools > Query > Query Manager >**

**SEGREGATE_DUTY_BOR**.

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

| Records | Query | Expressions | Prompts | Fields | Criteria | Having | Dependency | Transformations | View SQL | Run |
|---|---|---|---|---|---|---|---|---|---|---|

Proc/Func Name = Add/Edit Vendor, Business Unit=54000

View All | Rerun Query | Download to Excel | Download to XML                 First 1-13 of 13 Last

| | ACTIONNAME | User ID | Unit | Create Req Role | Approve Req Role | Create PO Role | Approve PO Role | Create Voucher Role | Approve Voucher Role | Cut Check Role | Add/Edit Vendor Role | Approve Vendor Role |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Add/Edit Vendor | arowell_54 | 54000 | | | | | | | BOR_AP_PAYCYCLE_APPROVE | | |
| 2 | Add/Edit Vendor | arowell_54 | 54000 | | | | | BOR_AP_VOUCHER_ENTRY | | | | |
| 3 | Add/Edit Vendor | cbentle3 | 54000 | | | | | | | | | BOR_PO_VENDORS_APPROVE |
| 4 | Add/Edit Vendor | csmith_54 | 54000 | BOR_EP_MAINT_REQ | | | | | | | | |
| 5 | Add/Edit Vendor | csmith_54 | 54000 | BOR_EP_MAINT_REQ_SCI | | BOR_PO_MAINTAIN | BOR_PO_APPROVE | | | | | |
| 6 | Add/Edit Vendor | lelliott | 54000 | BOR_EP_MAINT_REQ | | | | | | | | |
| 7 | Add/Edit Vendor | lelliott | 54000 | BOR_EP_MAINT_REQ_SCI | | BOR_PO_MAINTAIN | BOR_PO_APPROVE | | | | | |
| 8 | Add/Edit Vendor | sparker | 54000 | BOR_EP_MAINT_REQ | | | | | | | | |
| 9 | Add/Edit Vendor | sparker | 54000 | BOR_EP_MAINT_REQ_SCI | BOR_EP_REQ_APPROVE | BOR_PO_MAINTAIN | BOR_PO_APPROVE | | | | | |
| 10 | Add/Edit Vendor | ssmither | 54000 | BOR_EP_MAINT_REQ | | | | | | | | |
| 11 | Add/Edit Vendor | ssmither | 54000 | BOR_EP_MAINT_REQ_SCI | | | | | | | | BOR_PO_VENDORS_APPROVE |
| 12 | Add/Edit Vendor | tcannon | 54000 | BOR_EP_MAINT_REQ | | | | | | | | |
| 13 | Add/Edit Vendor | tcannon | 54000 | BOR_EP_MAINT_REQ_SCI | | BOR_PO_MAINTAIN | BOR_PO_APPROVE | | | | | |

If a user appears on this query, it does not necessarily mean that they are in violation. However, the campus security administrator should do further research to ensure that the user's access is not a violation and should then 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 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 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 10:

Login to fplay using your prod user name and password.

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

2. Choose Create Requisition.

3. Make note of user.

The User Preference Report is located at **Set Up Financials/Supply Chain > Common Definitions >User Preferences > User Preferences Report.** It can be run for an individual user or for all users.

![GEORGIA FIRST — FINANCIAL, INFORMATION & REPORTING SYSTEMS FOR TOMORROW — A Project of the University System of Georgia]

![PeopleSoft 9.2]

**Activity 11:**

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.

To run the Commitment Control Security report, follow the navigation: **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 12:**

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 may be several tasks. These tasks will be listed out in 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 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 assigns budget security to a user, that user still doesn'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 that they have the Matching Process groups.

**Q. What does the error message "No origin was found on your operator profile" mean?**

A. This error message is typically found when trying to enter a voucher. Go to the User Preferences for the user and go to Payables. Click and enter ONL in the origin field.

**Q. When I try to enter a User ID on the Expenses Approver Assignments page< I receive an error message saying that this person is a multi-campus user; however, I know they are not.**

A. Many times the issue is not with the person you are trying to enter. Sort the page by Employee ID. If there is a UserID that does not have an associated employee ID, then you need to replace the former user with the new one. If it is truly a multi-campus user issue, contact ITS.

**Q. When my ePro approver tires to approve the transaction in their worklist, they receive an error message saying that they 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. How do I assign Security Administrator to another employee?**

A. Create the User ID and assign all necessary roles. Then 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, although I have tried searching for their User ID and adding their User ID.**

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 allows a user to do only password resets?**

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

**Q. When I click save to reset a password for a user, I get 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 become 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 role probably existed in version 8.9 but is no longer available. Submit a ticket to ITS to remove it.

**Q. A user cannot get to Report Manger to retrieve reports.**

A. Assign them the BOR_FN_ADMIN_REPORTING role.

**Q. A user cannot pull up items from their worklist.**

A. The user has "Use standard layout mode" enabled under personalization options. The default is "Accessibility features off". Have the user return it to "Accessibility features off".

**Q. When a user tries to post a budget journal, they get the Security Error under Budget Header Status.**

A. If you receive 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 located under **Commitment Control > Define Budget Security > Assign Rule to User ID**. Once they assign this role, they will need to run the request build process that is in the same menu structure. You will need to reenter the budget journal.

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