PeopleSoft Security v9.1
Training Manual

1.0 Course Introduction

1.1 Objective

Developed specifically for PeopleSoft v9.1 Financials (FMS) functional end users, PeopleSoft Security v9.1 training quickly introduces students to the building blocks of PeopleSoft security. The goals of this class are achieved through a mixture of live PeopleSoft Security component walk-throughs and a hands-on exercise that allows students to apply security to a PeopleSoft FMS module as transactions are entered and processed.

1.2 Audience

The target audience is Functional end-users and/or Functional Project Team members. Please note that this is not a comprehensive class geared for Developers or Security Administrators.

1.3 Prerequisite

Intro to PeopleSoft v9.1 Financials Training

1.4 Duration

Two Days

1.5 Instructor Background

SpearMC Senior PeopleSoft Financials Consultant

1.6 Pre-class Items & Training Material

- SPEARMC Memo to Class and Expectations
- PeopleSoft Security Training Agenda
- PeopleSoft Security Training Manual
    - **Technical:** Not necessarily covered in this class – good future reference for tech users
    - **Notes:** Items of interest based on recent PeopleSoft v9.1 Security roll-outs
    - **Discussion Points:** Specific SpearMC points to discuss topic being covered
- PeopleSoft Security Training Exercise
- PeopleSoft Security Process Flow Example
- PeopleSoft Security Strategy and Considerations

2.0 Overview of PeopleSoft Security

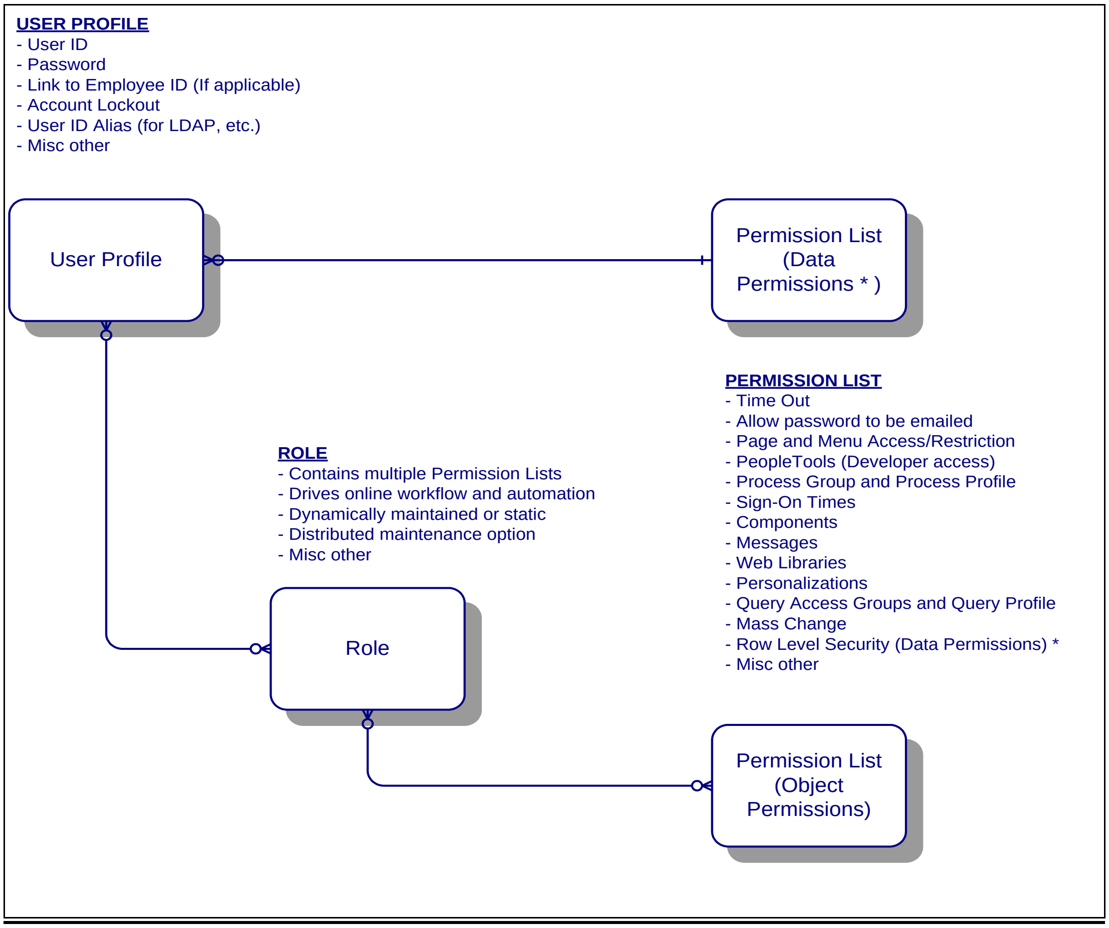
PeopleSoft security in v9.1 uses a **role-based security model.** This is considered a security leading practice as it allows the flexibility and robustness to maintain the integrity of the system and its data.

The concept of **decentralizing security** is also supported in PeopleSoft, as it makes it more convenient for non-security administrators (e.g. super users, managers) to assign roles to end-users without exposing all security administration functionality. This course will cover the core components of PeopleSoft Security specifically geared towards non-security administrators.

A security definition refers to a collection of related security attributes that are created using PeopleTools Security. The three main PeopleSoft security definition object types are:

- User Profiles, Roles and Permission Lists

Each user of the system has an individual User Profile, which in turn is linked to one or more Roles. To each Role, you can add one or more Permission Lists, which ultimately control what a user can and can't access. So a user inherits permissions through the role.


USER PROFILE
- User ID
- Password
- Link to Employee ID (If applicable)
- Account Lockout
- User ID Alias (for LDAP, etc.)
- Misc other
User Profile
Permission List (Data Permissions *)
PERMISSION LIST
- Time Out
- Allow password to be emailed
- Page and Menu Access/Restriction
- PeopleTools (Developer access)
- Process Group and Process Profile
- Sign-On Times
- Components
- Messages
- Web Libraries
- Personalizations
- Query Access Groups and Query Profile
- Mass Change
- Row Level Security (Data Permissions) *
- Misc other
ROLE
- Contains multiple Permission Lists
- Drives online workflow and automation
- Dynamically maintained or static
- Distributed maintenance option
- Misc other
Role
Permission List (Object Permissions)

The panel below (Figure 1) shows the Base Navigation Page for PeopleSoft Security.

Navigation: *PeopleTools > Security*

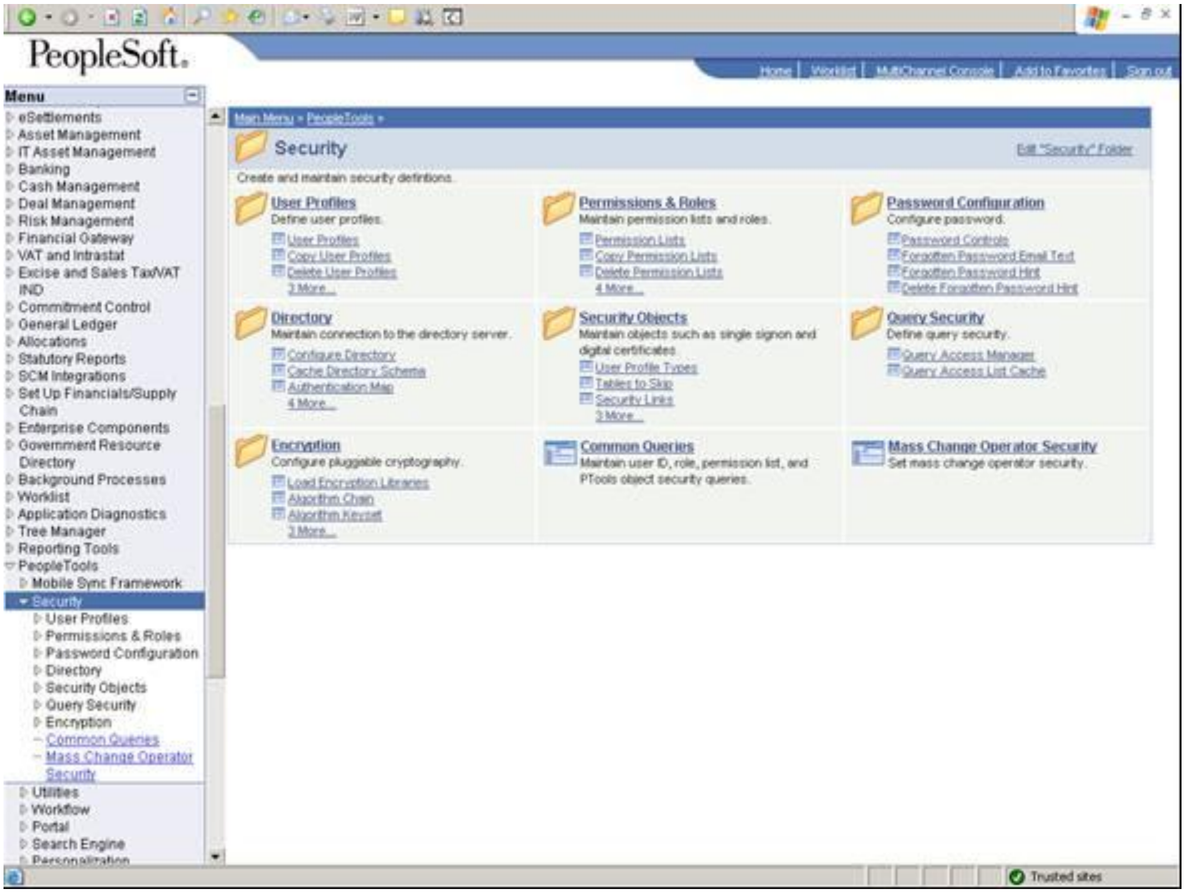


Figure 1

2.1 User Profiles Overview

A User Profile describes a particular user of the PeopleSoft system. This description includes everything from the low-level data that PeopleTools requires, such as Language Code, to application-specific data, such as the Table SetIDs a user is authorized to access within the PeopleSoft applications. User Profiles also maintain the Roles that are assigned to the user.

Technical: User Profiles are different from the application data tables, such as PERSONAL_DATA, that also store information about people. User Profiles are relevant when a user interacts with the system by logging in, viewing a worklist entry, receiving an email, and so on. Application data tables are involved with the core application functionality, such as payroll processing and expense sheet processing, not with system-wide user interaction.

2.2 Roles Overview

Roles are assigned to User Profiles. Roles are intermediate objects that link User Profiles to Permission Lists. Multiple Roles can be assigned to a User Profile, and you can assign multiple Permission Lists to a Role. Some examples of Roles might be Employee, Manager, Customer, and so on.

A Manager is also an Employee. Roles enable us to mix and match access appropriately.

Technical: There are two options when assigning roles; assign Roles manually or assigning them dynamically. When assigning roles dynamically, you can use PeopleCode, Light Directory Access Protocol (LDAP), and Query rules to assign User Profiles to Roles programmatically

2.3 Permission Lists Overview

Permission Lists are lists, or groups, of authorizations that you assign to Roles. Permission Lists store Sign-on times, Page access, PeopleTools access, and so on.

A Permission List may contain one or more types of permissions. The more types of permissions in a Permission List the more modular and scalable your implementation.

A User Profile inherits *most* of its permissions through the roles that have been assigned to the User Profile.

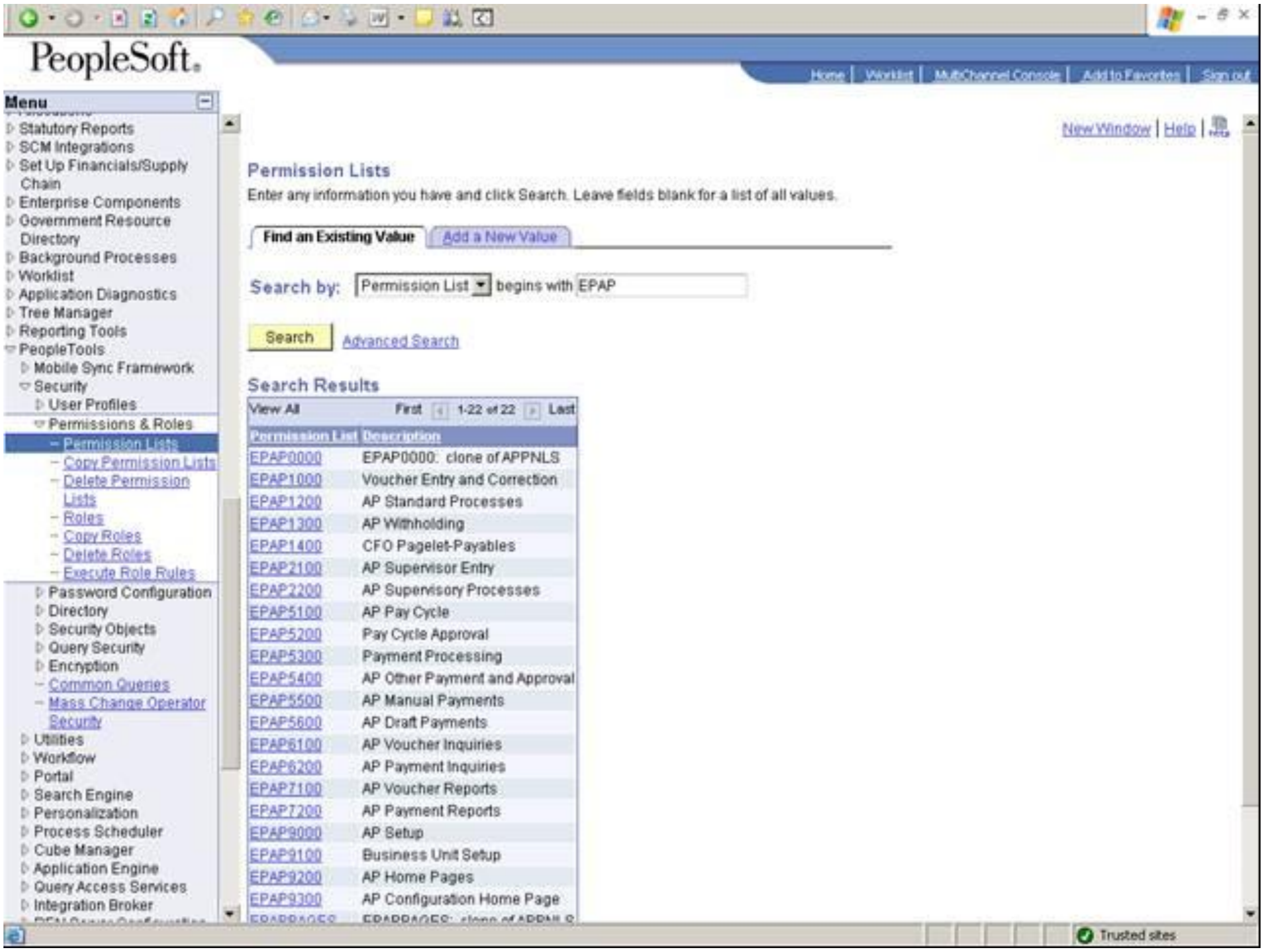
Data permissions, or row-level security, appear either through a Primary Permissions List or a Row Security Permissions list.

Review / Q&A: How are the different agencies currently handling security? Start thinking about similarities and/or differences that currently exist vs. the PeopleSoft model.

3.0 Permission Lists

Permission Lists (Figure 2) are the building blocks of end user security authorizations. Before beginning to define User Profiles and Roles, you typically create our list of Permission Lists. When defining Permission Lists, consider each type of Role and User Profile to which they will be attached.

Important to Note: PeopleSoft comes delivered with many pre-defined Permission Lists. SpearMC recommends that SpearMC make use of as many of these permission lists as possible.



Permission Lists

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

Search by: Permission List begins with EPAP

Search Results

View All First 1-22 of 22 Last

Permission List	Description
EPAP0000	EPAP0000: clone of APPNLS
EPAP1000	Voucher Entry and Correction
EPAP1200	AP Standard Processes
EPAP1300	AP Withholding
EPAP1400	CFO Pagelet-Payables
EPAP2100	AP Supervisor Entry
EPAP2200	AP Supervisory Processes
EPAP5100	AP Pay Cycle
EPAP5200	Pay Cycle Approval
EPAP5300	Payment Processing
EPAP5400	AP Other Payment and Approval
EPAP5500	AP Manual Payments
EPAP5600	AP Draft Payments
EPAP6100	AP Voucher Inquiries
EPAP6200	AP Payment Inquiries
EPAP7100	AP Voucher Reports
EPAP7200	AP Payment Reports
EPAP9000	AP Setup
EPAP9100	Business Unit Setup
EPAP9200	AP Home Pages
EPAP9300	AP Configuration Home Page

Figure 2

A Permission List may contain any number of the following permissions: (i) page permissions, (ii) signon times, (iii) process permissions, component interface permissions, and so on.

Important to Note: You will focus primarily on Page Permissions and Process Permissions for this class.

PeopleSoft Security is built off of the Permission List > Role > User Profile concept. Remember that a role may contain numerous permissions and a user profile may have numerous roles assigned to it.

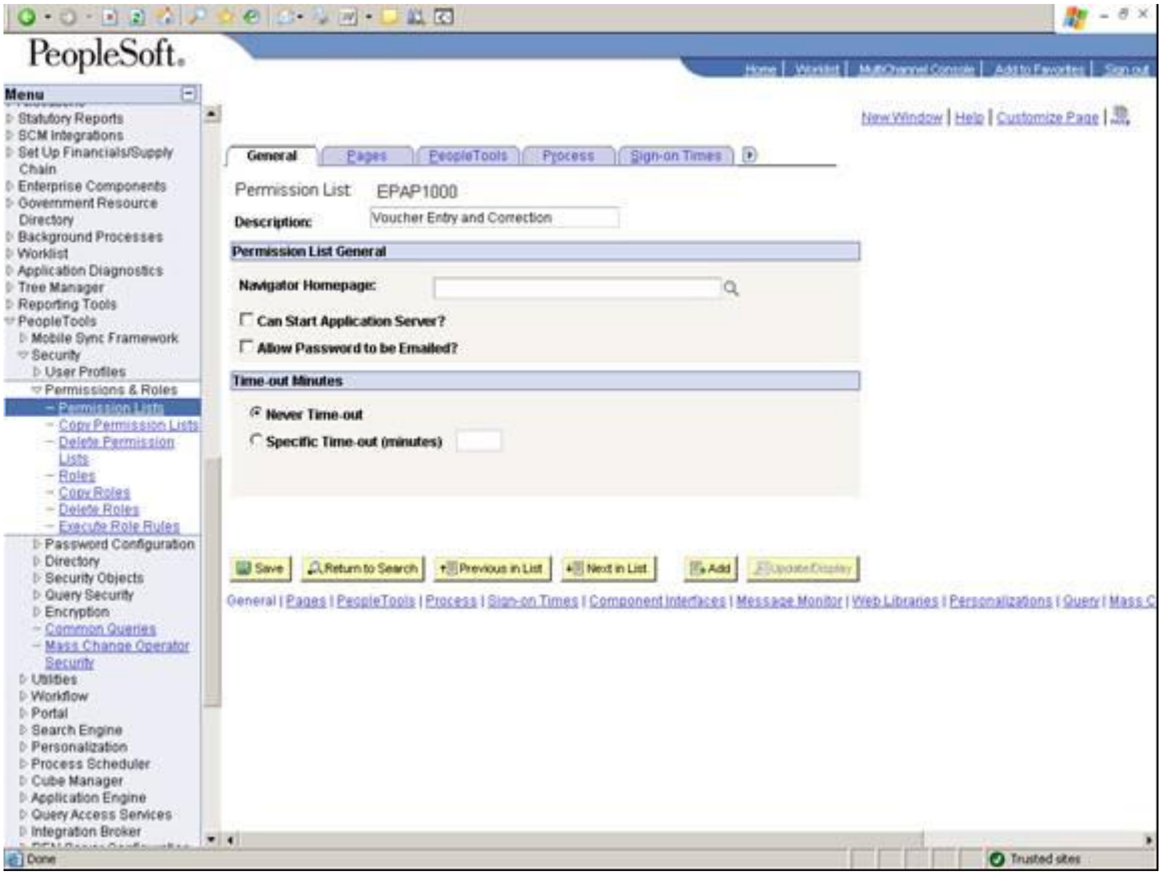
Because permission lists are applied to users through roles, a user inherits all the permissions assigned to each role to which the user belongs. The user's access is determined by the combination of all of the roles.

Review / Q&A: Make sure you understand the concept of PeopleSoft Security. At a high-level think of Permission Lists as the component that allows a user what navigation is available to them and what process they can run.

Theoretically, you can create a Permission List tailored for each and every Role, and that Permission List could contain a permission of every category from General to Libraries. Alternatively, you can use a more modular or "mix-and-match" approach. This approach involves numerous, specific Permission Lists that you can add and remove to Role definitions. As a general rule, permission lists should be assigned to roles so that the common user has in between 10 to 20 lists.

Technical: When you set component permissions and your library permissions, there is a "View Content References" link that enables you to be able to view the content references pointing to a given component or script. PeopleTools automatically propagates changes to permission lists to the content references. When copying (cloning) a permission list, the content references associated with the copied permission list are also copied. Also, when deleting a permission list, the content references associated with that permission list are also removed.

Hands-on: Select the PeopleSoft delivered role for Voucher Entry and Correction (Figure 3).



Permission List EPAP1000

Description: Voucher Entry and Correction

Permission List General

Navigator Homepage:

☐ Can Start Application Server?

☐ Allow Password to be Emailed?

Time-out Minutes

● Never Time-out

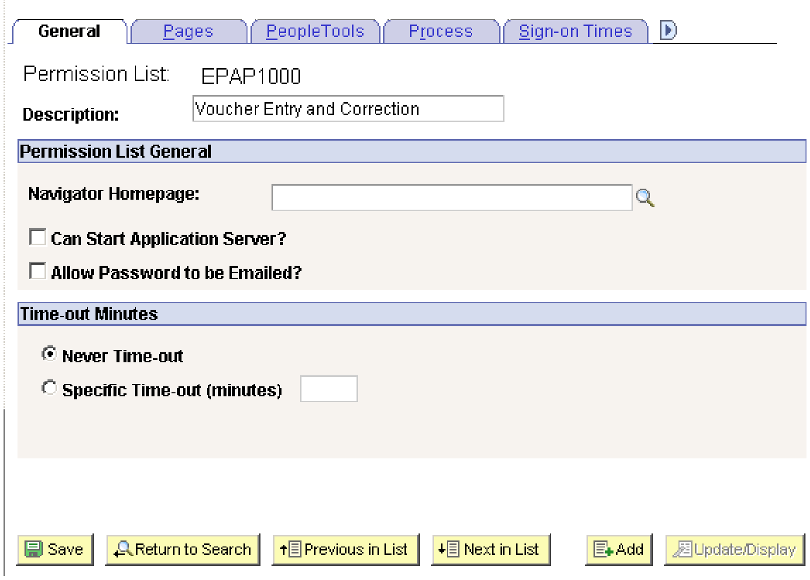
○ Specific Time-out (minutes)

Figure 3

3.1 Pages Used to Define Permission Lists

Page Name	Navigation	Usage
General	PeopleTools, Security, Permission Lists and Roles, Permission Lists, General	Set the general or miscellaneous attributes and system defaults. **Note:** Any General options will usually be set at a higher level default Permission List for all users.
Pages	PeopleTools, Security, Permission Lists and Roles, Permission Lists, Pages	Set page permissions.
PeopleTools	PeopleTools, Security, Permissions and Roles, Permission Lists, PeopleTools	Grant access to the standalone PeopleTools, like Application Designer, and grant access for specific operations within PeopleTools.
Process	PeopleTools, Security, Permissions and Roles, Permission Lists, Process	Specify to what capacity a user, or Role, can modify certain Process Scheduler settings.
Sign-on Times	PeopleTools, Security, Permissions and Roles, Permission Lists, Sign-on Times	Specify when users are authorized to sign on to the PeopleSoft system.
Component Interface	PeopleTools, Security, Permissions and Roles, Permission Lists, Component Interface	Grant access to any Component Interfaces that a user may need to use to complete business transactions.
Message Monitor	PeopleTools, Security, Permissions and Roles, Permission Lists, Message Monitor	Set permissions for administrators to monitor the messages and the components involved in the application messaging system.
Your Libraries	PeopleTools, Security, Permissions and Roles, Permission Lists, Your Libraries	Set your library permissions.
Personalizations	PeopleTools, Security, Permissions and Roles, Permission Lists, Personalizations	Enables to decide which personalizations users will be able to use and which ones they can customize.
Query	PeopleTools, Security, Permissions and Roles, Permission Lists, Query	Control what query operations a user can perform and what data they can access while they are using Query.
Mass Change Security	PeopleTools, Security, Permissions and Roles, Permission Lists, Mass Change	Set mass change security permissions.
Audit	PeopleTools, Security, Permissions and Roles, Permission Lists, Audit	Inquire when a permission list was last updated and by whom.

3.2 Setting General Permissions



Permission List: EPAP1000

Description: Voucher Entry and Correction

Permission List General

Navigator Homepage:

□ Can Start Application Server?

□ Allow Password to be Emailed?

Time-out Minutes

● Never Time-out

○ Specific Time-out (minutes)

Description

Use to more uniquely identify the definition. There is a 30-character limit for this value.

Navigator Homepage

A graphic representation of a business process that is displayed by the PeopleSoft Navigator. For each security profile definition, you can specify a map to be displayed upon startup.

If this is the user profile's Navigator Homepage permission list, the system gets this value at runtime.

Can Start Application Server?

Selecting this check box enables a user profile with this permission to start a PeopleSoft application server. This may be a user ID used solely for starting the application server. At least one of the permission lists associated with the user ID used for starting the application server must have this permission selected.

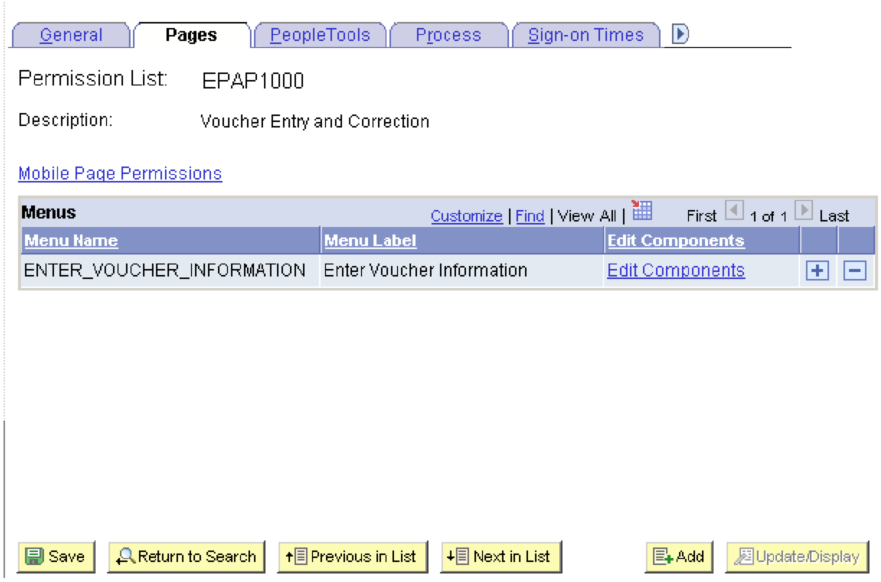
Allow Password to be Emailed?

When a user forgets their password, PeopleSoft provides the option to have it sent to the user through email.

Time-Out Minutes

Time-out minutes are the number of minutes of inactivity allowed at a terminal before the system automatically signs the user off the PeopleSoft online system. Inactivity means: no mouse clicks, keystrokes, import, file print, or SQL activity. The default time-out minutes setting is Never Time-out.

3.3 Setting Page Permissions



Permission List: EPAP1000

Description: Voucher Entry and Correction

Mobile Page Permissions

Menus

Menu Name	Menu Label	Edit Components
ENTER_VOUCHER_INFORMATION	Enter Voucher Information	Edit Components

Mobile Page Permissions This link enables to grant access to your mobile application pages.

Menu Name Prompts against all of the menu names in the database. Add the desired menu names to the list. This reflects the definition name in PeopleSoft Application Designer.

Menu Label Shows the menu label associated with the PeopleSoft Application Designer menu name.

Edit Components Enables you to drill into the components and grant access of varying degrees to specific pages.

Page permissions refer to the pages to which a user has access. Pages are contained within components, which are ultimately contained within a menu name.

To grant access to a particular page, determine the component it is in and the menu name the component falls under. This enables you to drill down to the appropriate page in this interface—beginning at the menu name level.

Note: To find the name of a page, you can use CTRL+J feature while accessing the page with the browser, or use the Find Definition References feature in Application Designer

After you add Menu Name, you grant access to its components and pages item on an item-by-item basis

In PeopleSoft applications, menu items represent components. If a component consists of more than one page, then selecting the menu item opens another layer with more items—individual pages.

Review / Q&A: You recommend that SpearMC use or at least begin building Permission Lists based on what is delivered. Click Edit Components to see all the components involved in just one Permission List.

Review / Q&A: Look at some of the other delivered PeopleSoft permission lists that deal with the AP module.