



# PeopleTools 8.12 Security PeopleBook

PeopleTools 8.12 Security PeopleBook

**SKU MTSCr8SP1B 1200.**

**PeopleBooks Contributors:** Teams from PeopleSoft Product Documentation and Development.

Copyright © 2001 by PeopleSoft, Inc. All rights reserved.

Printed in the United States of America.

All material contained in this documentation is proprietary and confidential to PeopleSoft, Inc. and is protected by copyright laws. No part of this documentation may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, including, but not limited to, electronic, graphic, mechanical, photocopying, recording, or otherwise without the prior written permission of PeopleSoft, Inc.

This documentation is subject to change without notice, and PeopleSoft, Inc. does not warrant that the material contained in this documentation is free of errors. Any errors found in this document should be reported to PeopleSoft, Inc. in writing.

The copyrighted software that accompanies this documentation is licensed for use only in strict accordance with the applicable license agreement which should be read carefully as it governs the terms of use of the software and this documentation, including the disclosure thereof.

PeopleSoft, the PeopleSoft logo, PeopleTools, PS/nVision, PeopleCode, PeopleBooks, Vantive, and Vantive Enterprise are registered trademarks, and *PeopleTalk* and "People power the internet." are trademarks of PeopleSoft, Inc. All other company and product names may be trademarks of their respective owners.

# Contents

## About This PeopleBook

Before You Begin .....	xii
Related Documentation .....	xii
Documentation on the Internet .....	xii
Documentation on CD-ROM .....	xii
Hardcopy Documentation .....	xiii
Typographical Conventions and Visual Cues .....	xiii
Comments and Suggestions .....	xv

## Chapter 1

### Understanding PeopleSoft Security

PeopleSoft Online Security .....	1-2
Signon and Time-out Security .....	1-2
Page and Dialog Security .....	1-3
Batch Environment Security .....	1-3
Process Security .....	1-3
Reporting Security .....	1-4
Object Security .....	1-4
Application Data Security .....	1-4
Query/Table-Level Security .....	1-5
Row-Level Security .....	1-5
Field Security .....	1-5
PeopleSoft Internet Architecture (PIA) Security .....	1-6
PeopleSoft Security Definitions .....	1-6
User Profiles .....	1-7
Roles .....	1-7
Permission Lists .....	1-8
PeopleSoft Authorization IDs .....	1-10
User IDs .....	1-10
Connect ID .....	1-10
Access IDs .....	1-11
Symbolic ID .....	1-11
Before you get Started .....	1-11

Understanding PeopleSoft Signon .....	1-12
Directory Server Integration.....	1-13
Authentication and Signon PeopleCode.....	1-13
Single Signon .....	1-14
Implementation Options .....	1-15
Authentication .....	1-15
PeopleSoft-based Authentication .....	1-15
Directory-based Authentication .....	1-15
Role Assignments.....	1-15
Static.....	1-16
Dynamic .....	1-16
Cross System Synchronization.....	1-17
Maintain Security Interface .....	1-17
Use.....	1-18
Setup.....	1-19
Process.....	1-20

## Chapter 2

### Working with Permission Lists

Getting Started .....	2-3
General Permissions .....	2-4
Description .....	2-5
Navigator Homepage.....	2-5
Can Start Application Server?.....	2-5
Allow Password to be Emailed .....	2-5
Time-Out Minutes .....	2-6
Page Permissions .....	2-6
PeopleTools Permissions .....	2-9
Object Permissions.....	2-10
Tools Permissions .....	2-12
Change Control .....	2-12
Build and Data Administration .....	2-13
Language Translations .....	2-13
PeopleCode Debugger.....	2-14
SQL Editor .....	2-14
Upgrade.....	2-14
Miscellaneous Permissions .....	2-14
Process .....	2-14
Process Group Permissions .....	2-15
Process Profile Permissions .....	2-16

Workstation Destinations .....	2-17
Server Destinations .....	2-17
OS/390 Job Controls .....	2-18
Allow Process Request.....	2-18
Allow Requester To .....	2-19
Override Output Destination .....	2-19
Override Server Parameters .....	2-19
View Server Status .....	2-19
Update Server Status .....	2-19
Enable Recurrence Selection.....	2-20
Run Client Process .....	2-20
Signon Times Permissions.....	2-20
Component Interface Permissions .....	2-21
Message Monitor Permissions .....	2-22
Web Libraries Permissions .....	2-23
Query .....	2-24
Defining Access Groups.....	2-24
Defining Query Profiles .....	2-27
PeopleSoft Query Use .....	2-28
PeopleSoft Query Output .....	2-29
Advanced SQL Features .....	2-29
Mass Change Security .....	2-29
Links .....	2-30
Audit .....	2-31

## Chapter 3

### Roles

General.....	3-2
Permission Lists.....	3-3
Members .....	3-3
Dynamic Members.....	3-4
Assigning Roles .....	3-4
Query Rule Example .....	3-6
Create a View .....	3-6
Create a Query.....	3-8
Create the Dynamic Rule .....	3-9
Dynamic Role Assignment Integration .....	3-10
ROLE_MAINT .....	3-10
DELETE_ROLE .....	3-11
Workflow.....	3-11

Links .....	3-11
-------------	------

## Chapter 4

### User Profiles

ID .....	4-2
General.....	4-3
Logon Information .....	4-3
Symbolic ID .....	4-3
Password/Confirm Password .....	4-4
General Attributes .....	4-4
Email ID .....	4-4
Language Code.....	4-4
Currency Code .....	4-4
Enable Expert Entry .....	4-4
Permission Lists .....	4-5
Roles .....	4-5
Working with Roles .....	4-5
Working with Dynamic Role Rules .....	4-6
Workflow.....	4-7
Workflow Attributes .....	4-7
Form ID.....	4-7
Alternate User ID .....	4-7
From Date .....	4-8
To Date.....	4-8
Supervising User ID.....	4-8
Routing Preferences .....	4-8
Reassign Work .....	4-8
Audit .....	4-9
Administrator.....	4-9
Links .....	4-9
User Profiles Tasks .....	4-10
Administer Personalizations.....	4-10
User Personalization Options .....	4-10
Enabling User Preferences .....	4-12
My Profile .....	4-14
Password .....	4-14
Set Personalizations .....	4-15
Email .....	4-17
Alternate User .....	4-17
Forgot My Password .....	4-17

Delete User Profile .....	4-18
---------------------------	------

## Chapter 5

### Setup Options and Processes

Setup Options.....	5-1
User Profile Options.....	5-1
User Profile Types.....	5-1
Profile Delete Tables to Skip .....	5-3
Passwords .....	5-3
Password Controls.....	5-4
Forgotten Passwords .....	5-6
Directory Authentication.....	5-8
Directory Setup .....	5-8
Mandatory User Properties .....	5-9
Optional User Properties .....	5-11
Directory Group Import .....	5-12
Security Links .....	5-15
Single Signon .....	5-16
Single Signon Component.....	5-18
Sample Single Signon Transaction .....	5-19
Single Signon Configuration Considerations .....	5-22
Digital Certificates .....	5-23
Why Implement SSL? .....	5-23
Certificate Authorities.....	5-24
Administer Certificates Page (Key Management) .....	5-25
Configuring SSL for Application Messaging.....	5-27
Security Processes .....	5-30
Execute Role Rules .....	5-31
Directory Group Import .....	5-31
Other Security Administration Tasks .....	5-32
Setting up Access Profiles.....	5-32
Access Profile Properties .....	5-33
Working with Access Profiles.....	5-35
Transferring Users between Databases .....	5-36
Considerations.....	5-37
Running the Scripts .....	5-37

## Chapter 6

### Object Security

Understanding Object Security .....	6-1
-------------------------------------	-----

Object Groups and Permission Lists .....	6-3
Object Security Rules.....	6-3
The Object Security Interface .....	6-4
File Menu .....	6-4
Change Menu .....	6-5
View Menu.....	6-5
Working with Object Groups.....	6-5
Viewing Object Groups .....	6-10
Selecting a View .....	6-10
Viewing All Objects.....	6-10
Viewing Objects of a Specific Object Type.....	6-11
Defining Object Groups.....	6-11
Adding and Removing Objects .....	6-12
Assigning Object Groups to Permission Lists .....	6-13
Display Only Mode.....	6-15

## Chapter 7

### Security Configuration Alternatives

Integrating with an LDAP Directory .....	7-1
Testing LDAP Connectivity.....	7-2
Enabling Signon PeopleCode for LDAP Authentication .....	7-3
Configuring Directory Authentication .....	7-4
Setting up the Directory .....	7-4
Specifying User Properties.....	7-6
Importing Directory Groups.....	7-7
Configure Directory Group Import .....	7-7
Run the Directory Group Import Process.....	7-8
Assigning Imported Directory Groups to PeopleSoft Roles .....	7-8
Signon PeopleCode.....	7-9
Modifying Signon PeopleCode .....	7-9
Enabling Signon PeopleCode.....	7-11
Permissions .....	7-12
Using Security Exits .....	7-13
Web Server Exit .....	7-13
Configuring the System.....	7-14
Creating a Default User.....	7-14
Modifying the configuration.properties File .....	7-14
Writing a Signon PeopleCode Program .....	7-15
Signing on through the Web Server .....	7-17
Windows Exits .....	7-19



Overview .....	7-19
Customizing PSUSER.DLL .....	7-21
Implementing a Customized PSUSER.DLL .....	7-26

## **Index**



## ABOUT THIS PEOPLEBOOK

In this book we describe the interface, the tables, and the profiles associated with PeopleSoft security. This information focuses primarily on the PeopleTools security components and how you can use them to secure pages, fields, and so on. Keep in mind that your application documentation also contains security topics that are more specific to the applications you have purchased.

This book is intended for technical users, system administrators, and programmers who will be implementing, maintaining, or developing applications for your PeopleSoft system. To take full advantage of the information covered in this book, we recommend that you have a basic understanding of how to use PeopleSoft applications, system administration, and basic internet architecture. You should know how to navigate through the system and how to add, update, and delete information using PeopleSoft tables and pages. You should also have a basic familiarity with relational database concepts and SQL. We recommend that you are very familiar with the security implementation at your site and have read the security documentation supplied by your network and database vendors. This book assumes that you have a working knowledge of the details and components related to internet security.

The Security PeopleBook contains the following chapters:

**Understanding PeopleSoft Security:** This chapter provides an overview of the components, the interface, and implementation options you have.

**Working with Permission Lists:** Permission Lists are what you create to grant access to objects like pages, component interfaces, and so on. This chapter describes the interface, procedures, and options related to permission lists.

**Roles:** Roles enable you to arrange permission lists into logical groupings such as manager, employee, and so on. This chapter describes the interface, procedures, and options related to roles.

**User Profiles :** Each user of you system has a user profile to which you apply roles and other authorizations. This chapter describes the interface, procedures, and options related to user profiles and user-specific options.

**Setup Options and Processes:** There are a variety of setup and administrative options that you perform while configuring and maintaining your security system. For example, you setup LDAP directory authentication, create forgotten password hints, execute dynamic role rules, just to name a few. This chapter describes the interface, procedures, and options related configuring your system.

**Object Security:** This chapter describes how you secure your development environment. Maintain Security secures your PeopleSoft applications, you use Object Security to lock down specific development objects in Application Designer.

**Security Configuration Alternatives:** Because the PeopleSoft Security system is flexible, you have numerous options with your configuration and approach. This chapter outlines some of the

more popular options, such as setting up LDAP authentication and modifying Signon PeopleCode.

## Before You Begin

To benefit fully from the information covered in this book, you need to have a basic understanding of how to use PeopleSoft applications. We recommend that you complete at least one PeopleSoft introductory training course.

You should be familiar with navigating around the system and adding, updating, and deleting information using PeopleSoft windows, menus, and pages. You should also be comfortable using the World Wide Web and the Microsoft® Windows or Windows NT graphical user interface.

## Related Documentation

To add to your knowledge of PeopleSoft applications and tools, you may want to refer to the documentation of the specific PeopleSoft applications your company uses. You can access additional documentation for this release from PeopleSoft Customer Connection ([www.peoplesoft.com](http://www.peoplesoft.com)). We post updates and other items on Customer Connection, as well. In addition, documentation for this release is available on CD-ROM and in hard copy.



**Important!** Before upgrading, it is *imperative* that you check PeopleSoft Customer Connection for updates to the upgrade instructions. We continually post updates as we refine the upgrade process.

---

---

### Documentation on the Internet

You can order printed, bound versions of the complete PeopleSoft documentation delivered on your PeopleBooks CD-ROM. You can order additional copies of the PeopleBooks CDs through the Documentation section of the PeopleSoft Customer Connection Web site:  
<http://www.peoplesoft.com/>

You'll also find updates to the documentation for this and previous releases on Customer Connection. Through the Documentation section of Customer Connection, you can download files to add to your PeopleBook library. You'll find a variety of useful and timely materials, including updates to the full PeopleSoft documentation delivered on your PeopleBooks CD.

---

### Documentation on CD-ROM

Complete documentation for this PeopleTools release is provided in HTML format on the PeopleTools PeopleBooks CD-ROM. The documentation for the PeopleSoft applications you have purchased appears on a separate PeopleBooks CD for the product line.

---

## Hardcopy Documentation

To order printed, bound volumes of the complete PeopleSoft documentation delivered on your PeopleBooks CD-ROM, visit the PeopleSoft Press Web site from the Documentation section of PeopleSoft Customer Connection. The PeopleSoft Press Web site is a joint venture between PeopleSoft and Consolidated Publications Incorporated (CPI), our book print vendor.

We make printed documentation for each major release available shortly after the software is first shipped. Customers and partners can order printed PeopleSoft documentation using any of the following methods:

### Internet

From the main PeopleSoft Internet site, go to the Documentation section of Customer Connection. You can find order information under the Ordering PeopleBooks topic. Use a Customer Connection ID, credit card, or purchase order to place your order.

PeopleSoft Internet site: <http://www.peoplesoft.com/>.

### Telephone

Contact Consolidated Publishing Incorporated (CPI) at **800 888 3559**.

### Email

Email CPI at [callcenter@conpub.com](mailto:callcenter@conpub.com).

## Typographical Conventions and Visual Cues

To help you locate and interpret information, we use a number of standard conventions in our online documentation.

Please take a moment to review the following typographical cues:

`monospace font`

Indicates PeopleCode.

### **Bold**

Indicates field names and other page elements, such as buttons and group box labels, when these elements are documented below the page on which they appear. When we refer to these elements elsewhere in the documentation, we set them in Normal style (not in bold).

We also use boldface when we refer to navigational paths, menu names, or process actions (such as **Save** and **Run**).

### *Italics*

Indicates a PeopleSoft or other book-length publication. We also use italics for *emphasis* and to indicate specific field values. When we cite a field value under the page on which it appears, we use this style: ***field value***.

We also use italics when we refer to words as words or letters as letters, as in the following: Enter the number *0*, not the letter *O*.

**KEY+KEY** Indicates a key combination action. For example, a plus sign (+) between keys means that you must hold down the first key while you press the second key. For ALT+W, hold down the ALT key while you press W.

**Jump links** Indicates a jump (also called a link, hyperlink, or hypertext link). Click a jump to move to the jump destination or referenced section.

**Cross-references** The phrase For more information indicates where you can find additional documentation on the topic at hand. We include the navigational path to the referenced topic, separated by colons (:). Capitalized titles in *italics* indicate the title of a PeopleBook; capitalized titles in normal font refer to sections and specific topics within the PeopleBook. Cross-references typically begin with a jump link. Here's an example:

---

For more information, see Documentation on CD-ROM in About These PeopleBooks: Related Documentation.

---

• **Topic list** Contains jump links to all the topics in the section. Note that these correspond to the heading levels you'll find in the Contents window.



Name of Page

Opens a pop-up window that contains the named page or dialog box. Click the icon to display the image. Some screen shots may also appear inline (directly in the text).



Text in this bar indicates information that you should pay particular attention to as you work with your PeopleSoft system. If the note is preceded by **Important!**, the note is crucial and includes information that concerns what you need to do for the system to function properly.



Text in this bar indicates For more information cross-references to related or additional information.



Text within this bar indicates a crucial configuration consideration. Pay very close attention to these warning messages.

## Comments and Suggestions

Your comments are important to us. We encourage you to tell us what you like, or what you would like changed about our documentation, PeopleBooks, and other PeopleSoft reference and training materials. Please send your suggestions to:

PeopleTools Product Documentation Manager  
PeopleSoft, Inc.  
4460 Hacienda Drive  
Pleasanton, CA 94588

Or send comments by email to the authors of the PeopleSoft documentation at:

[DOC@PEOPLESOFT.COM](mailto:DOC@PEOPLESOFT.COM)

While we cannot guarantee to answer every email message, we will pay careful attention to your comments and suggestions. We are always improving our product communications for you.





## CHAPTER 1

# Understanding PeopleSoft Security

For almost any type of business application, security is critical. This is especially true in core business applications, such as your PeopleSoft applications. Typically, you won't want every department in your company to have access to *all* of your applications. Nor will you want everyone within a department to have access to all the functions or all the data of a particular application. Additionally, you may want to restrict who can actually customize your applications with PeopleTools, so you don't have to worry about aspiring "programmers" getting creative with a database or a set of applications that you're about to move into production.

PeopleSoft provides you with security features, including components and PeopleTools, to ensure that your sensitive application data, such as employee salaries, performance reviews, or home addresses, doesn't fall into the wrong hands. Most likely, you probably use other security tools for your network and RDBMS. All these tools work together to protect your PeopleSoft system from unauthorized access.

As you implement the PeopleSoft Internet Architecture (PIA), you'll need a robust and scalable means by which you can grant authorization to users efficiently. When you deploy your applications to the Internet, the number of potential users of your system increases exponentially. Suddenly, you have customers, vendors, suppliers, employees, and prospects all using the same system. As such, how you design your access permissions is very important.

The PeopleSoft security approach is tailored for the internet. It enables you to easily create and maintain security definitions, and it also enables you to reduce the maintenance of your security system. If you want to ease the burden of your security administrator having to maintain thousands of security definitions, you can take care of many of the maintenance tasks programmatically.

You use the Maintain Security PeopleTool to apply security to all of the users of your system. Users can include employees, managers, customers, contractors, suppliers, and so on. This is where you divide your users according to roles. A role is an object that has properties, such as name, description, permission lists, and so on. One of the properties assigned to a role is the list of users assigned to it. For instance, there might be an Employee role, a Manager role, or an Administrator role. Users who belong to a particular role require a specific set of permissions, or authorizations, within your system so that they can complete their daily tasks.

Besides applying security authorizations to users, you also need to lock down the objects and definitions in your PeopleSoft development environment. The Object Security PeopleTool is what you use to restrict access to the objects developers create in Application Designer. Just like you restrict sets of end users from accessing particular pages and components, you also need to restrict the objects that your site's developers can access using Application Designer. An *object definition* refers to any of the definitions that you create within Application Designer, such as Records, Pages, or Business Components. Each one of these object definitions may have

individual security needs. For instance, you may have a large development staff, but perhaps you really only want a small set of developers to have access to specific Record definitions.

The components and tools you use to secure your PeopleSoft system are covered in the following chapters. After reading this chapter you should have a good overview of PeopleSoft security, and then in the following chapters you can drill down into the details.

Keep in mind that the scope of this discussion is limited to that which relates directly to your PeopleSoft system. That is, you will need to consult the documentation provided by your other vendors for other areas that need to be secured, such as databases, a file server, your network, and so on.



With PIA, PeopleSoft introduces an entirely new architecture. As such, we have introduced many new methods and approaches to securing the architecture. Because our technology continually evolves, PeopleSoft provides an additional document called *Security Answer Book*. This is where you go to find late-breaking information from the field, tips, and, most important of all, clarification to some of the more subtle aspects of implementing PeopleSoft security. You download *Security Answer Book* from the Continuous Documentation page in Customer Connection.

---

## PeopleSoft Online Security

The PeopleSoft system is comprised of many components, such as batch processes, object definitions, application data, and so on. Using PeopleTools security tools you can control access to most of these components.

The following sections introduce you to some of the main areas you secure with PeopleTools. That which you do not secure within in PeopleTools, you use application-specific interfaces, such as Administer Security.



**For more** information regarding your application security, refer to your PeopleSoft application documentation.

---

---

## Signon and Time-out Security

When a user attempts to sign on to PeopleSoft, they enter a User ID and a password on the PeopleSoft Signon page. If the ID and password are valid, PeopleSoft connects the user to the application and the system retrieves the appropriate user profile.

If the user attempts to signon during an invalid *signon time*, as defined in their security profile, they are not allowed to sign on. A signon time is an adjustable interval during which a user is allowed to signon to PeopleSoft. For example, if a given signon time is Monday through Friday from 7am to 6pm for a set of users, those users could not access a PeopleSoft application on Saturday or on Friday at 6:05pm, for that matter.

Once user signs on, they can stay connected as long as their signon time allows and as long as their browser doesn't sit idle for longer than their *time-out interval*. A time-out interval specifies how long the user's machine can remain idle—no keystrokes, no SQL—before PeopleSoft automatically disconnects the user from the application.

You specify both the signon times and time-out interval using Maintain Security. There are other timeout intervals that are not necessary related to security; your web server and other PIA components control them, but those are beyond the scope of this document.

---

## Page and Dialog Security

You use Maintain Security to control what parts of the PeopleSoft interface users can access. You do this by granting or restricting access to the PeopleSoft menus. You can set the access rights to the entire menu bar or just a specific item on that menu. The menu bars are what users click to access a PeopleSoft application or a PeopleTool, such as Administer Workforce or Maintain Security. Because the only way to access a PeopleSoft page is through a menu, if a user has no access to a particular menu or menu item, then you have effectively restricted that user's access to the corresponding page.

If you don't want to restrict an entire menu bar, you can just restrict access to specific actions or commands while a user has access to a page. For instance, you may want a clerk in your sales office to be able to access contract data, but you don't want the clerk to be able to Update the data. In this case, you grant them access to the set of pages, but you only allow them Display Only access. In this case, the clerk would not be able to Update or Correct any data. This approach enables you to allow users to get their work done while maintaining the security and integrity of your business data.

---

## Batch Environment Security

If a particular user needs to execute batch processes using Process Scheduler, you need to assign the appropriate Process Profile to the User Profile and create process groups for your processes. A user gets both process group and process profile authorizations by way of Permission Lists. A user gets permission to process groups through Roles, and they get a process profile through the Process Profile permission list.



You add the Process Profile Permission List directly to the User Profile, not to an intermediary Role.

---

## Process Security

Because PeopleSoft applications take advantage of other applications, such as SQR and COBOL, you need to make sure that you are running your batch processes in a secure environment.

There are three levels of security for batch programs.

- First, each batch program has a run control that you define before you can run the batch

program. The run controls are set up using Process Scheduler

- Second, also using Process Scheduler, you set up Process Groups, which are groups of batch processes. Then in Maintain Security you add Process Groups to a security profile. Users can run processes that belong to the Process Group(s) assigned to their security profile.
- Lastly, in your RDBMS environment, you can restrict off-line access to batch processes using the security tools described in your platform manuals.



For more information see Process.

---

## Reporting Security

The PeopleSoft Report Manager uses a logical space on a server, as in your web server, called the Report Repository. The Report Manager enables you to generate and distribute reports over the Internet, and it stores the output in the Report Repository. It's very important that wherever you decide to situate your repository make sure that the server is locked down from outside access. You want to make sure that only PeopleSoft can access and distribute the generated reports. Report Repository servlet takes things off of the web server and serves them up in the browser. With report distribution, you distribute reports and view them according to your role.

---

## Object Security

Object Security is a separate PeopleTool that you use to restrict access of your application developers to definition objects. You use Object Security to govern access to the individual database object definitions, such as Record definitions, Field definitions, and Page definitions. You create the definitions using Application Designer, and PeopleTools stores the definitions in the underlying PeopleTools tables. Using Object Security, you can protect particular object definitions from being modified by developers.



**For more** information on securing definition objects see Object Security.

---

---

## Application Data Security

Although Object Security is a form of data security, you use it to control access to particular rows of data—object definitions—in the PeopleTools tables, we also provide a number of ways to control the application data that a user is allowed to access in the PeopleSoft system. This task is also known as setting data permissions.

With application data security you can set data permissions at the following levels:

- Table level (for queries only)

- Row level
- Field level.

## Query/Table-Level Security

Query is a PeopleTool that helps you build SQL queries to retrieve information from your application tables. For each Query user, you can specify the records they are allowed to access when building and running queries. You do this by creating Query Access Groups in the Tree Manager, and then you assign users to those groups with Query Security. Keep in mind that Query security is only enforced when using Query; it doesn't control run-time *page* access to table data.



For more information on Query Security, see PeopleSoft Query.

---

## Row-Level Security

You can design special types of SQL views—security views—to control access to individual rows of data stored within your application database tables. In short, row-level security lets you specify what data that a particular user is permitted to access. PeopleSoft applications are delivered with built-in, row-level security functions that are tailored to specific applications.

For example, in PeopleSoft HRMS, we provide security tables that enable you to restrict user access to employee rows of data according to organizational roles. You could also permit a user to view and update rows for employees in their department only. Similarly, in PeopleSoft Financials you can use security views to determine who has access to which Business Units and Ledgers. You can also use security tables to grant privileges by access group to users who use PeopleSoft Query to access data from the database.



For more information about implementing row-level security for your applications, see your application security chapter.

---

## Field Security

Using PeopleCode, you can restrict access to particular fields or columns within your application tables. For example, if you want a certain class of user to be able to access certain panels, but not to view a particular field on those panels, such as compensation rate, you can write PeopleCode to hide the field for that user class.



For more information about field-level security PeopleCode functions, refer to PeopleCode Developer's Guide.

---

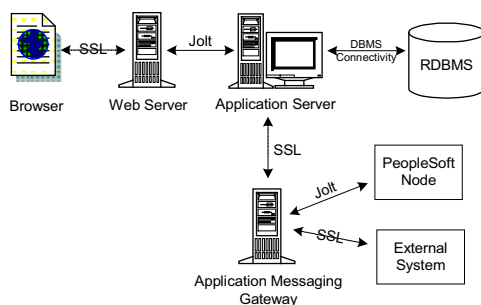
## PeopleSoft Internet Architecture (PIA) Security

The PeopleSoft Internet Architecture falls into the category of PeopleSoft online security, also known as runtime security. Only authorized users can connect to the web and application servers, and only authorized application servers can connect to a given database.

If you decide to deploy applications through PIA and implement our messaging solution, you will need to employ the use of a web server. For instance you'll need to know how to secure browser connections over the Internet as well as secure the messages that get published from your Application Messaging Gateway.

PeopleSoft uses authentication tokens imbedded in browser cookies to authorize users and enable single signon throughout the system. To secure the links between the numerous components within the system, including browsers, web servers, application servers, database servers and so on, PeopleSoft incorporates a combination of Secure Socked Layer (SSL) security and Tuxedo/Jolt Encryption.

The following diagram shows where the system uses SSL and Tuxedo encryption.



### SSL and Tuxedo/Jolt Encryption

There are a few security topics related to the application messaging system as well as the portal configuration that are covered elsewhere within PeopleTools documentation. Even when you are using the PeopleSoft portal for navigation, permission lists govern what a user accesses.



For more information on portal security issues see [Using Portal Administration Features](#).

## PeopleSoft Security Definitions

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

- User Profiles
- Roles
- Permission Lists



---

There is also a PeopleSoft security definition called an Access Profile, but these are defined at the database level.

---

Because rolling out your applications to the Internet significantly increases the number of potential users your system needs to accommodate, you need an efficient method of granting authorization to different user types. PeopleSoft security definitions provide a modular means by which you can apply security attributes in a scaleable manner.

Each user of your system has an individual User Profile, which in turn is linked to one or more Roles. To each Role, you add one or more Permission Lists, which ultimately control what a user can and can't access. So a user inherits permissions by way of the role. There are a handful of permissions that assign directly to the user profile, but these are the exception.

The following topics briefly describe each of these security definitions. Later in this PeopleBook, each definition is discussed in more detail in the proper context.

---

## User Profiles

A User Profile is a set of data describing a particular user of your PeopleSoft system. This data includes everything from the low-level data that PeopleTools requires, such as Language Code, to application-specific data, such as the SETIDs a user is authorized to access within the PeopleSoft financial applications. Some User Profile information, such as password, is truly security related. On the other hand, some of the information, such as the email address, is descriptive, and some of the information, such as Multi Language Enabled?, is a preference.

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, not with user interaction.

---

## Roles

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

A Manager is also an Employee, and who knows, she may even be a Student. Roles allow you to dynamically mix and match access appropriately.

You have two options when assigning roles; assign Roles manually or you can assign them dynamically. When assigning roles dynamically, you can use PeopleCode, LDAP, and Query rules to assign User Profiles to Roles programmatically.

## Permission Lists

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 fewer types of permissions in a Permission List the more modular and scalable your implementation. To what granularity you decide to take your permission lists is up to you.

A User Profile inherits *most* of its permissions through the Role(s) or roles that have been assigned to the User Profile. Some Permission Lists, such as Process Profile or row-level security, you apply directly to a User Profile.

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

Let's say you want to give your vendors access (display only) to a page that shows them your inventory status. Perhaps this enables them to improve their delivery of your supplies. To add authorization to such as page, you go to Maintain Security, Permission Lists. You can add new permission lists or modify existing ones. Once you're there, select the Pages page.

General Pages **PeopleTools** Process Sign-on Times

Permission List: VENDOR

Description: Vendor Inventory Pages

View All First 1 of 1 Last

**Edit Components Menu Name**

Edit Components [Search] [Add] [Remove]

Maintain Security, Permission Lists, Pages

To add access to a page you must first add access to the associated menu. Use the Menu Name drop-down list to select a menu.

General Pages **PeopleTools** Process Sign-on Times

Permission List: VENDOR

Description: Vendor Inventory Pages

View All First 1 of 1 Last

**Edit Components Menu Name**

[Edit Components](#) MAINTAIN\_INVENTORY [Add] [Remove]

Maintain Security, Permission Lists, Pages

After adding the menu, you drill down to the components within the menu by selecting Edit Components.



**Component Permissions**

MAINTAIN\_INVENTORY

View All First 1-8 of 26 Last

Edit Pages	Authorized?	Bar Label	Component
<a href="#">Edit Pages</a>	<input type="checkbox"/>	Use	Adjustments
<a href="#">Edit Pages</a>	<input type="checkbox"/>	Use	Transfers
<a href="#">Edit Pages</a>	<input type="checkbox"/>	Use	Shipping Lead Time
<a href="#">Edit Pages</a>	<input type="checkbox"/>	Use	Historic Lead Calculation
<a href="#">Edit Pages</a>	<input type="checkbox"/>	Use	Inventory Status
<a href="#">Edit Pages</a>	<input type="checkbox"/>	Use	Inventory Comments
<a href="#">Edit Pages</a>	<input type="checkbox"/>	Use	Lot Control Information
<a href="#">Edit Pages</a>	<input type="checkbox"/>	Process	Historical Lead Calculation

OK Cancel

Maintain Security, Permission Lists, Pages, Edit Components

From the Component Permissions interface you can drill down even further to specific pages, by selecting Edit Pages. In this case, let's say we want to add access to Inventory Status.

**Page Permissions**

MAINTAIN\_INVENTORY / Use / Inventory Status

View All First 1 of 1 Last

Page	Authorized?	Display Only
Inventory Status	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Actions**

☐ Add

☒ **Update/Display**

☐ Update/Display All

☐ Correction

☐ Data Entry

Select All

Deselect All

OK Cancel

Maintain Security, Permission Lists, Pages, Edit Components, Page Permissions

This is where you authorize user access, whether the access is display only, and/or what actions a user can perform on the page. Once you have completed the permission list, then you add it to a role, perhaps a Vendor role in this case. Then each user of the Vendor type gets assigned to the Vendor role, which contains the Vendor Inventory Pages permission list (among others).

All of the options described in the previous example are discussed later in this document. The previous example is intended to introduce the basic functionality and the look and feel of the Maintain Security interface.

## PeopleSoft Authorization IDs

The PeopleSoft system uses various authorization IDs and passwords to control user access to the system. You use Maintain Security to assign two of these IDs: User ID and Access ID. The primary purpose of many of the following IDs is to gain access to the system.



For more information on how each ID gets used in the signon process, see Understanding PeopleSoft Signon.

---

### User IDs

A PeopleSoft User ID is the ID you enter at the PeopleSoft signon dialog. Using Maintain Security, you'll assign each PeopleSoft user a User ID and password. The combination of these two items grants users online access to the PeopleSoft system. The system can also use a User ID stored within an LDAP directory server.

The User ID is also the key used to distinctly identify the User Profile definition.

---

### Connect ID

PeopleTools offers a connectivity feature called Connect ID. You can use this feature on any of our supported RDBMS platforms. The Connect ID performs the initial connection to the database.

A Connect ID is a valid user ID that, when used during login, takes the place of PeopleSoft User IDs for the logon process. Using Connect ID means you *don't* have to create a new database user for every PeopleSoft user you add to the system.



Connect ID is required for a direct connection (two-tier connection) to the database. So application servers and two-tier Windows Clients require a Connect ID. You specify the Connect ID for an application server in the Signon section of the PSADMIN utility, and for Windows Clients you specify the Connect ID in the Startup tab of the Configuration Manager.



**Important!** If you are configuring a Windows Client to connect directly to the database (two-tier) then you must specify a Connect ID in the Startup tab of the Configuration Manager. Without a Connect ID specified the system assumes that workstation is accessing PeopleSoft through an application server. As such, the option to override database type is disabled. Any two-tier connection requires a Connect ID.

---

## Access IDs

When you create any User ID, you must assign it an Access Profile, which specifies an Access ID and password.

The PeopleSoft Access ID is the RDBMS ID with which PeopleSoft application(s) are ultimately connected to your database once the PeopleSoft System validates the User or Connect ID. An Access ID typically has administrator-level database access; that is, it has all the RDBMS privileges necessary to access and manipulate data for an entire PeopleSoft application. The Access ID should have SELECT, UPDATE, and DELETE access.

It's important to understand that users do not know their corresponding Access IDs. They simply signon with their User or Connect ID and—behind the scenes—the system logs them onto the database using their Access ID.

Should they try to access the database directly with a query tool using their User or Connect ID, they wouldn't get far. User and Connect IDs only have access to the few PeopleSoft tables used during signon, and that access is SELECT-level only. Furthermore, PeopleSoft encrypts all sensitive data that resides in those tables.



Access Profiles are used in the following situations only: when an application server connects to the database, when a windows workstation connects directly to the database, and when a batch job connects directly to the database. Access Profiles are not used when end users access the applications through PIA. During a PIA transaction, the application server maintains a persistent connection to the database, and the end users leverage the Access ID that the application server domain used to signon to the database.

---

---

## Symbolic ID

PeopleSoft encrypts the Access ID when it is stored in the PeopleTools Security tables. Consequently, an encrypted value can't be readily referenced nor accessed. So when the Access ID, which is stored in PSACCESSPRFL, needs to be retrieved or referenced, the query selects the appropriate Access ID by using the Symbolic ID as a search key.

Also, the Symbolic ID acts as an intermediary entity between the User ID and the Access ID. All the User IDs are associated with a Symbolic ID, which in turn is associated with an Access ID. If you change the Access ID, you only need to update the reference to the Access ID within the Symbolic ID rather than each and every User Profile.

---

## Before you get Started

First, you'll need to customize your own User definition. PeopleSoft delivers at least one full-access User ID with each of our delivered databases. Your first order of business should be to sign on with this ID and personalize it for your needs—or, create a new, full-access ID from scratch—being sure to specify a new password. In fact, you should change the passwords of all our delivered IDs as soon as possible.



---

You'll find our delivered IDs and passwords documented in your installation manual.

---

When you install PeopleSoft, you're prompted for an RDBMS system administrator ID and password. This information is used to automatically create a default access profile. If you'll be using more than one access profile, you'll want to set up the others before creating any new PeopleSoft security definitions. Most sites only use one access profile.

How many database level IDs you create is up to your site requirements, but, in most cases, having fewer database level IDs reduces maintenance issues.

For example, if you implement a pure LDAP authentication, at the very least, you need two database-level IDs—your Access ID and your Connect ID. With this scenario, in PeopleSoft you only need to maintain a Symbolic ID to reference the Access ID and maintain a User ID that the application server uses during signon. With this minimal approach, each user who needs a two-tier connection to run an upgrade, for example, could use the same User ID that the application server uses.

## Understanding PeopleSoft Signon

One of the more fundamental aspects of any security system is how users logon to the system. The following topics introduce you to the PeopleSoft signon functionality.

The most common direct signon to the PeopleSoft database is the application server signon, so let's examine how the application server signs on to the database. Keep in mind that each ID discussed in this example, is discussed in the following sections.

The basic steps in a PeopleSoft signon are as follows:

- **Initial connection.** The application server boots, and uses the Connect ID and User ID specified in its configuration file (PSAPPSRV.CFG) to perform the initial connection to the database.
- **SELECT on security tables.** Once the Connect ID is verified, the application server performs a SELECT on various PeopleTools security tables, such as PSOPRDEFN, PSACCESSPRFL, and PSSTATUS. From these tables the application server gathers such items as the symbolic ID, access ID, and access password. Once the application server has the required information, it logs off from this initial connection.
- **Reconnects with access ID.** When the system verifies that the access ID is valid, the application server begins the persistent connection to the database that all PIA and Windows three-tier clients use to access the database. Typically, the users signing on using a Windows workstation are developers using Application Designer or end users who need to access Query or Tree Manager.



---

A Windows workstation attempting a two-tier connection uses the same process as the application server.

---

If all of your users signon through either PIA or three-tier Windows workstations, you only need two database level ID's, the Connect ID and the Access ID. Also the User ID, submitted by the application server needs to be maintained within PeopleSoft and supplied with the appropriate permission lists. Any users who need to perform an upgrade, run Data Mover scripts, or perform any administrative transactions that require two-tier connections, also need to have a valid User ID defined at the PeopleSoft level. Either these individuals use the same ID that the application server uses, or you maintain a separate User ID in PeopleSoft for each user who needs two-tier access. Signon PeopleCode does not run during a two-tier connection, so maintaining two-tier users in an LDAP server is not supported.

---

## Directory Server Integration

PeopleSoft is well aware that your site uses software produced by numerous vendors, and we know that each different product requires security authorizations for users. Most of these products adhere to the model that includes user profiles and roles (or groups) to which users belong. PeopleSoft enables you to integrate your authentication scheme for PeopleSoft with your existing infrastructure. You can reuse user profiles and roles that are already defined within an LDAP directory service.

It is quite common for organizations to store the User Profiles in a central repository that serves user information for all of the programs that require it. The central repository is typically an LDAP Directory Server.

Using a Directory Server enables you to maintain a single, centralized User Profile that you can use across all of your PeopleSoft and non-PeopleSoft applications. This approach reduces redundant maintenance of user information stored separately throughout your enterprise, and it reduces the possibility of user information getting out of synch.

You always maintain Permission Lists and Roles using Maintain Security. However, for user profiles, you have a choice. You can choose to maintain them in Maintain Security or you can all an external LDAP server to drive the maintenance of your user profiles.



For more information on incorporating a directory server into your authentication and user profile maintenance scheme, see Security Configuration Alternatives.

---

---

## Authentication and Signon PeopleCode

As far as authentication goes, PeopleSoft provides a variety of options. You can store your PeopleSoft passwords within PeopleTools, the PSOPRDEFN table. You can also store and maintain your user passwords and the rest of the user profile data in an LDAP directory server. PeopleSoft retrieves the information stored in an external directory server using a combination of the User Profile component interface and Signon PeopleCode.

If you opt to reuse existing user profiles stored in a directory server, you don't need to perform dual maintenance on the two copies of the user data—one copy in the LDAP server and one copy in PSOPRDEFN. PeopleSoft ensures that the user information stays synchronized. If you

configure LDAP authentication, you maintain your user profiles in LDAP and not in Maintain Security.

Signon PeopleCode executes whenever a user logs onto the system. Signon PeopleCode copies the most recent user profile data from a directory server to the local database whenever a user logs on. PeopleSoft applications reference the user information stored in the PeopleSoft database rather than making a call to the LDAP directory each time the system requires user profile information. Signon PeopleCode ensures the local database has a current copy of the user profile based on the information in the directory. Each time the user signs on, Signon PeopleCode checks to see if the row in the user profile cache needs to be updated.

The following list shows a high-level view of the signon process flow.

1. The user enters User ID and Password on signon page.
2. PeopleTools attempts to authenticate the user.
3. Signon PeopleCode executes. The default Signon PeopleCode program is designed to update the use profile based on the current data stored in the directory server.

If needed, you can use Signon PeopleCode and business interlinks to synchronize the local copy of the user profile with *any* data source at sign on time – the program that ships with PeopleTools is only designed to synchronize the user profile with an LDAP directory server. Because the signon program is PeopleCode you can modify it as you wish, incorporating any of the PeopleSoft integration technologies that PeopleCode supports.

To Edit the Signon PeopleCode program, you open the LDAP function library record and use the PeopleCode Editor to customize the PeopleCode. Developers who modify the Signon PeopleCode program need to have a good understanding of PeopleCode and the integration features it offers.



Only users who signon through PIA or three-tier Windows Clients take advantage of Signon PeopleCode.

---

---

## Single Signon

PIA uses browser cookies for seamless single signon across all PeopleSoft nodes. A node refers to a database and the application server(s) connected to it. For example, a user can complete an HR transaction, and then click on a link for a Financials transaction without ever reentering a password. Single signon is especially important to the PeopleSoft portal; which aggregates content from several different applications and data sources into a single, integrated display.



For more information on setting up single signon, see Single Signon.

---

## Implementation Options

The PeopleSoft security system is quite flexible. By using our integration technologies, you can configure it to work with numerous schemes. The following topics illustrate the key options that you need to consider as you begin to plan your security implementation.

As you explore more of the features with PeopleSoft security you'll most likely take advantage of more options.

---

### Authentication

One of the first options to consider is how you plan to authorize users as they attempt to signon to your PeopleSoft system. Do you want to store and maintain the PeopleSoft user passwords within PeopleSoft, or do you plan to take advantage of the existing user profiles in an external directory server?

#### PeopleSoft-based Authentication

This option is, for the most part, the way PeopleSoft customers have authorized users in previous releases. This option means that potentially thousands of PeopleSoft user passwords will be stored and maintained solely within PeopleSoft. It's not that this option requires much in the way of space, but it does add administration issues, mainly because your PeopleSoft passwords will be yet another password your users will need to remember.

With this option there are only two database-level IDs, the Access ID and the Connect ID. The passwords reside in the PSOPRDEFN along with the other user information.

#### Directory-based Authentication

The other option you have is to leverage a central repository for user information in a directory server. The directory server operates under the LDAP protocol.

The advantage with this option lies in the fact that a user has one password that allows access to numerous software systems within your organization.

---

### Role Assignments

How do you plan to assign authorizations to your users? Recall that users inherit permissions by way of the roles to which they are assigned. So when you plan your authorization assignment, you are really planning how you intend to assign roles to your users. There are two ways to assign roles to users. You can take the static approach or you can take the dynamic approach.

## **Static**

If you take the static approach, it means that you assign users to roles, manually. The static approach, although a perfectly acceptable method, is not scaleable to the thousands of users that are likely to have using your system when you deploy applications to the Internet.

The static method requires an administrator to maintain each user's set of roles. For that reason, PeopleSoft recommends that you explore and implement the dynamic assignment of roles.

## **Dynamic**

Assigning roles dynamically involves creating business rules that you run against your system and based on the execution of these rules, the system assigns the roles accordingly. You can manually execute the rule, but typically, you execute the rules from a scheduled batch process. The dynamic assignment of rules enables your security system to reflect the organizational structure of your enterprise through an automated means.

Let's say an employee changes jobs within your company. Suppose this employee not only changes departments, but also becomes a manager in a new department. When you run your dynamic rule, the system removes the roles associated with the employee's previous position and then add the appropriate roles required for her new position. In addition, you can have the rule publish a message to other nodes, such as a Financials node, that might subscribe to changes in the HR database.

If you opt for the dynamic assignment of roles, you also need to consider which method to use for assigning roles. You can use PS/Query, LDAP, or PeopleCode to define your dynamic role assignment. If necessary, you can use a mix and match approach with the rules for assigning roles. For example, you can have one role rule based on LDAP, another based on a Query, and so on. You can also have multiple rule types for one role, as in the Manager role could be derived partially from an LDAP rule and partially from Query rule. Where the information that drives your role assignments is stored determines the types of role rules you execute. The following sections describe the situations in which you use each rule type.

### ***Query***

If the membership data for your roles resides in your PeopleSoft database, then PeopleSoft recommends that you use PS/Query to construct your role rules. One query could be MANAGER, another EMPLOYEE, and so on. When the rule executes, the system assigns your employee users to the EMPLOYEE role and the manager employees to the MANAGER role based on the results returned from the Query.

### ***LDAP***

If you already have your LDAP directory server groups organized by region, department, position, and so on, you should base your rules on the existing LDAP structure. Based on the directory setup and hierarchy, your rule would assign PeopleSoft users to the appropriate roles. In essence, with this approach PeopleSoft is merely plugging into your LDAP configuration. You should use this role rule type in conjunction with LDAP authentication.



## *PeopleCode*

If you have user information in other third party systems, such as legacy mainframe applications or UNIX account groups, you can use PeopleCode. This option enables you to take advantage of the integration technologies that PeopleCode supports, such as business interlinks and component interfaces. The business interlinks retrieve the data from the external system and write it to the role assignment tables in the PeopleSoft database.

---

## Cross System Synchronization

If you have multiple PeopleSoft systems you also want to consider how you will keep user information synchronized across the systems. This is especially important for the portal deployment where users are likely to move from one system to another seamlessly. For instance, after completing a transaction in the HR system, a user may click a link that takes her directly to the Financials system.

If you are using dynamic role assignment, the dynamic role batch program, by default, publishes a message that indicates a particular change. You need to make sure that nodes that require such information changes are configured to subscribe to the message that publishes the changed data. For instance, suppose your financials system needs a list of the “Managers” for a particular transaction. Because the manager information resides in the HR system, the HR system publishes any changed information to the financials system to keep the data in synch.

PeopleSoft also publishes a message when a user profile changes. This functionality is most useful if you are not *not* using LDAP to store user information. If you store user information in PeopleSoft, the message makes sure that password changes are replicated across multiple databases. If you store your user information in a central LDAP server, then the passwords, and so on, are already—in a sense—synchronized.

Permission lists and roles are objects that you can upgrade using Application Designers upgrade features. For user information PeopleSoft provides Data Mover scripts to migrate user profiles between systems for upgrades or bulk loads.

## Maintain Security Interface

Usage	Maintain the security definitions within your PeopleSoft system, such as User Profiles, Roles, and Permission Lists.
Navigation	Click <b>Maintain Security</b>
Access Requirements	Proper security authorization.

Maintain Security is the PeopleTool that you use to create, define, and modify your PeopleSoft security information. Within Maintain Security you separately define and modify User Profiles, Roles, and Permission Lists.

The Maintain Security interface contains the following menus:

- Use
- Setup
- Process

The following sections briefly describe each menu. Later in this PeopleBook, each page that pertains to setting up your security is discussed in more detail within the proper context.

---

## Use

From the Use menu, you have the following options.

<b>Option</b>	<b>Description</b>
My Profile	This option offers the essential self-service tasks that users typically need, such as email and language preferences, password changes, and alternate users for workflow routings.
Forgot My Password	This is where end users go to get a new password issued if they have forgotten their previous one. This is an optional feature.
User Profiles	This is where you create and maintain your site's User Profiles.
Administer Personalizations	This is where users go to view the navigation, international, and save indicator preferences.
Delete User Profile	This is the interface you use to remove unneeded User Profiles.
Roles	This is where you create and maintain the numerous Roles of your system.
Role Save As	To clone a Role, use Role Save As.
Delete Role	This is the interface you use to delete unneeded Roles from your system.
Permission Lists	This is where you create and maintain Permission Lists.
Permission Lists Save As	To clone a Permission List use Permission Lists Save As.
Delete Permission List	This is the interface you use to delete unneeded Permission Lists from your system.

## Setup

From the Setup Menu you have the following options.

<b>Option</b>	<b>Description</b>
User Profile Types	This is where you set up User ID types, such as Employee, Customer, and Vendor types.
Profile Delete Tables to Skip	This is where you specify any tables that you want to be skipped by the delete user process.
Defined Personalizations	This is a read only page where you can view the setup information for the user personalizations.
Password Controls	This is where you set limitations on passwords, such as the duration of a password of the number of failed logon attempts allowed.
Forgotten Password Questions	This is where you set up the question, or list of questions, that users need to answer to have their password mailed to them.
Directory Authentication	Use this component to enable directory-based authentication. This is where you map attributes from the directory to fields in the PeopleSoft user record.
Directory Group Import	If you are using LDAP for dynamic role rules, you use this component to configure the process that copies a list of directory groups into the PeopleSoft database.
Security Links	To make it easier to navigate to other security pages within your PeopleSoft system, as in those that are specific to a particular PeopleSoft application, you can insert a link here. This, in effect, extends the scope of Maintain Security according to your site's requirements.
Single Signon	If you want to implement single signon you need to add configure it using this page. By default, single signon is not activated. You need to explicitly enable it and specify collections of nodes that "trust" each other.
Digital Certificates	The PeopleSoft Application Messaging technology uses SSL for secure message transport across the internet. For messaging nodes to communicate using SSL, you need to register the digital certificates that you receive from certificate authorities. You use this page to register and maintain your inventory of digital certificates.

---

## Process

The Process menu is where you go to check the status of the processes that you invoked from the Process menu. From the Inquire menu you have the following options.

<b><i>Option</i></b>	<b><i>Description</i></b>
Execute Role Rule	If you take advantage of dynamic role assignment, you can manually execute the dynamic rule batch program from this page. This is a process request page tailored for that program. It allows you to execute the dynamic rules for <i>all</i> the roles in the system.
Directory Group Import	You can import the list of group objects stored in your LDAP directory into your PeopleSoft system. You can manually execute the import program from this page. This is a process request page tailored for that program.

## CHAPTER 2

# Working with Permission Lists

This chapter contains information regarding the options on the Use menu that pertain to Permission Lists. Specifically, these options are Permission Lists, Permission Lists Save As, and Delete Permission List.

Permission Lists are the building blocks of your end user security authorizations. Before you begin creating your User Profiles and your Roles, you typically want to create your inventory of Permission Lists. When creating your Permission Lists you want to consider each type of Role and User Profile to which they will be attached. Each set of permissions has its own tab from which you can select the appropriate options.

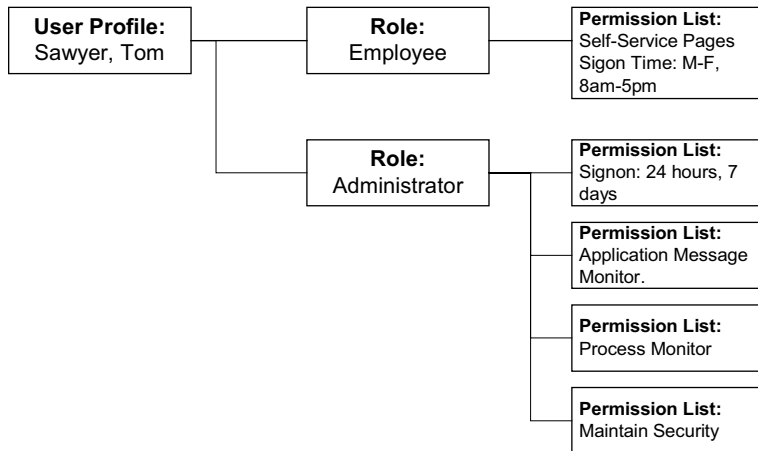
A Permission List may contain any number of the following permissions:

- General
- Pages
- PeopleTools
- Process
- Signon Times
- Component Interface
- Message Monitor
- Web Libraries
- Query
- Mass Change Security
- Links

A Permission List may contain one or more permissions, and the smaller the amount of permissions within a particular Permission List the more flexible and scaleable that Permission List is.

As you define your permission lists, anticipate how you will assign them to roles. Recall that roles are intermediary objects that exist between permission lists and users. Roles enable you to assign permissions to users dynamically. All of the permissions required for a particular role must be assigned to that role, or you run the risk of hampering a user's ability to use the PeopleSoft system to a full capacity.

In the following example notice that the permission lists are assigned to roles, which are then assigned to user profiles. A role may contain numerous permissions and a user profile may have numerous roles assigned to it. Because permission lists are applied to users by way of the 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.



### Security Definition Hierarchy

Assuming the previous example represents the security authorizations of Tom Sawyer, then Mr. Sawyer inherits the permission lists assigned to both the roles assigned to his user profile. In this example, he ultimately has access to the employee self-service pages, the message monitor, the Process Monitor, and Maintain Security. If Tom were to become a manager, then the permission lists assigned to the Manager role would be added to his profile. Currently, Tom has five permission lists.

Theoretically you could create a Permission List tailored for each and every Role, and that Permission List could contain a permission of every category from General to Web Libraries. In this case, what you have is a custom Permission List that only applies to a specific Role, and therefore will not scale to encompass Roles that might be similar, but not exactly alike. You'd have to create a new one from the ground up. As a definition, this Permission List would not exactly be reusable in other contexts, and thereby not the most efficient approach for larger, more complicated implementations.

On the other hand, you can take a more modular or "mix-and-match" approach. This approach involves numerous, specific, Permission Lists that you can add and remove easily to Role definitions. Let's say you have three 8-hour shifts at your site. Using the modular approach you could create three different "shades" of Signon permissions: one for 6 AM to 2 PM, one for 2PM to 10 PM, and another for 10 PM to 6 AM. Then depending on the shift for a particular Role, you can easily apply or remove the appropriate Signon permission as needed without affecting any other permissions.

How you elect to implement your Permission Lists is entirely up to your site's security scheme and your Security Administrator. However, PeopleSoft recommends that you lean more to the modular approach for increased scalability. As a general rule, your permission lists should be designed/assigned to roles so that the common user has in between 10 to 20 lists in total.

Some users may have more, and some may have less permission lists, but the average number of permissions lists that a user has should be within 10-20. This range represents a good blend of both performance and flexibility. If you have too many permission lists, you may notice performance degradation and if you have too few permission lists, you may be sacrificing flexibility.

## Getting Started

Before you begin learning about the different pages associated with creating your Permission Lists, you need to be familiar with the basics of creating, cloning, and deleting Permission Lists. The following procedures should get you acquainted with some of the basics.



---

All of the components associated with Maintain Security reside under **PeopleTools**, **Maintain Security**.

---

To create a new Permission List

1. Select Use, Permission Lists, and on the search page click Add a New Value.
2. In the **Permission List** edit box, enter the name of Permission List you want to create.



---

PeopleSoft HRMS requires certain naming conventions for permission lists, however PeopleTools does not enforce these application-specific requirements. Therefore, when creating permission lists in Maintain Security, PeopleSoft recommends that you keep the following conventions in mind. HRMS requires the following: primary permission lists need to start with PP%, and data permission lists need to start with DP%.

---

3. From the pages in the Permission List component select the appropriate permissions.
4. Save your work.

To clone a Permission List

1. Select Use, Permission List Save As.
2. In the search page, search for the Permission List that you want to clone, and click it.

This reveals the **Permission List Save As** page.

3. On the Permission List Save As page enter a new name in the **To:** edit box for the Permission List that you want to clone.
4. Click Save.

To delete a Permission List

1. Select Use, Delete Permission List.
2. On the search page, locate the Permission List that you want to delete and click it.

This reveals the **Delete Permission List** page.

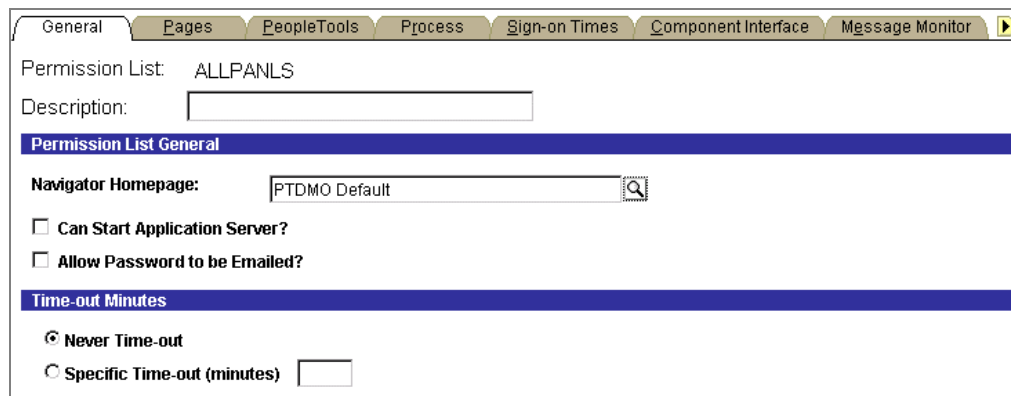


Maintain Security, Use, Delete Permission List

3. Click Delete Permission List.
4. Click **OK** to confirm the deletion, or click **Cancel** to abort.

## General Permissions

The General page is the first tab you see, by default, when opening a new or existing Permission List. This is where you set the general or miscellaneous attributes and system defaults.



Maintain Security, Use, Permission Lists, General

The General page offers the following options:

- Navigator Homepage
- Can Start Application Server?
- Allow Password to be Emailed
- Time-Out Minutes





For more information on setting the time out interval with PIA, see Setting Timeout Intervals.

---

The following sections explain these options.

---

## Description

The Description should help to more uniquely identify the definition. There is a 30-character limit for this value.

---

## Navigator Homepage

A Navigator Homepage is 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 start up.

If this is the user profile's "Navigator Homepage" permission list, the system grabs this value at run time.



For more information on setting the Navigator Display on Windows workstations see Configuration Manager.

---

---

## Can Start Application Server?

Selecting this checkbox enables a user with this permission list to start a PeopleSoft application server. This may be a User ID used solely for starting the application server or this ability may be reserved for your system administrative personnel. This does not refer to the user who signs on to an application server and boots it. Rather, this option applies to the "OPRID" and "OPRPSWD" that you enter into PSADMIN (or PSAPPSRV.CFG) in the Startup section.



For more information on PSADMIN see Domain Parameter Reference.

---

---

## Allow Password to be Emailed

When a user forgets their password, PeopleSoft provides the option to have it sent to the user by way of email. However, at some sites, the security administrator may not want passwords appearing unencrypted in anyone's email. As such, you decide whether or not you want to implement this feature by Permission List. None can use it, some can use it, or all can use it

depending upon your implementation. Those users who do not have the proper authority receive an error message if they attempt to have a new password emailed to them.



For more information on the email new password feature see Setup Options and Processes.

---

---

## 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 zero, which means there is no time-out interval; the user will never be timed-out.



Time out limits are controlled at the web server and application server level as well.

---

If you select **Never time-out**, an inactive user will never be automatically logged off. Otherwise, select the **Specific time-out (minutes)** radio button, and enter the appropriate value in minutes. Keep the following in mind while entering a custom time-out interval:

- It must be a positive integer.
- It must not contain edit characters, such as commas or a \$.
- It must be a SMALLINT in the valid range allowed for this field (0-32767).

## Page Permissions

Page permissions refer to the pages to which a Role has access.

Menu Name		
<a href="#">Edit Components</a> ADMINISTER_HR_SECURITY	+	-
<a href="#">Edit Components</a> ADMINISTER_INV_SECURITY	+	-
<a href="#">Edit Components</a> ADMINISTER_WORKFORCE_(GBL)	+	-
<a href="#">Edit Components</a> ADMINISTER_WORKFORCE_(U.S.)	+	-
<a href="#">Edit Components</a> ALTER_TESTS	+	-
<a href="#">Edit Components</a> APPLICATION_ENGINE	+	-
<a href="#">Edit Components</a> APPMSGMONITOR	+	-
<a href="#">Edit Components</a> BUS_EXP_IC	+	-

### Maintain Security, Use, Permission Lists, Pages

The Pages interface shows the various PeopleSoft menu bars containing pages to which a Permission List has access. Because every application and PeopleTool in the system has an associated menu bar, this view is essentially a listing of authorized applications and PeopleTools for a user.

By granting access to a menu, you effectively grant access to a particular page or application. This is true because the only way to access a PeopleSoft application is through the menu structure. Now keep in mind that you are not only granting access to PeopleSoft applications for your end users; you can also grant access to important page-driven PeopleTools like Process Scheduler.

For example, you can't access any of the pages that reside under the menu name ADMINISTER\_HR\_SECURITY without first having the Menu Name added to your Menu Name list. After adding the Menu Name, you then drill down further and grant access to specific pages and actions within that menu structure.

Granting access to any of the PeopleTools and PeopleSoft applications requires serious considerations. For each Role, you need to thoughtfully consider what the members of that Role need to access to complete their jobs and to what degree they need access. You don't want to grant too much access, and then again, you don't want to limit access such that you hamper a user's productivity.

Once you add a menu bar to a definition, you grant access to its menu items on an item-by-item basis. For example, if you added the UTILITIES menu bar to a definition, you could then opt to grant access to the Utilities, Use menu items but not to the Utilities, Process menu items. Or, you could grant access to only a few of the Use menu items, or to make some items Display Only.

In PeopleSoft applications, menu items represent components. If a component consists of more than one page, then selecting the menu item opens a cascading menu with more items—individual pages. If the component has more than one available action—Update/Display, Correction, and so on—choosing an item from the menu opens a cascading menu prompting you to choose an action.

So, the building blocks of menu item selections are pages and actions. These menu components are what you select or deselect when choosing which application menu items a user profile can access.

The following sections explain the subtle differences you'll encounter as you add access to the different types of PeopleSoft components. There are two categories of components to which you grant access permission.

- All PeopleSoft applications
- Page-driven PeopleTools.




With PeopleTools programs, the process of editing menu items varies. With page-based PeopleTools, such as Process Scheduler or Maintain Security, you can edit menu items just as you can for PeopleSoft applications. However, the other C++ PeopleTools programs don't allow you to grant item-by-item access; you can either access all the menus and menu items or you can't. Application Designer is an exception to this rule because you can restrict access to it at a more granular level.

The following procedure describes how to set access permissions to your PeopleSoft applications and your page-driven PeopleTools. In short, you begin at the Menu bar level and then drill down to the Component and Page level making the appropriate selections as you go.



The same procedure applies to both PeopleSoft applications and page-driven PeopleTools.

To add access to PeopleSoft menus, components, and pages

1. Click the **Pages** page.
2. In the **Menu Name** list click .
3. Using the search page, locate the appropriate Menu Name, and click it.

This returns you to the Menus page with the new item in the Menu name list.

4. Click Edit Components.

This takes you to the **Component Permissions** page. This page has the following lists:

- **Edit Pages.** An Edit Pages button appears for every Component under the current menu.
- **Authorized?** This display-only column reveals the Components in which the current Permission List has access to its pages.
- **Bar Label.** This shows the menu bar label that you users click to access a component.
- **Component.** This shows the name of each component beneath the authorized menu.

If you want to grant access to most or all items, click **Select All**. When you click **Select All**, all items are selected (highlighted). This button is handy when you want to quickly grant access to all menu items.

5. On the **Component Permissions** page locate the Component to which you want to grant access.

By default, when adding a new Permission List, no components are authorized.

6. Click the **Edit Pages** button associated with each component to which you want to grant access.

This takes you to the Page Permissions page. This where you set the actual user permissions on a page, as in what actions a user can complete on the page. You have the following options for each page that appears in the **Page** column:

- **Authorized?** By selecting this option you are allowing a user to access the page. After doing so, you need to decide the degree to which a user is authorized on a page by selecting **Display Only** or one or more of the available options in the **Actions** group.
- **Display Only.** By selecting this option you enable the user to view the information provided by the page, but not to alter any of the data. To enable write access to a page, its **DispOnly** value must be set to **No**, or unchecked. If the value is **Yes**, or checked, the system displays the page as read-only.
- **Actions.** If you want the user to be able to alter the data presented by the page, you need to select of the options that appear in the **Actions** group, such as **Add**, **Update/Display**, and **Correction**. The options that are available depend upon the options selected when the page was initially developed in Application Designer.

If you want to grant access to all pages and all the actions for each page, click **Select All**.

7. When you have finished making the appropriate selections, click **OK** on the Page Permissions page and then again on the Component Permissions page.

Keep in mind that for each menu name you will need to repeat each step.

## PeopleTools Permissions

The PeopleTools page enables you to grant access to the standalone PeopleTools, which include:

- Application Designer
- Data Mover
- Import Manager
- Query Security Access
- Object Security

General Pages **PeopleTools** Process Sign-on Times ▶

Permission List: ALLPANLS

Description:

**PeopleTools Permissions**

☒ **Application Designer Access** [Object Permissions](#) [Tools Permissions](#) [Misc. Permissions](#)

☒ Data Mover Access ☒ Object Security Access

☒ Import Manager Access ☒ Query Access

Maintain Security, Use, Permission Lists, PeopleTools, Misc. Tools

The standalone PeopleTools are those that are not page-driven; they are C++ programs that are not designed using Application Designer. The page-driven PeopleTools, such as Process Scheduler Manager, are designed using Application Designer, PeopleCode, and so on.

To grant access to standalone PeopleTools, select the checkbox associated with the appropriate PeopleTool.



With Application Designer the procedure is slightly more complex. The following links [Object Permissions](#), [Tools](#), and [Miscellaneous Objects](#) enable you to provide more detail to the Application Designer access permissions. Security for Application Designer is handled differently than for other PeopleTools and applications because rather than controlling access strictly by which menu items are available, security for this PeopleTool also controls what object definition types can be accessed and what degree of modifications can be made.

---

## Object Permissions

The Object Permissions page enables you to grant access to the definitions/objects that developers create using Application Designer. Notice that each type of object that you define with Application Designer appears in the Object Permissions list.



Object Permissions are separate authorizations than what you authorize in Object Security. With the App. Designer Objects list you add permissions to an object type, such as Application Engine programs. You grant access to specific objects, such as Payroll Application Engine programs, using Object Security.

---

**Object Permissions**

Permission List: ALLPANLS

Description:


Object	*Access
Activity	Full access
App Engine Program	Full access
Approval Rule Set	Full access
Business Interlink	Full access
Business Process	Full access
Component	Full access
Component Interface	Full access
Field	Full access
File Layout	Full access
HTML	Full access
Image	Full access
Menu	Full access

Full Access (All)

Read Only (All)

No Access (All)

Maintain Security, Use, Permission Lists, PeopleTools, Object Permissions

To grant permission to a particular object type, just click  in the Access Code column. This enables you to choose one of the following access levels:

- **Full Access.** Definitions of the specified type can be modified. For records, this setting allows access to the Build dialog, as well.
- **No Access.** No definitions of the specified type can be opened.
- **Read-Only.** Definitions of the specified type can be opened and viewed but *not* modified.
- **Update translates only.** This level only applies to Fields. This allows a user to modify only translate table values.
- **Data admin only.** This level only applies to Records. It allows a user to modify only those Record attributes found in the Tools, Data Administration menu (tablespaces).

You can set the access level of each of the Object types individually or you can set *all* object types in the list to the same access level at once by clicking one of the (ALL) buttons. To the right of the list, there is an (ALL) button for Full Access, Read Only, and a No Access.



If change control locking is enabled, the Change Control access setting (on the Tools tab) can override your Object Types settings.



For more information on enabling Change Control locking, see Change Tracking and Change Control.

---

## Tools Permissions

In addition to object definitions, Application Designer security also involves a collection of tools, such as Build and the PeopleCode Debugger, that you need to grant access for developers.

The tools within Application Designer include:

- **Access Profiles.** (Tools, Miscellaneous Objects, Access Profiles)
- **Build/data Admin.** (Build, Project and Tools, Data Administration)
- **Change Control.** (Tools, Change Control)
- **Language Translations.** (Tools, Translations)
- **PeopleCode Debugger.** (Debug, PeopleCode Debugger Mode).
- **SQL Editor.** (Application Designer's for adding SQL objects and statements to your applications and Application Engine programs.)
- **Upgrade.** (Tools, Change Control)

You can set access level individually for the **Tools** page options or you can use the (ALL) buttons to set “across the board” settings. Keep in mind that the access levels for some of the items don't correspond exactly to the names of the (ALL) buttons. And, not every button affects every access level for the Tools.

The following sections provide extra information for the settings on this tab for setting the access levels individually. Unless noted, the access levels are inline with the standard levels.

### Change Control

There are three Change Control access levels. These access levels, such as Developer or Supervisor, are only valid when change control is enabled. You enable Change Control locking using Application Designer.



For more information on enabling Change Control locking, see Change Tracking and Change Control.

---

- **Restricted access.** This access level restricts users from locking or unlocking objects. When change control locking is enabled, users with restricted access can only view Application Designer definitions—not create, modify, or delete them. This means a user can't lock any objects, and because they can't lock any objects, the user is not able to modify or delete them.



**Note.** With locking enabled, this setting overrides any Full Access settings on the Objects tab or Miscellaneous tab.

---

- **Developer access.** With developer access, a user is allowed to lock any unlocked objects and



to unlock any objects that they have locked.

- **Supervisor access.** A user with this access level can unlock any locked objects, regardless of who has locked them.

## Build and Data Administration

This is how you control access to the Build and Tools, Data Administration menu items. You can choose from the following access levels:

- **No access.** With this access level, a user cannot access the Build menu items or the Tools, Data Administration menu items.



**Note.** This setting is not available if you've set Records access to No Access or to Data Admin only.

---

- **Build scripts only.** A user with this access level can use the Build dialog, but the Execute SQL now and Execute and build script options are disabled. The Tools, Data Administration menu items are also disabled.



**Note.** This setting is not available if you've set Records access to No Access.

---

- **Build Online.** With this access level, a user can use all Build dialog options but the Tools, Data Administration menu items are still disabled.



**Note.** This setting is not available if you've set Records access to No Access.

---

- **Full data admin access.** A user with this access level can use all the **Build** dialog options and access the **Tools, Data Administration** menu items.



**Note.** This setting is not available if you've set Records access to No Access or to Read-only access.

---

## Language Translations

For this setting you can set only two levels of access, No access and Full access. You would enable this set of menu options for the individuals involved in translating or “globalizing” your applications.

## PeopleCode Debugger

Use this option to restrict the access of the PeopleCode Debugger.

## SQL Editor

Use this option to restrict developers from modifying the SQL in your applications.

## Upgrade

For Upgrade, selecting No access will disable all of the Upgrade menu items on the Tools menu. Developers could still access the Upgrade view and modify upgrade settings in the project definition, but they could not run any of the upgrade processes.

---

## Miscellaneous Permissions

The Miscellaneous page allows you to set the access levels for the Miscellaneous Objects items that appear on the Tools menu, which include Color, Field Format, Style, and Tool Bar.

**Miscellaneous Permissions**

Permission List: ALLPANLS

Description:

Feature	Access
Access Profiles	Full access
Color	Full Access
Field Format	Full access
Style	Full access
Tool Bar	Full access

Full Access (All)

Read Only (All)

No Access (All)

Maintain Security, Use, Permission Lists, PeopleTools, Misc. Permissions

Each of the Miscellaneous Objects can be set for No access, Read-only, or Full access. You can select the (ALL) buttons to grant across-the-board permissions.



For more information on the options on Application Designer's Tools, Miscellaneous Objects menu, see Using Application Designer.

---

## Process

Just as you define permissions for the pages a user can access, it is also critical to specify what batch (and online) processes that users can invoke through Process Scheduler. Typically, Process Groups are grouped by department or task. For instance, the batch programs having to do with

your payroll department probably all belong to the PAYROLL Process Group, or something similar.

Maintain Security, Use, Permission Lists, Process

Then when you create a Process Permission List, you add the appropriate Process Groups so that a user belonging to a particular Role can invoke the proper batch programs to complete their business transactions. You do this using the Process Group Permissions page.

In addition to invoking the proper batch programs, you also want to specify to what capacity a user, or Role, can modify certain Process Scheduler settings. You do this using the Process Profile Permissions page.

---

## Process Group Permissions

Process groups are collections of Process Definitions that you create using Process Scheduler. Typically, you group Process Definitions according to work groups within your organization, and only users who belong to a particular workgroup can invoke batch processes included in a specific Process Group. For instance, you may have a set of Process Definitions that relate to your Human Resources department and another set for your Manufacturing department.

Regardless of how you organize your Process Definitions, you must assign process groups to a Permission List. Users can run only those processes through Process Scheduler that belong to process groups assigned to their Role.

**Process Groups**

Permission List: ALLPANLS

Description:

View All First 1-3 of 3 Last

Process Group				
1	INALL	Q	+	-
2	INCOBOL	Q	+	-
3	TLSALL	Q	+	-

Maintain Security, Use, Permission Lists, Process, Process Group Permissions

The **Process Groups** page lists the various process groups associated with a Permission List. You insert an item into the list using the plus sign button and by doing so you grant access to that Process Group.



For more information on creating process groups and Process Scheduler, see Process Scheduler.

The following procedures cover the tasks involved with customizing Process Group access. Use the plus and minus signs to add and remove Process Groups from a permission list.

## Process Profile Permissions

Process Scheduler security involves more than simply adding a few Process Groups to a Permission List. You also need to specify to what capacity a Role (or set of users) can modify certain Process Scheduler settings. The Process Profile definition determines the default Process Scheduler settings for a user.

For instance, with the Process Profile, you specify such settings as where the system delivers the output of the process, whether the user can update the Process Request, and so on.

Permission List: ALLPANLS	
Description:	
<b>Workstation Destinations</b>	<b>Allow Process Request</b>
File: [%OutputDirectory%]	*View By: All
Printer: [%DefaultPrinter%]	*Update By: Owner
<b>Server Destinations</b>	<b>Allow Requestor To</b>
File: [%OutputDirectory%%]	<input checked="" type="checkbox"/> Override Output Destination
Printer:	<input checked="" type="checkbox"/> Override Server Parameters
<b>OS/390 Job Controls</b>	<input checked="" type="checkbox"/> View Server Status
Name:	<input checked="" type="checkbox"/> Update Server Status
Accnt:	<input checked="" type="checkbox"/> Enable Recurrence Selection
	<input checked="" type="checkbox"/> Run Client Process
OK	Cancel

Maintain Security, Use, Permission Lists, Process, Process Profile Permissions

The following sections describe the options that you can select for a process profile.

## Workstation Destinations

This section only applies to Windows workstations. If a process is scheduled to run on the Windows workstation, you can specify where the process delivers the output file or hardcopy. With processes running on a Windows workstation, you have the following options:

- **File.** If the output is going to file, then specify the directory to which the file should be written. %OutputDirectory% is a meta-variable that resolves to the Output Directory specified for a workstation on the Process Scheduler tab of the Configuration Manager. You can override this value with a specific directory if necessary, however, in most cases, the Output Directory is sufficient.
- **Printer.** Specify the network, or local, printer to which the hardcopy output should be sent. %DefaultPrinter% is a meta-variable that resolves to the printer defined as “default” for a particular workstation.

## Server Destinations

There are output variables that you can specify when running processes or jobs on a server. With processes and jobs on the server, you have the following options:

- **File.** If the output is going to file, then specify the directory to which the file should be written. %%%OutputDirectory%% is a meta variable that resolves to the output directory that you’ve specified in PSADMIN (or PSPRCS.CFG) for the Process Scheduler Server Agent.
- **Printer.** Specify the network, or local, printer to which the hardcopy output should be sent. You’ll need to explicitly specify the printer; there are no meta-variables available on the server for this value.

## OS/390 Job Controls



This group of options only applies to DB2 for the OS/390.

All the Process Scheduler's Shell JCL's, use meta-strings to pass data stored in the database. Process Scheduler takes advantage of meta-strings to generate the JCL job cards based on the user who initiated the request. For example, Job Name and Job Account can be passed by setting the **Name** and **Account** values, respectively, on the Process Profile page. For OS/390 you have the following options:

- **Job.** Enter %JOBNAME%
- **Account.** Enter %JOBACCT%.



For more information on JCL meta-variables/strings, see your RDBMS documentation and the PeopleSoft *Installation and Administration* guides.

## Allow Process Request

The **Allow Process Request** options apply to using the Process Monitor. Using these options you can restrict the processes that a user can view and update. For the Process Monitor you can specify restrictions described in the following topics.

### *View By*

Here you can specify what a user can view in the Process List. You have the following options:

- **Owner.** Select this radio button if you only want users to be able to view processes for which they are the owner, or processes that they submitted.
- **All.** Select this radio button if you want a set of users to be able to view all processes and jobs submitted by any user in the system.
- **None.** If you do not want a set of users to be able to view the status of their submitted processes, select this radio button. By doing so, no entries appear in the Process List.

### *Update By*

Here you can specify whether or not a user can update the status of a submitted process by way of the Process Monitor's Process Detail page in the Update Process group. For instance, you decide whether or not the user can restart or cancel a request by setting an Update By value.

You have the following options for Update By:

- **Owner.** Select this radio button if you only want a set of users to be able to update processes for which they are the owners, or processes that they submitted. For instance, they could only

restart a request that they originally submitted.

- **All.** Select this radio button if you want a set of users to be able to update all processes and jobs submitted by *any* user in the system. Most likely, this is the authority that you would grant only to system administrators.
- **None.** If you *do not* want a set of users to be able to update the status of their submitted processes, select this radio button. By doing so, the options in the **Update Process** group are disabled.



Be careful as you grant update authority to submitted processes. An inexperienced user can easily disrupt batch processing by deleting or holding processes. This is especially true with restarting processes. If a program is not coded for a “restart” then users should *not* be able to restart it. Restarting a program that is not properly coded to acknowledge the previous program run can threaten data integrity.

---

---

## Allow Requester To

The **Allow Request To** options apply to using the Process Monitor and Process Scheduler Request page. These options, discussed in the following topics, allow you to restrict the authority that a user has while monitoring scheduled processes.

### Override Output Destination

Select this option to allow a user to change the value in the Output Destination column on the Process Request page.

### Override Server Parameters

Select this option if you want a user to be able to select the Server Name and modify the Run Date/Time group on the Process Scheduler Request page.

### View Server Status

This option allows a user to access the Server List page in the Process Monitor.

### Update Server Status

This option allows a user to suspend, restart, or bring down a server using the Server Detail page from the Server List in Process Monitor.

## Enable Recurrence Selection

For processes and jobs scheduled to run on the server, you can apply a Run Recurrence value. To restrict being able to select a Run Recurrence, make sure this option is not selected.

## Run Client Process

This option only applies to sites using the Windows workstation to access PeopleSoft. This option allows you to control whether a user can run a batch process on the local Windows workstation. You might select this option in situations where you want optimum performance and to restrict the chance that a user might run an SQR program on the workstation.



PeopleSoft does not recommend running SQRs on a Windows workstation. The Access ID and Access Password may be exposed. PeopleSoft recommends using the Report Manager to distribute the output of SQRs and other reports.

## Signon Times Permissions

Signon days and times specify when users are authorized to sign on to the PeopleSoft online system. If users are signed on to the system when the signon time expires, they are automatically signed off.

*Day	Start Time	End Time	Time		
Sunday	00	00	23	59	+ -
Monday	00	00	23	59	+ -
Tuesday	00	00	23	59	+ -
Wednesday	00	00	23	59	+ -
Thursday	00	00	23	59	+ -
Friday	00	00	23	59	+ -
Saturday	00	00	23	59	+ -

Signon Times page

This page lets you pick a day from the **Day** drop-down lists and then set a signon duration using the **Start Time** and **End Time** edit boxes. To add and delete days from the **Day** list, click **+** **-** respectively.

Signon times use the 24-hour clock and run *through* the **End Time** value. For example, a user with an **End Time** of 16:30 can use the system until 4:31 PM, 1:00 PM is 13:00; noon is 12:00; and midnight is 00:00.



To create a signon time that spans multiple days, you must use adjoining signon times. For example, to create a signon time running from 8 PM Tuesday to 6 AM Wednesday, you need a Tuesday **Start Time** of 20:00 and **End Time** of 23:59. Then you need to add a Wednesday signon time with a **Start Time** of 0:00 and an **End Time** of 5:59.

When adding a new signon time, the **Start Time** defaults to 0:00 and the **End Time** to 23:59. You need to customize the signon times or else the user will, by default, have access to the all day, every day. By default, all of the days of the week appear in the Signon Times list. However, you can delete as many as you like, and you can even add multiple signon periods per day.

A single day can have more than one signon period as long as the periods don't overlap one another. If there are more than one non-overlapping signon periods for one day, that day will appear once for each of those signon periods.

When customizing signon authority, you can modify a default signon time period, add a new signon time, or delete a signon time.

## Component Interface Permissions

Just as you grant access to PeopleSoft pages, you also need to grant access to any Component Interfaces that a user may need to use to complete business transactions. You do this using the Component Interfaces page.

Sign-on Times Component Interface Message Monitor Web Libraries Query

Permission List: ALLPANLS

Description:

Name	Edit	
ABS_HIST	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
BUS_EXP	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
BUS_EXP_TEST	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
DISCIPLN_ACTN	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
NVSRPTS	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
PROCESSREQUEST	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
PSACTIVITYLOG	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
SUPPORT_DOC_TABLE	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
USER_PROFILE	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
WF_MONITOR_SEND	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
WF_TIMEOUT_DATA	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
WORKLIST	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>
WORKLISTENTRY	<a href="#">Edit</a>	<a href="#">+</a> <a href="#">-</a>

Maintain Security, Use, Permission Lists, Component Interfaces

The way you add access to Component Interfaces is similar to adding page access. It's a matter of first inserting a Component Interface into the Component Interface list using the [+](#) button, and then setting the method access mode for each method within the inserted Component Interface.

**Component Interface Permissions (48,188)**

ABS\_HIST

First 1-4 of 4 Last

Method	*Method Access
Cancel	Full Access
Find	Full Access
Get	Full Access
Save	Full Access

Full Access (All)  
No Access (All)

OK Cancel

Maintain Security, Use, Permission Lists, Component Interfaces, Edit

On the Component Interface Permissions page you grant full access or no access to the methods that appear in the Methods list. Use the (ALL) buttons to grant access to all or no access to all.

## Message Monitor Permissions

The Application Message Monitor is the utility that administrators use to monitor the messages and the components involved in your application messaging system. You add access to the Application Message Monitor using the Pages page, but after you add access to the Message Monitor, you need to customize user access to your channels.

You use the Message Monitor Permissions page to grant access to Message Channels, and by doing so you allow an administrator to view or edit messages within a particular channel.

Sign-on Times Component Interface Message Monitor Web Libraries Query

Permission List: ALLPANLS

Description:

First 1-13 of 13 Last


Channel Name	*Access		
BUS_EXP_MSG_CHNL	Full	+	-
EMAIL_CHNL	Full	+	-
JOB_CHANNEL	Full	+	-
MARKET_RATES	Full	+	-
MARKET_RATE_LOAD	Full	+	-
QE_GAME_CHNL	Full	+	-
QE_PLYRTRD_CHNL	Full	+	-
QE_PLYR_CHNL	Full	+	-
QE_UPS_TM_CHNL	Full	+	-
ROLESYNCH_CHANNEL	Full	+	-
TREE_MAINT	Full	+	-
USER_PROFILE	Full	+	-
WORKLIST_CHNL	Full	+	-

Insert All Channels

Remove All Channels

Maintain Security, Use, Permission Lists, Message Monitor

To grant access to a Message Channel

1. Add a channel to the Channel Name list using the  button.
2. From the drop-down list in the **Access** column select the appropriate access level.

If you want to apply a uniform access level, use the Insert All Channels or Remove All Channels buttons.

## Web Libraries Permissions

A Web Library is a derived/work record that has a name that starts with WEBLIB\_. All PeopleSoft iScripts are imbedded in records of this type. An Internet Client Script is a specialized PeopleCode function that generates dynamic web content.

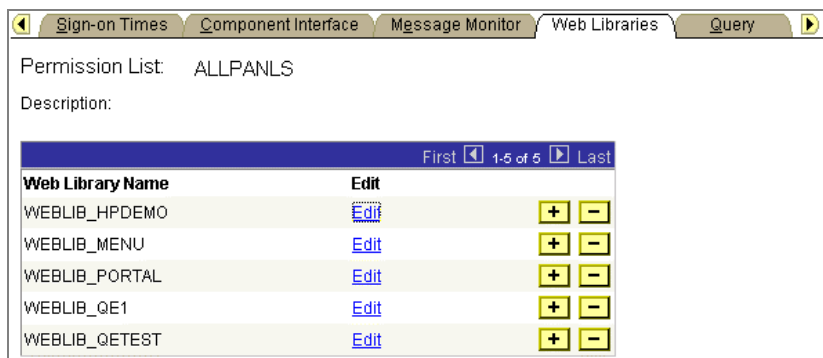
After you add the Web Library, you can set the access for each script function individually. Invoking an iScript requires the assembly of a URL. Developers "assemble" the URL using PeopleCode. If users are not authorized for a particular web library or script then they can't invoke it.



For more information on Web Libraries, see PeopleCode Reference.

Making sure users have the proper access to web libraries is important for administrators. For example, the default navigation system for PIA users is implemented using a web library. If users do not have the proper authorization to the web library and its associated scripts, then they won't get far in the system.

You set security access to the script functions using the **Web Libraries** page.



Web Library Name	Edit		
WEBLIB_HPDEMO	<a href="#">Edit</a>	+	-
WEBLIB_MENU	<a href="#">Edit</a>	+	-
WEBLIB_PORTAL	<a href="#">Edit</a>	+	-
WEBLIB_QE1	<a href="#">Edit</a>	+	-
WEBLIB_QETEST	<a href="#">Edit</a>	+	-

Maintain Security, Use, Permission Lists, Web Libraries

The following procedures cover the tasks involved with setting access to Web Libraries.

To grant access to a Web Library

1. In the **Web Library Name** list locate the Web Library to which you want to grant access.
2. Click **edit** to open the Web Library.

The functions contained in that library appear on the following page.

3. In the **Function** list locate the function to which you want to grant access.
4. Save your work.

## Query

Query takes advantage of user profiles and row-level security. With Maintain Security you can control what query operations a user can perform and what data they can access while they are using Query.

Maintain Security, Use, Permission Lists, Query

This section contains information concerning how to establish a security scheme for Query, which includes the following:

- Defining Access Groups
- Defining Query Profiles

There are other security related topics, such as building security query trees and creating record definitions in Application Designer such that Query enforces row-level security, that are beyond the scope of Maintain Security.



For more information on other Query Security considerations, see the PeopleSoft Query.

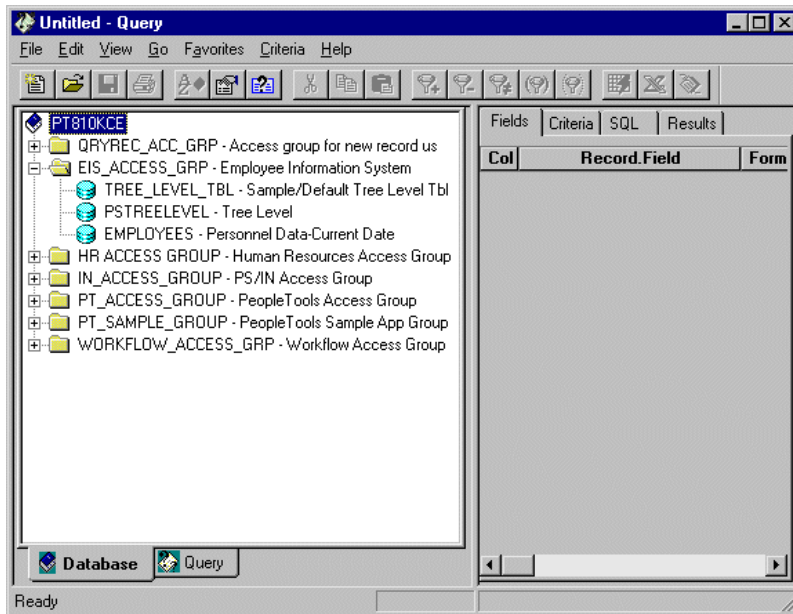
---

## Defining Access Groups

When you first open Query, it displays either an access group structure or an alphabetical list of records to which you have access. You can switch between these two views by selecting **View**,

**Preferences, Component View** and turning the **Show Access Groups** option on or off. Access groups provide a way for you to logically organize the record components to control security access within Query. *It is not a physical representation of your database.* The record components shown are those that the user has been granted access to.

In the example below, records are divided into functionally related access groups such as the Employee Information System, Human Resources Access Group, and so on. The folder icon indicates access groups. The database icon indicates record components.



Query Access Groups

You can only generate queries on and retrieve information from the tables whose record definitions are within these access groups. If, for example, you were querying an order table and wanted to display data from a related table (like the customer name rather than the customer code), you must have both tables—the order table and the customer prompt table—in your access groups.

Access groups are nodes in a query tree, which you build with Tree Manger. Once you've built a query tree, you give users access to one or more of its access groups. Then they can generate queries on any tables in the access groups accessible to them.

To create new queries, or even to run existing ones, users must have access rights to the record components used in the queries. Once you've built your query trees, you need to grant users access to them. You can grant and restrict access to entire query trees or portions of them through the Maintain Security, Access Groups page.

Permission List: ALLPANLS  
 Description:

*Tree Name	*Access Group	Accessible
QRY_CLONE_RECS	QRYREC_ACC_GRP	<input checked="" type="checkbox"/> + -
QUERY_TREE_EIS	EIS_ACCESS_GRP	<input checked="" type="checkbox"/> + -
QUERY_TREE_HR	HR ACCESS GROUP	<input checked="" type="checkbox"/> + -
QUERY_TREE_IN	IN_ACCESS_GROUP	<input checked="" type="checkbox"/> + -
QUERY_TREE_PT	PT_ACCESS_GROUP	<input checked="" type="checkbox"/> + -
QUERY_TREE_PT_APPS	PT_SAMPLE_GROUP	<input checked="" type="checkbox"/> + -
QUERY_TREE_WF	WORKFLOW_ACCESS_GRP	<input checked="" type="checkbox"/> + -

OK Cancel

Maintain Security, Use, Permission Lists, Query, Access Profiles

This page lists the **Access Groups** added to a Permission List.

To add an Access Group to a Permission List

1. Within Maintain Security, choose **Use, Permission Lists**.
2. Open the desired Permission List and select **Query, Access Groups**.
3. Select a Tree Name.

Use the drop-down lists to find the **Tree Name** you want.

4. Select the highest **Access Group** that the user can access.

Use the drop-down lists to find the **Access Group** you want. The system displays only the access groups in the selected query tree.

The **Access Group** selected should be the highest-level tree group to which this Permission List needs access. The **Accessible** check box is on by default. For example, users in the ALLPANLS permission list have access to all record components in the EIS\_ACCESS\_GRP and all access groups below it in the QUERY\_TREE\_EIS query tree—in other words, to all record components in the tree.

5. Deselect **Accessible**, if desired.

If you want to grant access to *most* of the record components in a high-level access group, but want to restrict access to one of the lower-level groups, you can add a new row for the lower-level access group and deselect the **Accessible** check box. Users can then access all record components within the higher-level group *except* for those you explicitly made inaccessible.



Because it hinders system performance, we don't recommend deselecting **Accessible** for lower-level access groups. If you need to restrict access to record components on a particular branch of a tree, you should consider creating a new tree for those definitions. Attempting to expand an access group that is not accessible will cause all access groups below that access group to be loaded into memory.

---

## 6. Save your changes.



When the system loads an access group into memory for the first time, you'll most likely experience a small delay. This delay is the result of a physical database read for each record component that is associated with that access group. For this reason, we don't recommend grouping a large number of record components into a single access group.

---

## Defining Query Profiles

Query Profiles specify what query operations are available to users. The first level of security is access to PeopleSoft Query itself. If you don't give users access to Query when you define their user ID, they can't create or run queries. Not every user needs to create their own queries.



To create queries, a user needs access to PS/Query. PS/Query only runs on Windows workstations. PIA users can run queries only.

You can give users the right to run queries but not create them, or to create regular queries but not workflow queries, or you can restrict the SQL operations they can perform. For users who do have access to Query, you control what query options or functions are available through their *query profile*.

Query profiles specify the type of access you'll permit users to have when they work with PeopleSoft Query. For example, you may want certain users only to run existing queries, not create new ones. For those you do allow to create new queries, you might want to restrict the types of queries they can create. You can also determine the output options users have for generating their queries.

By default, the query profile gives users access to all Query features—assuming, of course, that you gave them access to Query.

Permission List: ALLPANLS	
Description: <input type="text"/>	
<b>PeopleSoft Query Use</b> <input type="checkbox"/> Only Allowed to run Queries <input checked="" type="checkbox"/> Allow creation of Public Queries <input checked="" type="checkbox"/> Allow creation of Workflow Queries Maximum Rows Fetched: <input type="text"/> (0 = Unlimited)	<b>Advanced SQL Options</b> <input checked="" type="checkbox"/> Allow use of Distinct <input checked="" type="checkbox"/> Allow use of 'Any Join' <input checked="" type="checkbox"/> Allow use of Subquery/Exists <input checked="" type="checkbox"/> Allow use of Union <input checked="" type="checkbox"/> Allow use of Expressions Maximum Joins Allowed: <input type="text" value="9"/> (9 = Unlimited) Maximum 'In Tree' Criteria: <input type="text" value="9"/> (9 = Unlimited)
<b>PeopleSoft Query Output</b> <input checked="" type="checkbox"/> Run <input checked="" type="checkbox"/> Run to Excel <input checked="" type="checkbox"/> Run to Crystal	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Maintain Security, Use, Permission Lists, Query , Query Profile

## PeopleSoft Query Use

The Query Profile page contains the following options:

- **Only Allowed to run Queries.** Prevents users from being able to create queries, and also restricts them from running PeopleSoft Query. The values of the remaining options in this group are irrelevant if you have selected this option. This option exclusively limits the user to **run only** access to PeopleSoft Queries. Users who have this option checked in their Query Profile cannot modify queries or open the PeopleSoft Query tool.
- **Allow creation of Public Queries.** Determines whether or not users can create public in addition to private queries.
- **Allow creation of Workflow Queries.** Determines whether or not users can create workflow queries in addition to private queries. A Workflow query is a query used in PeopleSoft Workflow, either as a database agent query or a role query. Because they're part of the workflow, these queries are able to circumvent security restrictions; that is, the system doesn't check access group rights while running the query. If you want to make sure that users can't bypass the system's security, *don't* select **Allow creation of Workflow Queries**. If, on the other hand, users need to create role queries or database agent queries, select it.



For more information on database agent queries and role queries, see Types of Queries.

- **Maximum Rows Fetched.** Some queries can return many data rows. For performance or time considerations, you may want users to view only some of those rows rather than all of them. You can restrict the number of rows retrieved by a query by entering a suitable number in this edit box.



## PeopleSoft Query Output

At least one of the **PS/Query Output Options** must be selected for the user to be able to view the results of queries. The output options are as follows.

- **Run.** Query displays the query results in a view-only grid control, the Results tab in Query. This option is useful as users are refining their queries.
- **Run to Excel.** Query passes the query results to Microsoft Excel, where you can analyze the results further.
- **Run to Crystal.** Query passes the query results to Crystal Reports Pro, a report formatter, where you can use predefined formats or create new ones to print the results of your query.

## Advanced SQL Features

If you've given the permission list the ability to create new queries, designate the Advanced SQL Features they can use. It's a good idea to restrict less experienced users from generating complex queries, since such queries can affect system performance.



For more information on Query's advanced SQL options, see Advanced Query Options.

---

## Mass Change Security

Mass Change security controls:

- What Mass Change templates a user can access to create new definitions.
- Whether a user can run Mass Change definitions online.
- What Mass Change definitions a user can open, view, or execute. These definitions must also be based on a template with the same PeopleSoft Owner as the user.



A user inherits their Mass Change authorizations through their *primary* permission list, not through roles.

---

Maintain Security, Use, Permission Lists, Mass Change

Before you can use a new template to create definitions, you must have permission to access to it.



For more information on Mass Change templates see Mass Change.

To modify Mass Change template permissions

1. Add or remove templates from the Authorized Templates list.

To add a template, place your cursor in an existing row and click the plus sign button. Then select a template from the drop-down list. To delete a template, place your cursor in the field that contains the template, and click the minus sign button.



If you get an error message telling you that no records exist for the specified keys, you'll have to add security privileges for the profile.

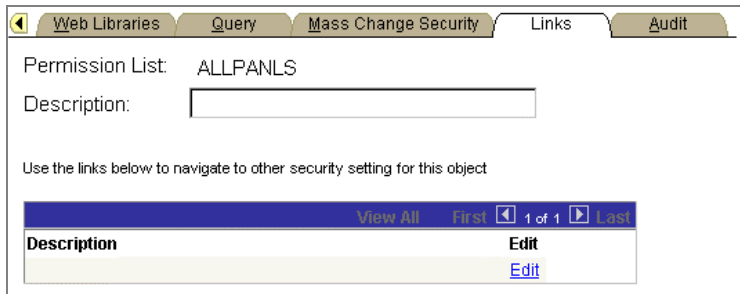
2. Select or deselect **OK To Execute Online?**, as needed.

When you have enabled the **OK To Execute Online?** option, users with the given permission list possess the ability to run Mass Change definitions online after saving any modifications to the Mass Change Definitions pages.

3. Save your work.

## Links

The Links page allows you to add links easily to other pages within your PeopleSoft system that pertain to a particular Permission List. For instance, perhaps a PeopleSoft application requires a specific security setting to be attached to a Permission List. Assuming that this application-specific setting appears on a page not in Maintain Security, you just add a link to that page so that anyone updating the Permission List can easily navigate to it.



Web Libraries Query Mass Change Security Links **Audit**

Permission List: ALLPANLS

Description:

Use the links below to navigate to other security setting for this object

View All First 1 of 1 Last

Description	Edit
	<a href="#">Edit</a>

Maintain Security, Use, Permission Lists, Links

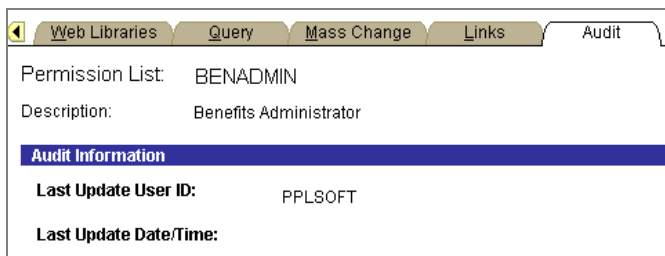
You create your inventory of links to security settings that exist outside of Maintain Security using the Security Links page (on the Setup menu). Once created and assigned to a security definition, such as a permission list, then the links appear in the security definition's list of links.



For more information on Security Links see Security Links.

## Audit

The Audit page is a read-only page that allows you to determine when a Permission List was last updated and by whom.



Web Libraries Query Mass Change Links **Audit**

Permission List: BENADMIN

Description: Benefits Administrator

**Audit Information**

Last Update User ID: PPLSOFT

Last Update Date/Time:

Maintain Security, Use, Permission Lists, Audit

You can also view who has made changes to security tables using the Database Level Auditing feature.



For more information on database audit, see Signon PeopleCode.



## CHAPTER 3

# Roles

Roles are an intermediate object that exist between Permission lists and User Profiles. They are designed to aggregate Permission Lists so that you can arrange permissions into meaningful collections. If you implement dynamic Roles, then Roles enable you to add permissions to users dynamically, which reduces administration tasks.



---

In previous releases, Roles were associated with PeopleSoft Workflow. PeopleTools has expanded their definitions to include system permissions. There is only one role object, and you maintain it within Maintain Security.

---

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

You assign data permissions directly to the User Profile either through a Primary Permissions list or Row Security Permissions list. Navigator Homepage and Process Profile are also assigned directly to the User Profile.

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

Other users may obtain membership in a role programmatically. You can run a batch process that executes predefined role rules and assigns roles to user profiles according to these rules. This approach is called dynamic membership, and users who become role users of a particular role programmatically are Dynamic Role Users.

The dynamic role assignment is the way to make your security system scale to meet the demand of an ever-increasing user population. Otherwise, members of your IT staff need to manually make every change to a user profile. If you have thousands of users in your system, the security administrator becomes the bottleneck.

At the top of each page you'll see the Role Name and Description edit box. The Role Name is read only and reflects the name you chose for the Role when you created it. The Description edit box is where you have the option of adding a short description to help you identify a particular Role on the other pages.

Also at the top of each page, there is Role Status group box. You can select **Active** or **Inactive**. **Active** means the Role is ready to accept members, or users, and **Inactive** means that the Role is off limits. For example, Roles that you are still modifying might be set to Inactive. Users belonging to an "inactive" roll can not sign on to the system until you reactivate the role.

Before we discuss the options you select in the Roles component, you need to understand the options you have for assigning your Roles.



**Important!** A page named Role Grant appears within the Roles component in the following examples. This tab is reserved for future use and is only used internally by PeopleSoft. Currently, this page is not deployed for customer use.

Before you get started working with roles, you'll want to keep the following basics in mind.

- To create a new role definition, select **Use, Roles** and then click **Add a New Value**.
- To clone a role definition, select **Use, Role Save As**, and then enter the name of the role you want to clone and provide a new name.
- To delete a role definition, select **Use, Delete Role**, and then select the unneeded role, and click Delete.

## General

The General page enables you to describe the role and disable the Role if needed as well as add a long description to help identify the role.

PeopleTools, Maintain Security, Use, Roles, General

The text you add in the Description edit box appears throughout the component at the top of each page. The text you add in the Long Description should provide specific details describing the purpose of the role.

To temporarily disable, as in for testing purposes, select the **Role Disabled** checkbox in the Role Status group. If you no longer need the role, you should disable it.

## Permission Lists



The permission lists are the objects that control what a user can and can't access in your system. In most cases, users have a collection of permission lists. Once you have completed the process of defining Permission Lists, you need to grant those permissions to Roles.

It's very important to keep in mind that a user's access is determined by the sum of all the permission lists. For instance, let's say you add permission list X and permission list Y to a role. Permission list X has a signon time of 8 AM to 5 PM and permission list Y has a signon time of 1 PM to 9 PM. In this scenario, the users assigned to this role can sign on to the system between the interval 8 AM to 9 PM. If this is your intention, then there is nothing to become concerned about. The point is that you need to be very conscious of the contents of each permission list prior to adding them to a role.

PeopleTools, Maintain Security, Use, Roles, Permission Lists

Remember that the users inherit the combination of all of the permission lists applied to each role to which they belong.

To add a Permission List to a Role

1. Click .
2. In the **Permission List** column click .
3. From the search page, click the Role that you want to add.

## Members

The Members page is a display only page that reveals the current list of Static Members that belong to the current Role.

When you add a Role to User Profile using the Maintain Security, User Profile pages, the User ID and Description (Name) of the user appears in the Members list. When you remove the Role from the User Profile, then the corresponding User ID and Description do not appear in the Members list.



This page shows those users who are added to a role using the static approach.

---

## Dynamic Members

This is a display-only page that reveals the current list of members/users who belong to the current role dynamically as a result of business rule invoked in real-time or batch mode. If you are not taking advantage of the Dynamic Members functionality, then this list is not populated.

PeopleTools, Maintain Security, Use, Roles, Dynamic Members

This page is also where you point to the rules that the dynamic rules process needs to invoke for a particular role. As stated previously, a dynamic role rule is defined in PS/Query, PeopleCode, or your LDAP directory.

---

## Assigning Roles

In order for the rule to successfully assign a particular role to the appropriate users, you need to select the rule type you have in place for a particular role, and then specify the object that contains the rule you coded.



You need to define your role rules before you apply the options in the Rule group on the Dynamic Members page.

If defined your rule with PS/Query, select Query Rule Enabled. The Query Rule group appears below the Rules group. Use the Query drop down list to select the query that contains your role rule.

Assigning a Query Rule



Likewise, if your rule is in the form of a PeopleCode program, select PeopleCode Rule Enabled. The PeopleCode Rule group appears. There you specify the Record, Field, Event, and Function associated with your role rule.

If your role rule is based on information in your directory server, select Directory Rule Enabled. With a directory-based rule you need to assign directory groups. Notice that, by default, the PeopleCode Rule appears because Directory rules are implemented using a PeopleCode program. The DynRoleMembers PeopleCode program uses the Directory business interlink to retrieve user and group information from the directory. You can see exactly how it works by viewing the program in the Application Designer.

Assigning a Directory Rule

Click Assign Directory Groups to select a particular directory group that exists in your LDAP server hierarchy. For instance, say you have your LDAP server grouped by geographic region. If so, your rule could maybe, assign a new self-service role to all users in the North America group.

Selecting a Directory Group

Use the Directory Group drop-down list to select the appropriate directory group value. The values are derived from the LDAP data that you import using the Directory Group Import process.



For more information on the Directory Group Import process, see Directory Group Import.

After you run a rule, you click **Refresh** to repopulate the grid with updated information. Because the role rules get executed by an Application Engine program that runs through Process Scheduler, you can use the **Process Monitor** link to view the status of the program run.

After the program runs, it publishes a message containing the list of users in the role, and exits. The program does not update any tables; the message (subscription PeopleCode) performs the actual database updates. To check the status of the message, you use the **Message Monitor Link**. Just because the dynamic roles program completed successfully, that does not necessarily mean your roles are updated. The associated message must also be successfully delivered.



For more information on Process Scheduler, see Process Scheduler. For more information on setting up the application messaging system, see PeopleSoft Application Messaging.

## Query Rule Example

This section describes the process of creating a Query rule that assigns dynamic role membership. This general example should also help to illustrate similar techniques that you would use for a PeopleCode or LDAP rule.

In the following example, we need to create a query that selects user IDs based on job criteria. Specifically, we need to find all the users that currently have the job code KC012 (Human Resource Analyst), and add them to the appropriate role. The assigned role grants them access to the necessary components that a Human Resource Analyst needs.

In order to do so, we perform the following:

- Create a View.
- Create the query.
- Run the dynamic rule.

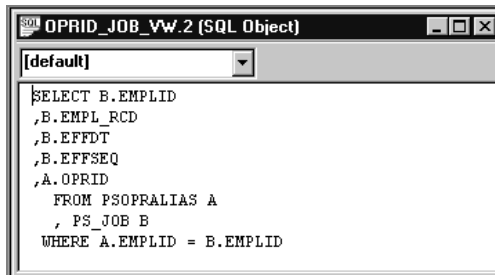
### Create a View

You can create a view for the information that your query needs. For example, the view definition might be similar to the following.

OPRID_JOB_VW (Record)											
Record Fields		Record Type									
Num	Field Name	Type	Key	Ordr	Dir	Cur	Src	List	Sys	Audt	Default
1	EMPLID	Char	Key	1	Asc		No	No	No		
2	EMPL_RCD	Nbr	Key	2	Asc		No	No	No		
3	EFFDT	Date	Key	3	Desc		No	No	No		%date
4	EFFSEQ	Nbr	Key	4	Asc		No	No	No		
5	OPRID	Char					No	No	No		

Dynamic Role Rule—Query View

The SQL Object as follows.

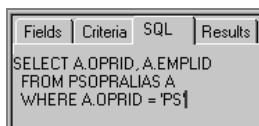


Dynamic Role Rule—Query View SQL Object



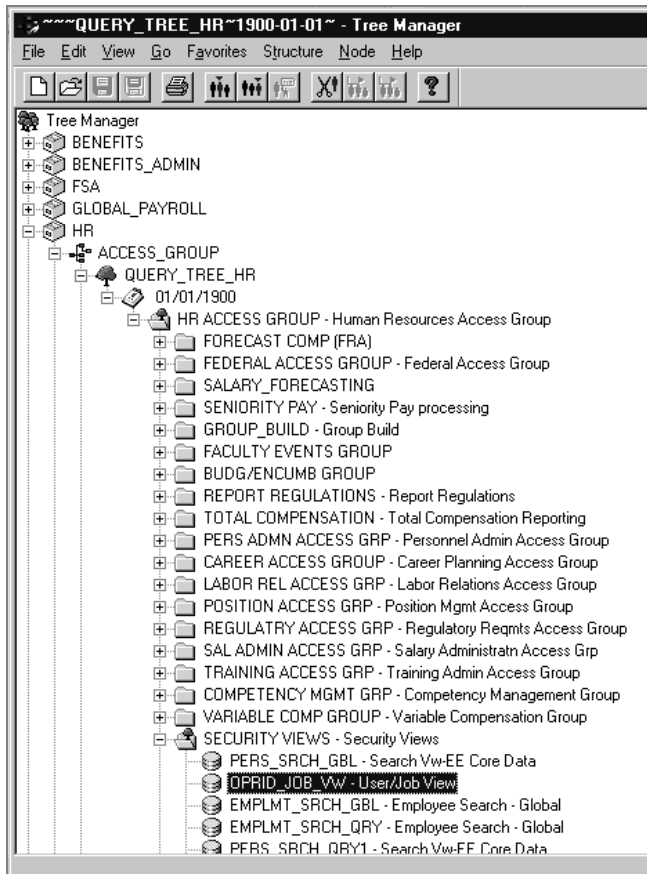
The OPRID must not be a key in this view because PeopleTools appends AND OPRID = “current users oprid” in Query. This occurs if we use the record OPRALIAS directly in our query.

And the SQL appears as follows.



Query View SQL

After you create the view, you add it to the appropriate query tree. In this case, we add the new view to the QUERY\_TREE\_HR.



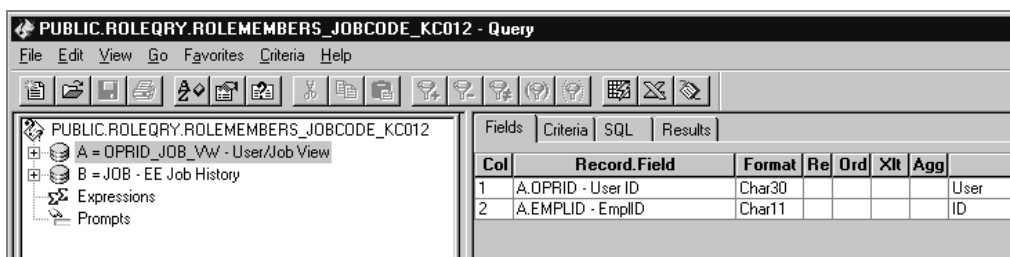
Adding the View to a Query Tree



For more information on creating views, see Application Designer.

## Create a Query

With the view created, you then create a query. In this example, the properties we assign to the query enable it to assign a role to users who currently have the Job code KC012, Human Resource Analyst.



Query Definition

The Query contains the following criteria.

Fields	Criteria	SQL	Results
Logical	Expression 1	Operator	Expression 2
	A.EFFDT - Effective Date	Eff Date <=	Current Dt (EffSeq = Last)
AND	A.EMPLID - EmplID	equal to	B.EMPLID - EmplID
AND	A.EMPL_RCD - Empl Rcd Nbr	equal to	B.EMPL_RCD - Empl Rcd Nbr
AND	B.EFFDT - Effective Date	equal to	A.EFFDT - Effective Date
AND	B.EFFSEQ - Effective Sequence	equal to	A.EFFSEQ - Effective Sequence
AND	B.SETID_JOBCODE - Job Code	equal to	SHARE
AND	B.JOBCODE - Job Code	equal to	KC012

### Query Criteria

The SQL for the query is as follows.

Fields	Criteria	SQL	Results
<pre> SELECT A.OPRID, A.EMPLID FROM PS_OPRID_JOB_VW A, PS_JOB B, PS_EMPLMT_SRCH_QRY B1 WHERE B.EMPLID = B1.EMPLID AND B.EMPL_RCD = B1.EMPL_RCD AND B1.ROWSECCLASS = 'DPALL' AND (A.EFFDT = (SELECT MAX(A_ED.EFFDT) FROM PS_OPRID_JOB_VW A_ED WHERE A.EMPLID = A_ED.EMPLID AND A.EMPL_RCD = A_ED.EMPL_RCD AND A_ED.EFFDT &lt;= SUBSTRING(CONVERT(CHAR, GETDATE(), 121), 1, 10)) AND A.EFFSEQ = (SELECT MAX(A_ES.EFFSEQ) FROM PS_OPRID_JOB_VW A_ES WHERE A.EMPLID = A_ES.EMPLID AND A.EMPL_RCD = A_ES.EMPL_RCD AND A.EFFDT = A_ES.EFFDT) AND A.EMPLID = B.EMPLID AND A.EMPL_RCD = B.EMPL_RCD AND B.EFFDT = A.EFFDT AND B.EFFSEQ = A.EFFSEQ AND B.SETID_JOBCODE = 'SHARE' AND B.JOBCODE = 'KC012') </pre>			

### Query SQL

Notice that because the view doesn't have OPRID as a key, the resulting SQL does not contain the extra 'AND B.OPRID = 'PS'.

## Create the Dynamic Rule

With the view and the query created, you then need to set up the query rule in Maintain Security. Notice in the following example that **Query Rule Enabled** is selected and that the query created in the previous section appears in the **Query Rule** edit box.

Home > PeopleTools > Maintain Security > Use > Roles

General Members **Dynamic Members** Permission Lists Workflow Role Grant Links

Role Name: DynJobCodeRule  
Description: Dynamic Role based on Jobcode

View All First 1 of 1 Last

User ID	Description

Rules

☒ **Query Rule Enabled**  
☐ PeopleCode Rule Enabled  
☐ Directory Rule Enabled  
[Assign Directory Groups](#)

Test Rule(s)  
Execute Rule(s) Refresh

[Process Monitor](#)  
[App Msg Monitor](#)

Query Rule

Query: ROLEMEMBERS\_JOBCODE\_

### Enabling the Query Rule

After enabling the query rule, you then want to test the rule to make sure the system is assigning the appropriate roles to the appropriate users.

Home > PeopleTools > Maintain Security > Use > Roles

**Dynamic Role Test Results**

Role Name: DynJobCodeRule  
Description: Dynamic Role based on Jobcode

After executing the rules, the listed users will be assigned to the current role.

View All First 1 of 1 Last

User ID	Description	Query	PCode	Dir
KC0004	Charles M Reid	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Testing the Query Rule

To populate the role membership table, click **Execute Rule**.

## Dynamic Role Assignment Integration

If you are using dynamic role assignments, you need to make sure that the role definitions are synchronized across databases. For instance, suppose you create a new role on one database. That new role should be published to all databases in the system. The User Role EIP publishes the membership information, and the following messages synchronize your role definitions.

### ROLE\_MAINT

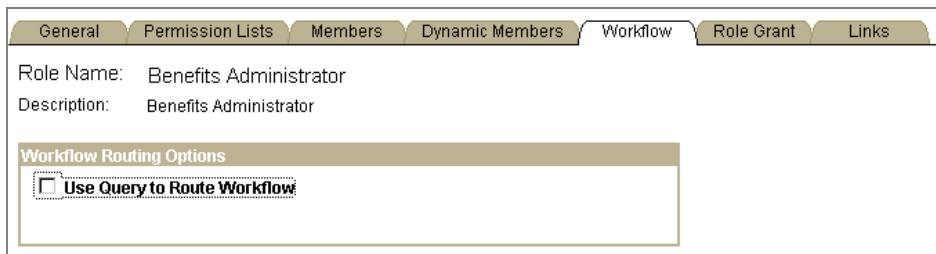
ROLE\_MAINT updates and adds role changes. The Roles component in Maintain Security calls ROLE\_MAINT from the SavePostChange PeopleCode. To facilitate the delivery of this message, you use the ROLE\_MAINT channel.

## DELETE\_ROLE

The DELETE\_ROLE message publishes information about roles that you delete. The DELETE\_ROLE message is called from SavePostChange of the Delete Role component. This message points to the channel DELETE\_ROLE.

## Workflow

You use the Workflow page to specify whether the workflow routings for a particular role should be determined by a workflow query. The option you select depends on your workflow scheme. If you want the workflow routings to be set by a query, then select **Use Query to Route Workflow**.



The screenshot shows the 'Workflow' tab in the PeopleTools interface. The 'Role Name' is 'Benefits Administrator' and the 'Description' is 'Benefits Administrator'. Under the 'Workflow Routing Options' section, the checkbox 'Use Query to Route Workflow' is checked.

PeopleTools, Maintain Security, Use, Roles, Workflow



For more information on setting up your workflow routings see PeopleSoft Workflow.

## Links

If you have added any additional links for user profiles in the Security Links component (Maintain Security, Setup, Security Links), they appear on the Links page.



For more information on setting up additional links, see Security Links.





## CHAPTER 4

# User Profiles

User Profiles define individual PeopleSoft users. You define User Profiles and then link them to one or more Roles. Typically, a User Profile must be linked to at least one Role in order to be a valid profile. The majority of values that make up a User Profile are inherited from the linked Roles.



It's possible to have a User Profile with no Roles. This might be a user that isn't allowed access to the PeopleSoft application, however, they have workflow generated email sent to them.

---

The topics in this chapter relate to the items on the Maintain Security, Use menu that pertain to user profiles. First, information regarding how to define user profile appears, then afterwards the tasks related to user profiles appear, such as emailing new passwords and deleting user profiles.

Defining User Profiles involves entering the appropriate values in the User Profile pages of Maintain Security. The User Profile contains values that are specific to a user such as a user password, an email address, an employee ID, and so on.

At the top of each page there is the User ID and the Description to help you recall which User Profile you are viewing or modifying as you move through the pages. Also you'll see an Account Lockout check box. If you want to deactivate any User Profile for any reason, simply click the Account Lockout check box. The user can't signon until you have deselected that option.



The Account Lockout checkbox is also automatically checked by the system if the user exceeds the maximum number of failed logon attempts. The administrator would then need to manually open the User Profile and uncheck the checkbox in order to reinstate the user.

---

This section covers the pages and procedures related to creating User Profiles.

To create a new User ID

1. Select Maintain Security, Use, User Profiles.
2. On the Find Existing Values page, click **Add a New Value**.
3. On the Add a New Value page, enter the new User ID in the **User ID** edit box, and click **Add**.

The User ID can contain up to 30 characters.

- Specify the appropriate values from the pages in the User Profiles component, and click **Save**.

## ID

The ID page enables you to apply attributes specific to the User ID. You can select the ID Type and Attribute value. Separating user profiles by ID Type allows you to have multiple categories of user profiles with ID numbers all within a range of 1-1000, for example, and it also enables you to grant data permission by entity (Customer, Employee, and so on). So when users sign on to your benefits or pay roll deductions application, they only see information that applies to them—their own data.

A user profile is a set of data set about an entity—a user—that interacts with the system. Your HR system, which keeps track of your employee data, is more interested in your employee user types. On the other hand, your Financials system is more interested in keeping track of customer and supplier user types. ID types allow you to link user types with the records that are most relevant when a user interacts with the system.

The screenshot shows the 'ID' page in PeopleTools. The 'General' tab is selected. The 'User ID' field contains 'PTDMO' and the 'Description' field contains 'Unger,Annette'. There is a checkbox for 'Account Locked Out?'. Below this is a section titled 'ID Types and Values' with a 'View All' link and pagination (First, 1 of 1, Last). The 'ID Type' is set to 'Employee'. A table lists attributes: 'EmpID' with value '8488' and description 'Unger,Annette'. At the bottom is a 'User Description' section with a text box containing 'Unger,Annette' and a link 'Set Description'.

PeopleTools, Maintain Security, Use, User Profiles, ID

The Attribute Value is where you select the value associated with the Attribute Name. In this case, the value reflects the employee number, but it could be a customer number or vendor number.

The User Description section enables you to help identify the user. You can add a description, such as a name of an individual or an organization, for the user profile, or you can click Set Description to populate the edit box with an existing description in the database.

Before you assign a user type to a user, you need to create your user types first. You create user types at Maintain Security, Setup, User Profile Types.



For more information on ID Types, see User Profile Types.

## General

The General page contains information that is only applicable for User Profiles. The General tab is where you specify the User Attributes, or attributes that are user-specific. Some of the attributes, such as a password, are required while others, such as Email ID are optional.

General ID Roles Workflow Audit Administrator Links

User ID: 8001

Description: Schumacher, Simon ☐ Account Locked Out?

**Logon Information**

Symbolic Id:

\*Password:

\*Confirm Password:

**General Attributes**

Email ID:

Language Code:  ☐ Multi Language Enabled?

Currency Code:  ☐ Enable Expert Entry

**Permission Lists**

Navigator Homepage:  [Explain](#) Primary:  [Explain](#)

Process Profile:  [Explain](#) Row Security:  [Explain](#)

PeopleTools, Maintain Security, Use, User Profiles, General

The following topics describe the options available on the General page.

## Logon Information

The logon information is where you enter the values that a user requires for logging on to the system.

### Symbolic ID

The **Symbolic ID** is associated with a user's encrypted Access ID and Access Password. The correct Symbolic ID needs to be entered in order to retrieve the appropriate Access ID and password for signon. This value determines what Access ID and password will be used to log the user onto the database after the system validates their User ID.



The Access ID is only required when a user needs to connect directly to the database (in two-tier). With PIA, the application server maintains the connection to the database and there is the only component that needs to submit an Access ID.

## Password/Confirm Password

Both of these values are required. The User Password you enter is the password string that the user must supply at signon. The Confirm Password value must match that of **User Password**.

---

## General Attributes

The General Attributes section is where you enter the email address, language code, and currency code.

### Email ID

If a user is part of your workflow system or you have other systems that generate emails for users, you enter an email address in the **Email ID** edit box.

### Language Code

The Language Code on the User Profile page has a limited use. For example, when a user runs a batch job, the system needs to know what language to generate the reports in for the user that submitted the job.

If the user is going to access PeopleSoft in a variety of languages, select **Multi Language Enabled**.

In PIA, the user's language preference is based on the selection they make on the signon page.

For Windows workstations, the user's language preference is derived from the Display tab in Configuration Manager. For the Windows environment, the value specified as Language Code in the User Profile acts as a default in case the language code isn't specified in Configuration Manager.

### Currency Code

If the user deals with international prices, you want to set the currency code to reflect the native or base currency. That way values appear in the currency the user is familiar with.

### Enable Expert Entry

You can specify that some users, your expert or power users, have the option of deferring the processing of the data they enter. This enables users to reduce the amount of trips to the server for data processing. You enable this option in the Application Designer, and you specify which users have this option using the Enable Expert Entry checkbox.

If you want a particular user to be able to specify deferred processing, then select the checkbox. If not, leave the check box deselected.



For more information on the design time elements of this feature, see Processing Mode.


---

---

## Permission Lists

Recall that not all permissions are inherited by the Roles assigned to a User Profile. You apply some of the permissions directly to the User Profile. This is the case with the following Permission Lists:

- **Navigator Homepage.** The homepage is associated with PeopleSoft Workflow.
- **Process Profile.** The Process Profile contains the permissions a user requires for running batch processes through Process Scheduler. For instance, the process profile is where users are authorized to view output, update run locations, restart processes, and so on. Only the Process Profile comes from this permission lists, not the list process groups.
- **Primary and Row Security.** PeopleSoft determines which data permissions to grant a user by looking at the Primary Permission List and Row Security Permission List. Which one is used varies by application and data entity (Employee, Customer, Vendor, Business Unit, and so on). Consult your application documentation for more detail. PeopleSoft also determines Mass Change, and Object Security permissions from the Primary Permission List.

Click  to reveal the list of valid options for each Permission List.

## Roles

The Roles that you add to a User Profile ultimately define what the user can and can't access in your PeopleSoft system. Through roles, the user inherits Permission Lists.

---

## Working with Roles

The Role page enables you to add and remove roles from a user profile.

Role Name	Description	Dynamic	Route Control	+	-
Facilities Administrator		<input type="checkbox"/>	<a href="#">Route Control</a>	+	-
MIS Administrator		<input type="checkbox"/>	<a href="#">Route Control</a>	+	-
UPG_ALLPANLS		<input type="checkbox"/>	<a href="#">Route Control</a>	+	-
UPG_APPSRVR	Can start application server	<input type="checkbox"/>	<a href="#">Route Control</a>	+	-

PeopleTools, Maintain Security, Use, User Profiles, Roles


The Role Name and Description columns enable you to identify the roles assigned to a user profile. The Dynamic check box is checked if the system has assigned a particular role dynamically.

Route Control enables you to enable a route control profile. For each role assigned to a user, you can specify a route control profile. For example, let's say you have a role named EXPENSE\_REP. If you wanted a particular expense representative to handle all of the expense reports submitted by people that had last names beginning with "A", you could assign the user a specific route control profile—one sending him reports submitted by individuals with a last name beginning with "A".

To add a Role to a User Profile

1. Click .

The system adds a new row to the page.

2. Click  in the Role Name column for the row you just added to the page.
3. On the search page, click the Role Name that you want to add to the User Profile.

## Working with Dynamic Role Rules

Also on this page you use the **Dynamic Role Rule** options to test and manually execute your rules for assigning roles dynamically. You design your role rules using PS/Query, PeopleCode, or they exist within your LDAP setup.

Dynamic Role Rules

- **Test Rule(s).** To see if your rules are going to produce the desired results for a particular user,

you can test them by clicking this button. None of the roles are actually assigned, but the system provides you a report as to what roles will be assigned when you run the rule.

- **Execute Rule(s).** Use the Execute Rule(s) button to run your rules and assign the appropriate roles to a particular user. This is the manual approach. Typically, you execute role rules through Process Scheduler on a regularly scheduled basis.

## Workflow

The Workflow page enables you to maintain your Workflow user and routing definitions within the security Role.

The screenshot displays the 'Workflow' tab for a user profile. At the top, there are tabs for ID, General, Workflow, Roles, Audit, Administrator, and Links. Below these, the 'User ID' is 'PTDMO' and the 'Description' is 'Unger,Annette'. The 'Workflow Attributes' section contains several input fields: 'Form ID' (empty), 'Alternate User ID' (empty with a search icon), 'From Date' (empty with a calendar icon), 'To Date' (empty with a calendar icon), and 'Supervising User ID' (empty with a search icon). To the right of these fields is a 'Routing Preferences' box with three checked options: 'Worklist User', 'Email User', and 'Forms User'. Below the attributes is a 'Reassign Work' section with a checkbox labeled 'Reassign Work To:' followed by an empty field with a search icon. At the bottom, it states 'Total Pending Worklist Entries: 1'.

PeopleTools, Maintain Security, Use, User Profiles, Workflow

---

### Workflow Attributes

In order for a use to join the workflow system, you need to specify the following information.

#### Form ID

In the Form ID box, enter the appropriate Lotus Notes Form ID use for routing forms.

#### Alternate User ID

If this role user is temporarily out (on vacation, for instance), select an **Alternate Role User** to receive routings sent to this role user.

If there's a role user name in the list box, the system automatically forwards the current role user's work items to the alternate role user.



The system forwards *new* work items to the Alternate Role User. It doesn't reassign items already in the user's worklist. To reassign the existing work items, you need to go to the Role User Archiving component.

---

### From Date

This edit box applies to the Alternate User ID. Here you enter the date the current role user is going to begin a temporary vacancy.

### To Date

This edit box applies to the Alternate User ID. Here you enter the date the current role user is going to return from a temporary vacancy.

### Supervising User ID

Select the User ID of the user's supervisor in the **Supervising Role User** list box. The system uses this value when it needs to forward information to the user's supervisor.

The system uses the PERSONAL\_DATA record to determine the user's supervisor.



If you're using PeopleSoft HRMS applications, the **Supervising Role User** field shouldn't appear. If it does, then you need to set your Workflow System Defaults.

---



For more information see Defining Roles and Users.

---

### Routing Preferences

Specify which types of routings this role user can receive. The **Routing Preferences** box shows the three places where the system can deliver work items: to a worklist, an email mailbox, or a forms mailbox. If this user doesn't have access to one or more of these places, deselect its check box. For example, if this person isn't a PeopleSoft user, deselect **Worklist User**.

---

### Reassign Work

This is where you reassign any pending work for this role user if positions change or a user is going on a temporary leave, such as a vacation.

If this user has work items waiting for their attention (as shown by the **Total Pending Worklist Entries** in your Workflow interface), select the **Re-assign Work To** check box and select the



user to forward their work items to from the list box. When you save the page, the system reassigns existing worklist entries to the specified user.



If you don't reassign pending work items, they will remain unprocessed.

---

## Audit

The Audit page is a display-only page that enables you to determine when a profile was last updated and who updated it.



For more information on auditing changes see Signon PeopleCode.

---

## Administrator

If a user is a system administrator, check the **Is User System Administrator?** checkbox.

During development, new object definitions may be created and re-created several times a day. And, using standard security definitions, the developers and testers working on those definitions would need security updates for each re-creation in order to be able to view and test their changes. For this type of user, we provide the System Administrator option.

When users move about in the PeopleSoft system, their security definitions are continually validated against various security tables to see what they're allowed to access. However, System Administrator users aren't validated at all. They automatically have access to just about any menu item and process definition in the system, 24 hours a day. Setting up your developers and testers as System Administrators helps to minimize the time you spend updating security and the time they spend waiting for such updates.

Setting up a user as a System Administrator does *not* affect:

- General or user attributes (such as password, access profile, and so on); these attributes must still be defined.
- Process Profile settings.

## Links

If you have added any additional links for user profiles in the Security Links component (Maintain Security, Setup, Security Links), they appear on the Links page.



For more information on setting up additional security links, see Security Links.

---

## User Profiles Tasks

The following topics describe the tasks related to user profiles that you complete by way of the Maintain Security, Use menu. Some of these tasks, such as the features offered by the My Profile component, are appropriate for end users, while others, such as Delete User, should only be performed by administrators.

---

### Administer Personalizations

PeopleSoft offers a variety of options that enable end users, especially power users, to complete business transactions in a more efficient manner. These options improve a user's navigation speed through the system and enable users to select international preferences, such as date and time formats. This section describes the options that PeopleSoft provides and the procedure to follow to implement a set of options.

### User Personalization Options

This section provides a reference for the available user options. The Explain button on both the My Profile and Administer pages briefly describes the option online. For example, when you click Explain, a Personalization Explanation page appears containing information to help you understand the option.

**Personalization Explanation**

**Message Set Number:** 48      **Message Number:** 161



CSYM - Currency Symbol  
 Any string up to 5 characters long, often '\$', '¥', '€' or '£'. This determines the default value for fields if no Currency Control field is specified.


[Return](#)

My Profile, Set Personalizations, Explain

The following table provides any additional information for the personalization options.

<i>Item</i>	<i>On by Default?</i>	<i>Description</i>
Tab over Add/Delete buttons		Tab over the + and - buttons within grids and scrolls. This is a Yes/No option.
Afternoon Designator	Yes, PM	Designate the time of afternoon, such as PM or pm. The value has a 5-character limit.

<b>Item</b>	<b>On by Default?</b>	<b>Description</b>
Tab over calendar buttons		Tab over the calendar controls on pages. Calendar controls appear as  . This is a Yes/No option.
Currency Symbol	Yes, \$	Enter the local currency symbol. The value has a 5-character limit.
Currency Symbol Position	Yes, leading	Specify whether the currency symbol appears to the left or right of the numerical value. Choose between L, leading, or T, trailing.
Decimal Separator	Yes, ','	Specify how you want values with decimals to appear. Typically, you use a '.' but if you prefer a ',' then 1.00 appears as 1,00. This field has a 1-character limit.
Date Format	Yes, MM/DD/Y Y	Specify how the date is expressed. You have the following options: <ul style="list-style-type: none"> <li>• <b>D.</b> DD/MM/YY</li> <li>• <b>M.</b> MM/DD/YY</li> <li>• <b>Y.</b> YY/MM/DD</li> </ul>
Date Separator	Yes, /	Specify how you want to separate the month value from the day, and so on. For example, you can use a '-' for 01-01-2001, or a '/' for 01/01/2001. This field has a 1-character limit.
Tab over grid tabs		Enable users to tab over the tabs or headings within grids. This is a Yes/No option.
Tab over header icons		Enable users to tab over header icons, which appear at the top of each page and include Home, Help, and Sign Out. This is a Yes/No option.
Tab over lookup button		Enable users to tab over the  buttons to the right of edit boxes that have an associated list of Valid Values. This is a Yes/No option.
Local Time Zone	Yes, Pacific	Specify the local time zone, as in PST for Pacific Standard Time, TST for Tokyo time, or GMT for Greenwich Mean Time, to name a few.
Morning Designator (AM, am)	Yes, AM	Designate the time of morning, such as AM or am. The value has a 5-character limit.
Tab over navigation bar		Enable users to tab over navigation bars, which appear at the top of grids and scroll areas to control the rows that display. This is a Yes/No option.

<b>Item</b>	<b>On by Default?</b>	<b>Description</b>
Tab over browser elements		You can restrict tabbing to the PeopleSoft elements of the page only. This is a Yes/No option.
Tab over page links		Enable users to tab over links to other pages. This is a Yes/No option.
Tab over pop-up icon		Enable users to tab over the icons for pop-up menus,  . This is a Yes/No option.
Save Confirm	Yes, Yes	With this option enabled, users see a message confirming a save action.
Save Warning		With this option enabled, users see a message warning to the any unsaved changes made while accessing the current page.
Tab over toolbar		Enable users to tab over the toolbar at the bottom of a page. Toolbar items include buttons that control standard operations on the page, such as Save, Return to Search, and so on.
Time Format	Yes, h:mm:ss	Specify how you want time to appear. You have two choices: civilian time (01:05:00 PM) or military time (13:05:00). Whether or not microseconds appear is not a personalization option.
Time Separator	Yes, :	Specify whether the hours and minutes and seconds are separated with a ':' or a '.', and so on. This field has a 1-character limit.
Thousands separator	Yes, ','	Specify how you want numerical values over 999 expressed—with a ',' as in 1,000 or with a '.' as in 1.000.
Use local time zone		Specify whether transactions are to use the local time zone or the time zone or that of the server or corporate time zone.



If you want to view more information regarding any of the user options, select Maintain Security, Setup, Defined Personalizations.

## Enabling User Preferences

As a system administrator, you select the user preferences to implement at your site from the Use, Administer Personalizations, Administer Personalization Options page. The user options that you

select, appear in the My Profile, Personalization page for the user to view and modify (if allowed).

Only the options that you enable in the Administer Personalization Options page appear in the My Profile, Set Personalizations interface. PeopleSoft does, however, have the following options enabled by default.

Option	Default Value	Override Value	
Afternoon designator (PM, pm)	PM	<input type="text"/>	<a href="#">Explain</a>
Currency Symbol	\$	<input type="text"/>	<a href="#">Explain</a>
Currency Symbol Position	Leading	<input type="text"/>	<a href="#">Explain</a>
Decimal Separator	.	<input type="text"/>	<a href="#">Explain</a>
Date Format	MM/DD/YY	<input type="text"/>	<a href="#">Explain</a>
Date Separator	/	<input type="text"/>	<a href="#">Explain</a>
Local Time Zone	Pacific Time, Tijuana	<input type="text"/>	<a href="#">Explain</a>
Morning designator (AM, am)	AM	<input type="text"/>	<a href="#">Explain</a>
Save Confirmation	Yes	<input type="text"/>	<a href="#">Explain</a>
Time Format	h:mm:ss (8:05 AM)	<input type="text"/>	<a href="#">Explain</a>
Time Separator	:	<input type="text"/>	<a href="#">Explain</a>
Thousand Separator	,	<input type="text"/>	<a href="#">Explain</a>

### Default User Personalizations

To enable user personalization options

1. Click PeopleTools, Maintain Security, Use, Administer Personalizations.
2. Scan the options on the Administer Personalization Options page, and decide which options are suitable for your site.

The Image column (if applicable) and Explain links aid you in identifying the intent of each personalization option.

3. Click the **Enable Option** checkbox to enable a particular option.
4. If you want the end user to be able to override the default value that you provide, click the **Allow User Value** checkbox.

This enables users to enter their own values in the My Profile, Set Personalizations interface. If a custom value might jeopardize data integrity, leave this box unchecked.

5. Add a value in the **Default Value** edit box.

For example, for Currency Symbol you might enter \$.



Adding a default value is required for all options that you enable.

6. Repeat these steps for each user option you want to make available for end users.
7. Sign off the system and then sign on to activate the selections.

The options are set during signon.

## My Profile

The My Profile option enables users to modify their own user preferences. Users are not allowed to add roles to their user profile, but they can add a new email address or change their password if needed.

Users complete these self-service security tasks with the General Profile Information page.

**Password**

[Change password](#)

[Change or set up forgotten password help](#)

**Personalization**

My preferred language for reports and email is:

Currency Code:

[Set Personalizations](#)

**Email**

E-mail Address:

**Alternate User**

If you will be temporarily unavailable, you can select an alternate user to receive your routings.

Alternate User ID:

From Date:  (example:12/31/2000)

To Date:  (example:12/31/2000)

[Miscellaneous User Links](#)

PeopleTools, Maintain Security, Use, My Profile

## Password

There are two self-service options related to passwords.

### *Change Password*

Users can change their passwords by completing the following procedure.

To change a password

1. Select PeopleTools, Maintain Security, Use, My Profile.

The actual navigation may differ depending on your implementation or if you are using the PeopleSoft portal.

2. Click Change Password.

The Change password page appears.

3. In the **Password** edit box enter the new password.

4. In the **Confirm Password** edit box, enter your new password again.
5. Click **OK**.

### *Change or setup forgotten password help*

If a user forgets the signon password, you have the option of emailing the user a new, randomly generated password. If you opt to use this feature, you can also allow users to answer a pre-defined question, and if they provide the correct answer, the system emails them a new password.

Users can add their own question or they can select from an inventory of questions that an administrator created on the Setup, Forgotten Password Questions page.



If you are using LDAP authentication, you can't take advantage of the forgotten password feature because this feature that you're using PeopleSoft authentication, where the password is stored within the PeopleSoft database.

---

A user can change or set up password help by completing the following procedure.

To change or setup password help

1. Select PeopleTools, Maintain Security, Use, My Profile.
2. Click Change or setup forgotten password help.
3. Either add your own question, or select a question from a predefined set of questions.
4. Enter the appropriate response to the question you selected or created.
5. Click **OK**.

### **Set Personalizations**

The Preferences section enables a user to change language settings, and currency settings.

Also, PeopleSoft offers a variety of user personalizations intended to help end users navigate and set defaults for their typical transactions. Your system administrators decide which options to enable for your site.

Based on the user personalizations that an administrator has selected end users can view and modify the available pool of options. To view the available user personalizations, select Use, My Profile, and click the Set Personalizations hyperlink. This page reveals all of the user personalizations that are available for your site.

If end users are permitted to override the default value specified in, Administer Personalizations, then an edit box appears under the Override Value column in which end users can add custom values. Override means to add your own custom value to suite your current needs. In some situations, you may not be permitted to override any default values.

The Personalization page contains the following columns:

- **Option.** The name of the user personalization.
- **Image.** If applicable the image of the page control appears to help you identify it.
- **Default Value.** This default value that has been specified for your site. For instance, if your organization does business in the U.S., the default value for Currency Symbol is likely to '\$' to indicate U.S. Dollars.
- **Override.** System administrators can enable end users to override the defaults that they have specified. This means that you can add a custom value in place of the default value. For instance, perhaps your company has '\$' set as the default currency symbol. However, suppose that you are an Accounts Receivable clerk that mainly interacts with your British customers. In such a case, you may elect to switch the default currency symbol to reflect the British Pound. If you're system administrators have not allowed you to modify any of the default values, the override column is empty.
- **Explain.** A link that you click to view more details, such as your override options, regarding a particular user personalization. For each option available, you should view the explanation in the Explain link.

To override a user personalization default value

1. Select PeopleTools, Maintain Security, Use, My Profile, and click the Set Personalizations hyperlink.

The Personalizations page appears.

2. View the list of user options made available by your system administrators, and make sure all the default values apply to the transactions you typically complete.

If you want to change a default value then complete the following steps.

3. Click the **Explain** link to view any details regarding valid values for the option, as in the number of characters that are allowed.

For example, if the option has a 1-character limit (or single-character limit), the system expects a symbol, such as '.', '\$', ':' and so on.

4. Enter the custom value into the edit box in the Override column.

You can enter custom values using the following methods.

- **Single Character.** Manually add the desired character, as in '\' or '.'
- **5-Character.** Manually add the character string. You can add up to 5 characters.
- **Yes/No.** If the option is a Yes/No or toggle option, you can disable it by entering an 'N' in the edit box. Or you can click the lookup button and select the appropriate value.
- **Prompt.** For options, such as time zone, where there are multiple possibilities you click the lookup button and select the appropriate value from the Search Results list.



5. After you have made the appropriate selections/modifications click **OK**.
6. Sign out of the system, and then sign in again for your selections to be activated.

## Email

Add the email address that you want your workflow routings to be sent, as well as other items, such as new passwords and so on.

## Alternate User

The Alternate User options expose the Workflow attribute, Alternate User, to self-service. If you are set to be on vacation or some other type of temporary leave, you can add the User ID of a colleague who is looking after your tasks in your absence. The From Date and To Date edit boxes are where you specify the duration of your absence. After that time has passed, your routings automatically get routed back to you.

---

## Forgot My Password

If a user forgets a password, you can opt to have the system randomly generate a new password and email it to the forgetful user. If the Allow Password to be emailed setting is not included in a user's permission lists, then they can't have a new password mailed to them.

If a user is allowed to receive new passwords through email, they can do so by completing the following procedure.



Before the system can email you a new password, you need to have the following in place: a forgotten password hint, an email address specified in your user profile, and your security administrator needs to permit you to have a new password emailed.

---

To request a new password

1. Select PeopleTools, Maintain Security, Use, Forgot My Password.
2. On the Forgot My Password page, enter your User ID.
3. Click Continue.
4. On the Email New Password page make sure the system is set to send the new password to the appropriate email address.

If the appropriate email address does not appear, contact your system administrator. System administrators need to make sure that the email address is correctly represented for each user who intends to use this feature.

5. Respond to the user validation question.

6. Click Email New Password.

---

## Delete User Profile

After a user profile is no longer needed, for the sake of general house keeping, you should delete the old user profile to reclaim space for new users.

The Delete User Profile removes information related this particular user profile that appears in every security table in the system, PeopleTools and application tables. If you want to prevent any of the information from being deleted you can specify tables that the delete user process bypasses.



For more information on specifying tables for this process to bypass, see Profile Delete Tables to Skip.

---

To delete a user profile

1. Select PeopleTools, Maintain Security, Use, Delete User Profile.
2. On the Delete User Profile page, make sure you have selected the *correct* user profile.
3. Click Delete User Profile.

A prompt appears; either confirm your deletion or cancel it.

## CHAPTER 5

# Setup Options and Processes

PeopleSoft provides a number of special security features, for those users who are interested in controlling their system security in unique or customized ways. PeopleSoft provides extra ways for you to manage passwords or setup user profile types, to name a few.

None of these added features are required in order to roll out your applications in a production environment. However, for some sites, the security options we provide will save you time and resources in maintaining your PeopleSoft system.

## Setup Options

The following topics describe the options under the Setup menu in Maintain Security. You arrive at these options by selecting **PeopleTools, Maintain Security, Setup**.

---

### User Profile Options

The following topics describe the options available for your user profiles.

#### User Profile Types

When deploying your applications to the Internet, you have the potential to generate thousands of different user profiles. In some situations, it may be necessary to aggregate your user profiles in a categorical fashion. For instance, having ID Types enables you to have Employee ID numbers beginning at 1 as well as Customer ID numbers beginning at 1.

User Profile Types provide a means to link User Profiles with data stored in application specific records. PeopleSoft applications need this link mostly for self-service transactions. For example, you want an employee to see their benefits only, or you want a customer to view and pay their *own* bills. Customer ID, Employee ID, and so on are the keys for the application data. User Profile Types enable the system to find the "right" ID based on the user profile. The system needs the value because there's no guarantee that Personal Data and Vendor Contact data won't have the same key field. Because the Personal Data and Vendor contact data resides in different records, there's no edit that prevents the two records from having the same key.

To create User Profile Types you use the PeopleSoft ID Type page. After you create User Profile Types, you then assign this type, along with an ID for this type to User Profiles.

**User Profile Types**

ID Type: CNT ☒ Enabled?

Description: Customer Contact \*Sequence number: 3

Description:

Customer Contact

Field Information			View All	First	1-2 of 2	Last
*Field Name	*Edit Table	Description Fieldname				
1 SETID	SETID_TBL	DESCR				
2 CONTACT_ID	CONTACT	NAME1				

PeopleTools, Maintain Security, Setup, User Profile Types



Don't enable the ID type until the fields and tables in the Field Information section have been defined and built with Application Designer.

The PeopleSoft ID Type page contains the following controls:

- **ID Type.** The ID Type is the abbreviated form the profile type name.
- **Description.** The Description edit box enables you to add an intuitive name for a profile type. This is the value that appears on the ID Page in the User Profiles component. You have a 30-character limit.
- **Enabled?** You disable and enable a profile type by clicking this checkbox. Once enabled, you can assign it to user profiles. If it is disabled then it does not appear in the drop-down list on the ID page for user profiles.
- **Sequence number.** This option is used by the Set Description function. On the User Profiles, ID page you can click on a Set Description link to generate the User Description based on the values in the Description FieldName for the user types assigned to the user. The Sequence Number determines which user type to use when the user is assigned to multiple user types. The User Description is set to the value in the Description Fieldname of the user type with the lowest sequence number and non-blank value. For example, if a user is assigned to user types of Employee (seq no 1) and Customer Contact (seq no 3), the Description would be set to PERSONAL\_DATA.NAME, unless it is blank. If PERSONAL\_DATA.NAME is blank, the Description would be set to CONTACT.NAME1.



For user types with multiple fields, the system uses the Description Fieldname corresponding to the last field. For example, the Customer Contact user type has two fields: SETID and CONTACT\_ID. The Set User Description function uses the Description Fieldname CONTACT.NAME1 corresponding to the last field, CONTACT\_ID.

- **Description (Long).** The Description edit box provides an opportunity to provide details about a given profile type. You have a 250-character limit

- **Field Information.** The fields you select enable the User Profile component to prompt for an ID value when you select a type on the ID page. Let's say the user picks "Employee" from the ID page. In this case, the system needs to know the valid ID values to prompt the user with. The Edit Table column specifies the record, the Field Name column specifies the field. You can specify multiple fields if the ID has multiple keys, as in when the keys for Customer information are Customer ID and SETID.

## Profile Delete Tables to Skip

There are many occasions when you need to delete a user profile from your system. For instance, perhaps an employee retires. Regardless of the situation, you don't want to keep the unnecessary user data in your system. So it's a good idea to purge your system of obsolete user data, such as personal queries, to reclaim space for new user data. This process targets all tables that are keyed by User ID.

However, in the case of an employee, you may not want to keep their page or signon access information in the system, but you might be interested in keeping user data stored in an audit table that tracks changes made to vital company data. You may need to check that information a few months later. You might discover some interesting financial allocations, and if so, you'll want to know who's responsible.



**Important!** Keep in mind that the automated process of deleting a user profile deletes every row of data in your system associated with a particular user profile. You want to make sure that any information you might need in the future is safe.

If there are any tables that store data associated with user profiles that you want to preserve, add the record name, to the Bypass Table page.

Bypass Tables	
Bypass these tables during User Profile Deletion	
Record (Table) Name	Record Description
1 PRG_USR_PROFILE	User Profile Purge History

PeopleTools, Maintain Security, Setup, Profile Delete Tables to Skip

You select either PeopleTools security tables or PeopleSoft application security tables from the **Record (Table) Name** drop-down list.

## Passwords

One of the fundamental tasks of any security system is managing user passwords. You want to make sure that your users select passwords that aren't obvious, and you want to make sure that they change them regularly enough to frustrate any would-be hackers.

The password restrictions that you set apply globally to all of the PeopleSoft users on your site. You can't apply separate password restrictions per user or role, for example.

The following topics describe the PeopleSoft password management interface. If you use a third party utility to manage your passwords on a site-wide basis, then you don't need to implement the PeopleSoft solution. Also, if you use other authentication methods, such as LDAP, then you don't need to use PeopleSoft password controls. These password controls apply to passwords stored in PeopleSoft.

## Password Controls

You use the **Password Controls** page to set any password restrictions that you might want to impose on your end users. To access this page, select **Maintain Security, Setup, Password Controls**.

Before you use the Password Controls, keep the following items in mind:

- These options apply when you are maintaining your user profiles in PeopleSoft, not an LDAP directory server.
- You need to activate the controls using the **Enable Password Controls?** checkbox.

PeopleTools, Maintain Security, Setup, Password Controls

The following sections explain the PeopleSoft password controls.

### *Enable Password Controls?*

If you want to enable the PeopleSoft password controls, then click this checkbox. If you are not interested in password controls, as in you already have a third party utility that performs equivalent features, then leave this check box deselected.

Password controls are implemented in Signon PeopleCode. As a result, you can extend the controls by modifying the PeopleCode.

### *Age*

You define a number of days (between 1-365) that a password is valid. Users logging on after a password expires must change their password to log on. If you don't want the password to expire, then select Password Never Expires. When a password expires the user can't sign on to the system.

PeopleSoft delivers a default permission list named PSWDEXPR (Password Expired). When a password expires for a user, the system automatically removes all of the user's roles and permission lists and temporarily assigns them the PSWDEXPR permission list only.

A user whose password has expired can only access items in the PSWDEXPR permission list, which typically grants access to the My Profile component only. For the duration of the session, as in until the user changes the password, the user is restricted solely to the PSWDEXPR permission list.

By adding the My Profile component to the permission list, users can at least sign in to issue themselves a new password. If there are additional requirements that you need to append to the delivered PSWDEXPR permission list, you can add them using Maintain Security.



The actual User Profile stored in the database is not changed in any way when the password expires. You don't need to redefine the profile. When the password gets changed the system restores the user profile's previous roles and permission lists.

---

### ***Account Lockout***

This control enables you to lock an account after  $n$  number of failed logon attempts. For instance, if you set the **Maximum Logon Attempts** value to 3, and a user fails three logons, they are automatically locked out of the system. Even if they correctly enter a user ID and password on the fourth attempt, the user is not permitted to logon. This feature reduces the risk of any "brute force" intruders into your system. It also "helps" your end users to learn the lesson of remembering the password they choose.

After the account is locked out, you need to open the User Profile and uncheck the Account Locked check box.

### ***Miscellaneous***

The Allow password to match User ID control enables administrators to make sure users don't use their own User ID as a password. This helps you to prevent hackers from "guessing" passwords based on a list of employee names.

### ***Minimum Length***

Administrators can opt to set a minimum length for passwords maintained by their PeopleSoft system. If the minimum length is set to 0, the PeopleSoft password controls do not enforce a minimum length on the user's password. This does not, however, imply that the password can be blank. When you create a new user or a user changes a password, the system checks this value. If it is non-zero, the system tests the password to ensure it meets length requirements, and if not, an error message appears.

## ***Character Requirements***

Administrators can require a set number of digits or special characters within a password. Special characters, or "specials," refer to symbols such as # and @, and digits refer to numbers (integers), such as 1 or 2.

Here is the list of characters you can include within a password:

! @ # \$ % ^ & \* ( ) - \_ = + \ | [ ] { } ; : / ? . > <

## **Forgotten Passwords**

Before the system emails a new, randomly generated password for a forgetful user, you want to make sure they are who they claim to be. The Forgotten Password Questions feature enables you to pose a standard question to users requesting a new password because they forgot the previous one. If the user enters the appropriate response, then the system automatically emails them a new password so that they can signon on to the system.

### ***Adding Text to be Mailed with New Password***

The system sends the user a new password within an email message. You can have numerous password hints, but typically, you'll send all new passwords using the same email message template. Because of this PeopleSoft provides a separate page just for composing the standard email text.

You need to add the following text string in the Email Text edit box:

<<%PASSWORD>>

This is where the system looks to insert the new password. The %PASSWORD variable resolves to the generated value.

**Forgot My Password Email Text**

Enter the text of the new email to be mailed with the new password below.  
Please include the exact string <<%PASSWORD>> to be replaced with the new randomly generated password.

**Email Text:**

PeopleTools, Maintain Security, Setup, Forgotten Password, Email Text

Perhaps you might instruct the user to change the password to something more intuitive after they logon to the system with the randomly generated password.





Only users that have the Allow Password to be Emailed (on the General page) option enabled in a permission list can receive a new password by way of this feature.

### *Creating Password Hints*

You add your hint in the Question edit box on the Password Hint page, making sure that the Active checkbox is selected.

PeopleTools, Maintain Security, Setup, Forgotten Password, Password Hint

Then on the Email Text page you add any text that you want to appear in the generated email containing the new password.

With these hints set up, users, upon forgetting their password, navigate to the Forgot My Password page (PeopleTools, Maintain Security, Use, Forgot My Password). The user answers the question correctly and gets a new password sent through your email system.

Users don't have to use the password question created by an administrator. If they would like to add their own password question, they can do so in the My Profile component.

### *Deleting Forgotten Password Hints*

To delete a password hint, select Maintain Security, Setup, Delete Forgot My Password Hint.

Then either enter the code for the hint or perform a search for it. On the Delete Forgot My Password Hint page, make sure you've selected the appropriate hint, and click **Delete**.

### *Configuring the Forgotten Password Site*

You need to perform the following

- Set up a separate site on your web server.
- Setup a direct connection to the site, as in a link the leads right to it.
- Specify a default user in the configuration.properties file on the web server and enable bypass signon so they don't have to enter an ID and password. This “direct” user should have limited access, as in only to the Email New Password component. Users go directly to it, and get a new password mailed.



For more information on the web server configuration files, see Configuration Files.

- Place a link to the “forgotten password” site, within the public portion of the PeopleSoft portal, or on another public web site. Notify your user community of the link.

## Directory Authentication

PeopleSoft supports integration with LDAP directory servers. You have the option of having PeopleSoft or a directory server authenticate users. If you opt to use directory authentication then you need to enable directory authentication, specify connect information for the LDAP server, and specify the properties you want the PeopleSoft signon process (Signon PeopleCode) to retrieve from your directory server. The following sections describe the three pages in the Directory Authentication component.

### Directory Setup

The Directory Setup page is where you enable directory authentication and specify important LDAP server information so that your PeopleSoft system can connect and retrieve information from it.

PeopleTools, Maintain Security, Setup, Directory Authentication, Directory Setup

If you want to enable directory authentication, then you need to click the Use Directory Authentication checkbox. This turns on directory authentication for the local database. Signon PeopleCode uses this information to connect to the LDAP server and retrieve information stored there. After you have enabled directory authentication, you need to enter connect, search, and mandatory user property information.

### ***Directory Connect Information***

So that the PeopleSoft system successfully connects to your directory server, enter the appropriate connect information. This includes the server name (DNS or IP address) and the listening port number. You also need to enter the User DN (Distinguished Name) and associated password.

The PeopleSoft application server uses the User DN and password to connect to the LDAP server to retrieve user profile information about the specific user signing on to the system. The User DN must reflect a user with the appropriate LDAP browse rights. The User password is stored in encrypted form in the database, not even individuals with administration access to the database can view the password.

### ***User Search Information***

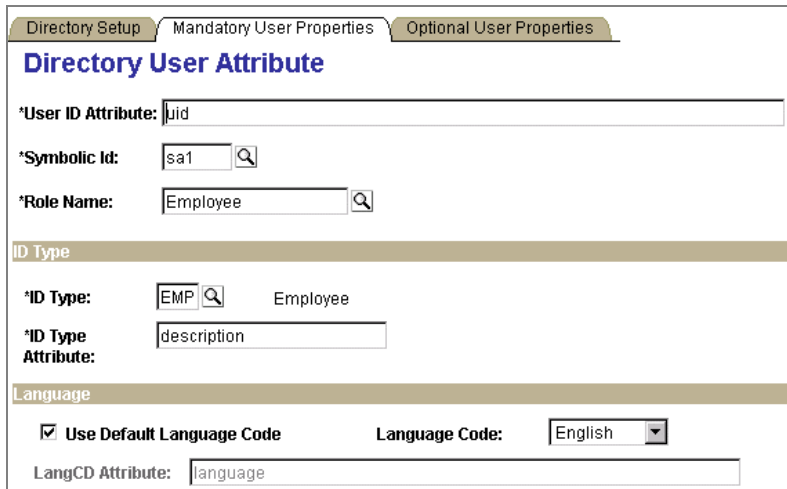
To refine the scope of the search, enter the appropriate values in the User Search Information group. This includes setting the proper Scope.

- **SUB.** Searches the entire sub tree beneath the Search Base that you specify.
- **ONE.** Searches one level beneath the Search Base that you specify.
- **BASE.** Searches only the Search Base that you specify.

The Search Base needs to indicate the entry (or "container") at which to begin the search. The Search Attribute needs to reflect the attribute to which the specified User ID should be matched. This is the attribute in the directory server that matches the ID value the user has entered on the signon page.

### **Mandatory User Properties**

If you are going to use directory authentication there are a handful of user attributes that are required to be available at signon time for the Signon PeopleCode. You specify the attributes required for signon on the Mandatory User Properties page. You can opt to have the system retrieve these mandatory values from the directory server, or you can enter default values.



PeopleTools, Maintain Security, Setup, Directory Authentication, Mandatory User Properties

The mandatory properties include Symbolic ID, Role Name, ID Type, and Language preference.

- **Symbolic ID.** The Symbolic ID is never stored in LDAP. You enter it here on this page, and you enter one value for all users.



For more information on Symbolic IDs see Symbolic ID.

- **Role Name.** This value applies to users the first time they signon and have not had any roles dynamically assigned to them. Typically, this role just has basic access authorizations, such as only the self-service pages. User's should get most of their permissions through dynamically assigned roles.
- **ID Type.** Like Symbolic ID, this value needs to be entered on this page.
- **ID Type Attribute.** Specifies the attribute in the directory that holds the desired ID value. In this case the ID value is Employee ID.
- **Language.** You can retrieve the Language attribute from the LDAP server or specify a default value. To use the LDAP language value, deselect **Use Default Language Code** check box. Then in the LangCD Attribute edit box, specify the attribute in the directory that holds the desired language value. If you want to specify a default language, leave the **Use Default Language Code** check box, selected, and select a value from the **Language Code** drop-down list.

The "NEWUSER" role is not a role that PeopleSoft delivers. You can name the role to suit your requirements. When a new user enters the system, and you have implemented dynamic rules, the user does not belong to any roles until your role rules execute. If you have a new employee entered into the system, at first all they would be able to access is the "public" pages you authorize for the NEWUSER role. Then when your dynamic role rules execute, the new employee becomes a member of all the roles that apply to his or her position.

To implement a "NEWUSER" role, perform the following:

- Create your "NEWUSER" or "EVERYONE" role.
- Add permission lists to the role so that members of this role have access to all the pages that are appropriate for all users within the directory, like My Profile and any other areas that don't pose a threat to your system security.
- Apply roles. If you are using dynamic role assignment, you wait until the batch program runs, if you are using static role assignment, then the user needs to wait until an administrator manually applies the appropriate roles.

If your role rules run only one once in a 24-hour period, it might not be until the next day that a new employee has access to the system. If your rules run more frequently, it may only be a couple of hours. If it's not acceptable to wait the duration until the next run of the dynamic role rule, you can use one of the following options:

- Add any "required" pages to the "NEWUSER" role.
- Reduce the duration between the dynamic rule execution.



Reducing the execution interval of the dynamic rules may have performance impacts depending on how the rules are implemented.

---

- Add a Signon PeopleCode script that detects that the user needs access to a certain role. You can accomplish this by running a query against LDAP, the database, or wherever the information resides. Then use the User Profile component interface to add the appropriate roles to the user, according the query results.

## Optional User Properties

In addition to the mandatory user properties that you must store in the directory, there are also a variety of optional user properties that you may also opt to store in and retrieve from the directory.

You add the optional user properties on the Optional User Properties page. Here you can specify General, Permission List, and Workflow Attributes. All of these attributes appear in the User Profile component.



For more information on the User Profiles component, see User Profiles.

---

Directory Setup	Mandatory User Properties	Optional User Properties
<b>Directory User Attribute</b>		
<b>General</b>		
<input checked="" type="checkbox"/> User Descr	LDAP Attribute:	cn
<input checked="" type="checkbox"/> Email	LDAP Attribute:	mail
<input type="checkbox"/> Currency Code	LDAP Attribute:	
<b>Permission List</b>		
<input type="checkbox"/> Navigator HomePage	LDAP Attribute:	
<input type="checkbox"/> Process Profile	LDAP Attribute:	
<input type="checkbox"/> Primary	LDAP Attribute:	
<input type="checkbox"/> Row Security	LDAP Attribute:	
<b>Workflow Attributes</b>		
<input type="checkbox"/> FormID	LDAP Attribute:	
<input type="checkbox"/> Supervising UserID	LDAP Attribute:	
<input type="checkbox"/> ReassignWork	LDAP Attribute:	
<b>Routing Preferences</b>		
<input type="checkbox"/> WorkList User	LDAP Attribute:	
<input type="checkbox"/> Email User	LDAP Attribute:	
<input type="checkbox"/> Forms User	LDAP Attribute:	

PeopleTools, Maintain Security, Setup, Directory Authentication, Optional User Properties

If you want to incorporate an existing LDAP attribute to an equivalent PeopleSoft field, you use this page to map the LDAP attribute to the PeopleSoft field. To do so, click the checkbox next to PeopleSoft value. This enables the LDAP Attribute edit box in which you add the corresponding LDAP attribute name.

This page enables you to take advantage of LDAP information. Keep in mind that PeopleSoft retrieves the LDAP information and creates a local cache in database tables. PeopleSoft applications use this cache rather than making a call to LDAP each time a transaction requires user information. This means that after a user signs on and the Signon PeopleCode executes, there is a row for that user in the user definition table. You do not need to maintain the local cache of user information; Signon PeopleCode maintains this row automatically. Whatever changes are made in the directory server, are propagated to the local cache.

---

## Directory Group Import

The Directory Group Import functionality enables you to retrieve a list of group names from your LDAP configuration and insert them into the PeopleSoft database. This allows PeopleSoft applications to prompt against the list of LDAP groups. PeopleSoft needs to prompt against LDAP group information when you are implementing dynamic roles based on LDAP directory group structure. When you specify the Directory Rule Enabled, you need to assign the directory group list that you import with this utility.

The utility you use to import LDAP Group values is called “Directory Group Import”. Directory Group Import enables you to define how data should be mapped between an LDAP object and a PeopleSoft Record. Specifically, you import the LDAP values into PeopleSoft and populate a pre-

defined record called PS\_DIRGROUPS. Then, the Roles component prompts against the PS\_DIRGROUPS table for the LDAP Group name value.

The Directory Group Import functionality consists of an Import Map definition that you create. Then you run an underlying Application Engine program called LDAPMAP, which contains a PeopleCode program with a function that calls a Business Interlink. This Business Interlink makes the appropriate calls to the LDAP directory and returns the appropriate values to your PeopleSoft system.

You define the LDAP import map by selecting **Maintain Security, Setup, Directory Group Import, Settings**. Then after you define the map, you run the import process by selecting **Maintain Security, Process, Directory Group Import**.

The LDAP Map is intended for a very specific purpose, which is to import LDAP Group name values into your PeopleSoft system and populate the pre-defined record, PS\_DIRGROUPS. PeopleSoft supports only limited customizations to this functionality. Supported customizations are discussed in the following procedure.

This following procedure covers defining your import map.

To define an LDAP map

1. Select PeopleTools, Maintain Security, Setup, Directory Group Import, Settings.

This reveals the following component.

The screenshot displays the 'Directory Group Map' settings page. At the top, there are tabs for 'Settings' and 'Attributes'. Below the tabs, the title 'Directory Group Map' is shown, followed by 'Map Name: DIRGROUPS'. The page is divided into three main sections: 'Directory Connect Information', 'User Search Information', and 'Target'. The 'Directory Connect Information' section includes fields for 'Server name' (billyp.peoplesoft.com), 'Port' (389), 'User DN' (cn=Admin,o=PeopleSoft), and 'Password' (masked with asterisks). The 'User Search Information' section includes a 'Scope' dropdown (set to SUB), a 'Search Base' field (o=PeopleSoft), and a 'Filter' field ((objectclass=groupOfNames)). The 'Target' section includes a 'Message' field (DIRGROUPS) and a search icon.

PeopleTools, Maintain Security, Setup, Directory Group Import, Settings

2. On the **Settings** page, specify the values that identify the appropriate directory server to enable a successful connection.

Enter the appropriate values in the Directory Connect Information group.

- **Server name.** Enter the name of the LDAP server.
- **Port.** Specify the LDAP connection port.
- **User DN.** This refers to the “distinguished name” of the user name used to connect to the LDAP server when running the import. This user must have permission to retrieve all the required data.
- **Password.** Enter the password for the User DN, or connect user. This password is encrypted and stored in the database.

Enter the appropriate values in the **User Search Information** group.

- **Scope.** Define the scope of the search. SUB, or “Sub Tree” means the search starts at “Search Base” and continue searching all the child nodes, and their child nodes, and so on. ONE means search begins at one level beneath the Search Base that you specify. Base means the searches only covers the Search Base that you specify.
- **Search Base.** This refers to the location in the LDAP tree in which the search is to start.
- **Filter.** Enter the LDAP search filter. The filter is similar to a SQL "WHERE" clause. The example shows Filter specifying all objects that are groups.

Enter the appropriate values in the **Target** group. Here you specify the “message” into which the system writes the returned values from the LDAP search.

You do this using the **Message** drop-down. In this context, the Message value refers to the record that the LDAPMAP program populates with data. The attribute values specified on the **Attributes** page returned from LDAP are mapped into the Record/Fields specified in the message.



**Note.** PeopleSoft only supports specifying the DIRGROUPS message (record). The only supported customization is changing the name of the LDAP attributes to which the fields in PS\_DIRGROPS are mapped.

3. Select the **Attributes** page, and associate PeopleSoft fields with their LDAP counterparts.

Field Name	LDAP Attribute Name
GROUPNAME	cn
DESCRLONG	description

PeopleTools, Maintain Security, Setup, Directory Group Import, Attributes

In the **Field Name** column, select the appropriate PeopleSoft field from the drop-down list.



In the adjacent **LDAP Attribute Name** edit box, enter the LDAP value to which the PeopleSoft field needs to be mapped. The name must exactly match what appears in the LDAP directory.



**Note.** The only customization PeopleSoft supports is modifying the **LDAP Attribute Name** such that it exactly matches the value that appears in the LDAP directory. For example, for DESCRLONG perhaps the equivalent value in your LDAP directory might be *longdescription*. Modify the **LDAP Attribute Name** accordingly.

4. After entering the appropriate connect and attribute information, save your work.



For more information on running the import map process, see Directory Group Import.

## Security Links

If you administer security information outside of the Maintain Security interface, as in you use application-specific pages for application security, then you have the option of adding links to those pages to the Maintain Security interface. This enables administrators a convenient way to access application-specific security pages without having to spend time navigating to them.

You add the extra security links by selecting **PeopleTools, Maintain Security, Setup, Security Links**. You can add links to the User Profile component, the Role component, or the Permission List component. To add links to a security profile, just select the appropriate page in the Security Links component and add the link information for the target page. After you save your link information, the link appears on the Links page for the appropriate security profile. For instance if you add an additional security link to the User page in the Security Links component, then when you modify a user profile in the User Profiles component, the Links page contains the link to the application-specific security administration page.

Description	*Menu Name	*Menu Bar Name	Bar Item Name	Item Name	Test
HR Query User	ADMINISTER_HR_SECURITY	USE	QUERY_SECURITY	QUERY_PROFILE	Test

PeopleTools, Maintain Security, Setup, Security Links, Permission Lists

To add a Security Link

1. Select PeopleTools, Maintain Security, Setup, Security Links.
2. Select the security profile type, as in user, role, or permission list, to which you want to add

extra links.

3. If there are existing links, click the plus sign button to add a new row.
4. Add the following information on the User, Role, or Permission List page:
  - **Description.** Add a description of the page that contains the extra security information. This description is the text that appears on the Links page for the security profile.
  - **Menu Name.** From the drop-down list add the menu name. This is the application in which the page resides, such as Administer HR Security.
  - **Menu Bar Name.** From the drop-down list add the menu bar name, such as Use, Setup, Process, and so on.
  - **Bar Item Name.** From the drop-down list add the bar item name. For instance the bar item name for this page is Security Links.
  - **Item Name.** From the drop-down list add the item name. For instance, the item names for this component are User, Role, and Permission List.
5. After you've entered the appropriate link information, click **Test** to make sure the link is pointing to the correct target.
6. Save your work.



If you need to migrate the security links setup data from one database to another. You can use the following Data Mover scripts, SECOTHER\_EXPORT.DMS and SECOTHER\_IMPORT.DMS. These scripts reside in the \<PS\_HOME>\scripts directory.

---



---

## Single Signon

PeopleSoft supports single signon for use with the PIA configuration. Within the context of your PeopleSoft system, single signon means that after a user has been authenticated by one PeopleSoft application server, that user can access a second PeopleSoft application server without entering an ID or a password. Although the user is actually accessing a different application and database, the user navigates seamlessly through the system. Recall that each suite of PeopleSoft applications, such as HR or Student Administration, resides in its own database.

After the first application server/node authenticates a user, PeopleSoft delivers a web browser cookie containing an authentication token. PIA uses web browser cookies to store a unique access token for each user after they are initially authenticated. When the user connects to another PeopleSoft application server/node, the second application server uses the token in the browser cookie to re-authenticate the user behind the scenes so they don't have to go through the signon process again.

Single signon is critical for PeopleSoft portal implementations because the portal integrates content from various data sources and application servers and presents them in a unified interface. When the users sign on through the portal, they always take advantage of single signon. Users

need to signon once and be able to navigate freely without encountering numerous signon screens. Because single signon is so integral to the portal, you always need to configure it before deploying the portal.



The browser cookie is an in-memory cookie and is never written to disk. The cookie is also encrypted to prevent snooping and digitally signed using a check sum to prevent tampering.

The following table presents the fields that appear in the PeopleSoft authentication token.

<b>Field</b>	<b>Description</b>
UserID	This field contains the user ID of the user to which the server issued the token. When the browser submits this token for single signon, this is the user that the application server logs on to the system.
Language Code	This field specifies the language code of user. When the system uses his token for single signon, it sets the language code for the session based on this value.
Date and Time Issued	This field specifies the date and time the token was first issued. The system uses this field to enforce a time out interval for the single signon token. Any application server that accepts tokens for signon has a "time out minutes" parameter configured at the system level. A system administrator sets this parameter using the Maintain Security, Setup, Single Signon page. The value is in Greenwich Mean Time (GMT) so it does not matter which time zone the application server is in.
Issuing System	This field shows the name of the system that issued the token. When it creates the token, the application server retrieves this value from the database. Specifically, it retrieves the defined Local Node used for application messaging. Single signon is not related to application messaging, except for the fact that single signon functionality leverages the messaging concept of message nodes, and local nodes. You configure a node only to "trust" single signon tokens from specific nodes. Consequently, an application server needs a value of "issuing system" so that it can check against its list of trusted nodes to see if it "trusts" the issued token.

<b>Field</b>	<b>Description</b>
Signature	<p>This field contains a digital signature that enables the application server using a token for single signon to ensure that the token hasn't been tampered with since it was originally issued. The system issuing the token generates the signature by concatenating the contents of the token (all the fields that appear in this table) with the message node password for the local node. Then the system hashes the resulting string using the SHA1 hash algorithm. For example ("+" means concatenation),</p> <pre>signature = SHA1_Hash ( UserID + Lang + Date Time issued + Issuing System + Local Node Pswd )</pre> <p>There is only one way to derive the 160 bits of data that make up the signature, and this by hashing exactly the same User ID, Language, Date Time, Issuing System, and node password.</p>



Single signon does not depend on LDAP directory authentication. You can implement single signon and not LDAP, you can implement LDAP and not single signon, or you can implement both LDAP and single signon.

To summarize, the key security features of the cookie authentication token are:

- The cookie exists in memory; it is not written to disk.
- There is no password stored in the cookie.
- You can set the expiration of the cookie to be a matter of minutes or hours. Hardly enough time for a hacker to decrypt the information.

## Single Signon Component

The following topics describe the settings you modify when implementing single signon.

Single Signon			
<b>Authentication Token expiration time</b>			
Expiration Time in minutes:	<input type="text" value="720"/>	Valid values are 1 - 10,000	
<b>Trust Authentication Tokens issued by these Nodes</b>			
Message Node Name	Description	Local Node	Distinguished Name
<input type="text" value="QE_LOCAL"/>		1	
		<input type="button" value="+"/> <input type="button" value="-"/>	

PeopleTools, Maintain Security, Setup, Single Signon

### *Authentication Token expiration time*

You need to set an expiration time for tokens this system accepts for authentication. Otherwise, the user, once authenticated could be authenticated, and signed on to the system with the token,

for as long as it stays up and running. You can set the authentication interval to be minutes, hours, or days depending on your signon strategy.

The value is in minutes. For example, 480 minutes is 8 hours. This is global setting for all users of your PeopleSoft system that get issued the cookie. A short expiration period is more secure, but less convenient because users need to enter their passwords more frequently.

The system accepting the token controls the expiration time, not the issuing system. For instance, suppose Node HRMS\_WEST, which has an expiration time of 100 minutes, issues a token to a user. Then let's say the user attempts to use that token to sign on to Node FIN\_EAST, which has an expiration time set to 60 minutes. In such a situation, if a period greater than 60 minutes has transpired, then Node FIN\_EAST rejects the token. When a node rejects a single signon token, the system prompts the user to enter a user ID and password on the standard signon screen.



---

This expiration time is separate from the timeouts you specify in the Permission Lists and the web server configuration files.

---

### ***Trust Authentication Tokens issued by these Nodes***

In order to "share" authentication tokens between nodes, the nodes need to "trust" each other. By adding a node to this grid, you indicate that a particular node is known to the system and trusted and as such the local node accepts tokens issued by it.

By default, no nodes appear in the "trusted" nodes. If you want to implement single signon, you need to explicitly configure your system to support it by adding trusted nodes.

First, you need to add the local node to the grid. A node must be able to trust its own tokens. When you sign on to the portal, the system authenticates users with a single signon token issued by the local system. The portal won't be able to sign on unless the local node is trusted.



---

You define nodes (Message Nodes) in Application Designer.

---

### **Sample Single Signon Transaction**

Now that you have a general understanding of why a single signon implementation is useful and some of the details involved with PeopleSoft single signon, this section presents an example of how the PeopleSoft single signon scheme works.

Suppose there are two databases, or nodes: and HRMS database and Financials database. Recall that the terms database and node are synonymous. Each database has one application server and one web server. The following steps describe the "under-the-covers" events that occur when a user signs on to the HRMS database, completes a transaction, and then click a link that targets a page in the Financials database.

### Step 1: User Signs on to HRMS Application

- User PTDMO goes to link <http://HRMS.peoplesoft.com/peoplesoft8/signon.html>
- User enters ID and Password at the signon page, clicks login.

### Step 2: Application Server Authenticates User

- Web server relays login request to HRMS application server.
- Application server authenticates the user.

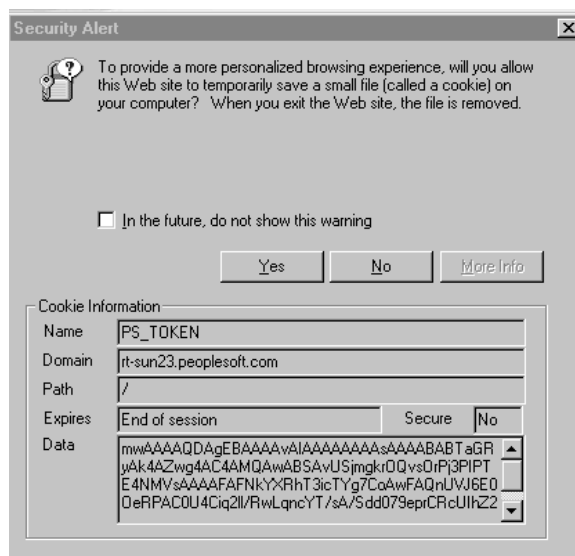
### Step 3: Application Server Generates Single Signon Token

- If the signon attempt to the HRMS application server is successful, the application server generates a single-signon token. This token contains the following fields: User ID, Language Code, Date and Time Issued, Issuing System, and Signature.
- Application server encrypts and base 64 encodes the token.
- Application server sends the token to the web server, along with a return code indicating that the system authenticated the user.

### Step 4: Web Server Creates Cookie in User's Browser

When the web server receives the single-signon token from the application server, it creates a cookie and inserts a cookie in the user's browser.

If the browser is configured to show the Security Alert dialog, then the user sees a message similar to the following example. In most cases, you don't configure browsers to show this dialog; this dialog box is just an example of the data that's the browser receives.



Message Alerting User about the Cookie

The cookie that the web server distributes for PeopleSoft single signon is named PS\_TOKEN.. In this case the domain, rt-sun23.peoplesoft.com, set the cookie.

Notice that the cookie expires at the end of session. This indicates that the system never writes the cookie to disk, the cookie exists in the memory of the browser for the duration of the session.

The web server inserts the single-signon token within the "Data" field of the cookie. So that the system can send the character data across the HTTP protocol, the cookie is encrypted and base 64 encoded.

### Step 5: User Needs to Access Financial Application

After the user completes a few transactions in the HRMS system, suppose they arrive at a page containing a link to the Financial system. The user clicks the link, and because they've already signed on (entered their ID and Password) to the HRMS system they don't need to sign on again.

The user's browser sends the PS\_TOKEN cookie to the Financials web server.

### Step 6: Financials Web Server Receives PS\_TOKEN Cookie

The Financials web server detects that the user hasn't been authenticated by the Financials system yet, however, because the web server received the signon cookie it does not display the signon page.

To retrieve the page the user requested (by way of the link in the HRMS application), the Financials web server attempts to connect to the Financials application server. It only passes the Data field from the PS\_TOKEN cookie; the application server only needs the information in the Data portion.

### Step 7: Financials Application Server Authenticates PS\_TOKEN

The Financials application server performs the following checks against the PS\_TOKEN Data field before allowing the user to connect:

- **Trusted Node?** The application server checks to see that the message node name listed as the "Issuing System" is a "trusted" node. The list of trusted nodes for the Financials system resides in the PSTRUSTNODES table. You configure the list using Maintain Security, Setup, Single Signon. The Single Signon page enables the administrator of the Financials system to "trust" authentication tokens generated from HRMS as well as any other nodes deemed "trusted."
- **Has the token expired?** The application server checks that the authentication token hasn't expired. Using the Issued Date and Time field within the token, the Financials application server makes sure that the token was issued within the interval between the "time out minutes" value and the current time. You configure a token's expiration time on the Maintain Security, Setup, Single Signon page.



It is important to note that the expiration parameter specified in the Financials system is the relevant value, not the expiration value specified in HRMS. This enables the Financials administrator to control the maximum age of an acceptable token. It's also important to consider that all times are in Greenwich Mean Time (GMT), so it doesn't matter what time zones the systems are in.

---

- **Has the signature been tampered with?** The application server checks that the signature is valid. The Financials application server takes all the fields in the token and the Node password for the issuing node and generates a hash. The token is valid only, if the signature within the token *exactly* matches the one generated by the Financials application server. Because an exact match is the only acceptable situation, Financials can be sure that HRMS generated the token, and that it hasn't been tampered with since it was generated. If a hacker intercepted the token in transit and changed the User ID, Language, and so on, the signatures wouldn't match and as a result the Financials application server would reject the token.



For this scheme to work, the HRMS and Financials systems must share a secret, the Message Node password. The message node password for the local node in the HRMS system must match *exactly* the password on the HRMS node definition in the Financials system. This same requirement exists if you publish application messages across domains using password authentication.

---

## Single Signon Configuration Considerations

The following topics describe some items you may want to consider as you implement your single signon configuration.

### *Single Domain Limitation*

Web servers must be part of the same domain, and the server name in the URLs used to access them must contain the domain name. Browsers only send cookies back to the same domain from which it received the cookie.

Furthermore, the server that generates the cookie needs to have the domain that shares the PS\_TOKEN cookie specified in the configuration.properties of the local PIA web site. For example, in the context of our HRMS to Financials example, the configuration.properties file in the peoplesoft8 directory for the HRMS web server must contain the following value for the AuthTokenDomain parameter:

```
AuthTokenDomain=.peoplesoft8.com
```



You must specify the leading dot (.).

---

The single domain issues occur in the following situations:

- You're using straight PIA, as in you are deploying applications but not by way of the portal.
- You're using the portal with frame-based templates. Frame-based templates aren't proxied automatically. Proxying just means that a URL is rewritten to point to a location on the portal servlet, rather than the original location of the URL.

You can avoid this limitation by using the portal and configuring it to proxy web content from servers in different domains. For example, you could implement single signon between



hrms.vantive.com and fin.peoplesoft.com if both web servers are registered as content providers in the portal. In this case, the portal proxies the content from these servers.



For more information on the PeopleSoft Portal, template types, the proxy process, see Portal Technology.

### ***Domain Names***

You need to use a fully qualified domain name when addressing the web server in your browser. For example, you would need to enter the following:

```
//todd.peoplesoft.com
```

and not the following:

```
//todd/peoplesoft8/signon.html
```

---

## **Digital Certificates**

PeopleSoft leverages HTTPS, Secure Socket Layer (SSL), and digital certificates to secure the transmission of data from the web server to an end user's web browser and also to secure the transmission of data between PeopleSoft servers and third party servers (for B2B processing) over the internet.

PeopleSoft customers can implement PIA using HTTP or HTTPS. The native SSL support in commercially available web browsers and web servers is used to provide HTTPS communication between the web browser and web server.

### **Why Implement SSL?**

With B2B applications, where systems communicate with each other over the internet, data must flow securely. As such, system-to-system authentication is critical. PeopleSoft Internet Architecture leverages HTTPS and digital certificates for secure transmission of data between systems and system-to-system authentication. The SSL implementation for secure HTTP is provided through the use of the Entrust/Toolkit™ for Java™ that is embedded within PeopleTools. This requires no additional Entrust Technologies licensing by PeopleSoft customers and is designed for use with digital certificates provided by popular certificate authorities including Entrust and VeriSign.

PeopleSoft uses Extensible Markup Language (XML) messaging over HTTPS in Application Messaging and Business Interlink technologies to deliver system-to-system integration over the Internet. HTTPS is used to guarantee secure transmission of the XML message. The digital signature of the XML message is used for authentication between systems. Using digital certificates, XML messages are digitally signed to prove that the message came from the server that created and signed the message and to prove the message has not been altered.

The following table shows the PeopleSoft technologies that leverage HTTPS / SSL and how it is implemented in for each technology.

<b>Technology</b>	<b>How Used</b>	<b>How HTTPS/SSL is provided</b>
PIA Transactions	Secure page transport	Uses web server platform to provide server side SSL.
PeopleSoft Portal	Secure page transport	Uses web server platform to provide server side SSL.
	Secure access to remote content providers	Application Server uses the embedded Entrust SSL Toolkit for Java to provide client side of SSL connection to gateway.  Uses web server platform to provide server side SSL.
Application Messaging	Secure message transport to remote nodes	Application Server uses the embedded Entrust SSL Toolkit for Java to provide client side of SSL connection to gateway.  Uses web server platform to provide server side SSL.
Business Interlinks	Secure calls to remote data sources or modules	Application Server uses the embedded Entrust SSL Toolkit for Java to provide client side of SSL connection to gateway.  Uses web server platform to provide server side SSL.
User Authentication	Certificate-based client authentication	Use web server SSL client authentication; pass certificate data to application server.  Application Server trusts web server's authentication; uses distinguished name of certificate to logon to PeopleSoft system.

## Certificate Authorities

Anytime you implement SSL with mutual authentication (both client and server authenticate to each other) you need the following three items:

- Server Certificate (issued by some trusted third party or certificate authority)
- Client Certificate (issued by the same trusted third party or certificate authority)
- Client and server both need a copy of a root certificate for the trusted third party. The root certificate has the crypto keys of the authority. Using these keys and the client and server

certificates, each party is able to authenticate the other.

When you logon to an SSL server using your browser, you don't have to worry about a Root Certificate because they come bundled with the browser.

You don't have to worry about having a client certificate for yourself because the web server doesn't require "Client Side Authentication".

## Administer Certificates Page (Key Management)

The Administer Certificates page displays your inventory of server-side digital certificates. This page also enables you to import new certificates from a certificate authority.



For user certificates, no redundant setup of user certificates is required. With a few lines of Signon PeopleCode, you can reuse the existing PKI server you have in place.

To view details regarding a particular certificate, click **Details**.

Digital Certificates					
Digital Certificates					
Find First 1-17 of 17 Last					
*Type	*Alias	*Issuer Alias			
Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root	<a href="#">Detail</a>	+	-
Root CA	GTE CyberTrust Root	GTE CyberTrust Root	<a href="#">Detail</a>	+	-
Root CA	KeyWitness Root	KeyWitness Root	<a href="#">Detail</a>	+	-
Root CA	PeopleTools	PeopleTools	<a href="#">Detail</a>	+	-
Root CA	Root SGC Authority	Root SGC Authority	<a href="#">Detail</a>	+	-
Root CA	Thawte Personal Basic	Thawte Personal Basic	<a href="#">Detail</a>	+	-
Root CA	Thawte Personal Premium	Thawte Personal Premium	<a href="#">Detail</a>	+	-
Root CA	Thawte Premium Server	Thawte Premium Server	<a href="#">Detail</a>	+	-
Root CA	Thawte Server	Thawte Server	<a href="#">Detail</a>	+	-
Root CA	Verisign Class 1	Verisign Class 1	<a href="#">Detail</a>	+	-
Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2	<a href="#">Detail</a>	+	-
Root CA	Verisign Class 2	Verisign Class 2	<a href="#">Detail</a>	+	-
Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2	<a href="#">Detail</a>	+	-
Root CA	Verisign Class 3	Verisign Class 3	<a href="#">Detail</a>	+	-
Root CA	Verisign Class 3 - G3	Verisign Class 3 - G3	<a href="#">Detail</a>	+	-
Root CA	Verisign Class 4	Verisign Class 4	<a href="#">Detail</a>	+	-
Root CA	Verisign/RSA Secure Server CA	Verisign/RSA Secure Server CA	<a href="#">Detail</a>	+	-


PeopleTools, Maintain Security, Setup, Digital Certificates

The Certificate Detail page reveals subject and certificate information so you can determine such characteristics such as the serial number, the fingerprint, the encryption algorithm, and so on.

Certificate Detail - GTE CyberTrust Global Root	
<b>Subject Information</b>	
<b>Common Name:</b>	GTE CyberTrust Global Root
<b>Org Unit:</b>	GTE CyberTrust Solutions
<b>Organization:</b>	GTE Corporation
<b>Locality:</b>	
<b>State/Province:</b>	<b>Country:</b> US
<b>Certificate Information</b>	
<b>Serial Number:</b>	01:A5
<b>Fingerprint:</b>	CA:3D:D3:68:F1:03:5C:D0:32:FA:B8:2B:59:E8:5A:DB
<b>Valid from</b>	07/03/1998 17:29:00 to 07/01/2018 16:59:00
<b>Algorithm:</b>	MD5 with RSA encryption
<b>Description:</b>	<div> Version: 1  Serial number: 421  Signature algorithm: md5WithRSAEncryption  Issuer: CN=GTE CyberTrust Global Root, OU=GTE CyberTrust Solutions, Inc., O=GTE Corporation, C=US  Valid not before: Wed Aug 12 17:29:00 PDT 1998 </div>
<a href="#">Return</a>	

PeopleTools, Maintain Security, Setup, Digital Certificates, Details

To add a digital certificate

1. Select PeopleTools, Maintain Security, Setup, Digital Certificates.
2. Click .

This adds a new row to the grid.

3. From the **Type** drop-down list, select a certificate type.

You have two options: Root or Node.

4. Enter the Alias and Issuer Alias values.
5. Click Request.

The Request New Certificate page appears.

6. Enter the necessary information on the Request New Certificate page.
  - Subject Information.
  - Key Pair Information.
  - Additional Certificate Attributes.
7. After entering values on the Request New Certificate page, click **OK**.

## Configuring SSL for Application Messaging

The following sections describe the steps you need to complete to configure Securer Socket Layer (SSL) security for use with application messaging.

For SSL with application messaging, we require SSL with client-side authentication. This means that you need all three of the certificates. The following list outlines the items that you need to complete to implement Application Messaging SSL.

- **Server certificate.** You need to get a web server certificate and import it into the web server. The certificate can be from any certificate authority, including an internal corporate certificate authority that issues its own certificates.
- **Client certificate.** You also need to get a client certificate. In Application Messaging, the SSL client *is not* the browser. The client is the application server posting the message. For the root certificate on the client (application server) side, PeopleTools bundles root certificates from the leading certificate authorities, just like web browsers and servers do. You have the option of getting other certificates for the application server and importing them into the database using the Administer Certificates page in Maintain security.
- **Root certificate.** For the root certificate, your web server came bundled with certificates from the leading certificate authorities. You may also import a root certificate from your own certificate authority.



The following sections assume a general knowledge of Application Designer, Message Nodes, and Maintain Security. Also, you should have working knowledge of Certificate Authorities (CA) and digital certificates.

---

### Source Node

The following procedure describes the steps you need to complete on the source node, the node making the HTTP message post.

To configure the source node for SSL

1. Make sure you have the Sun Java Runtime Environment version 1.2 (JRE 1.2) installed.
2. In the application server configuration file, set the JavaVM Shared Library parameter in the PSTOOLS section.

For example

```
<jre install location>\bin\classic\jvm.dll
```

3. Clear your classpath environment variable.

For example, from the command prompt, enter:

```
set classpath=
```

4. Configure your application server using PSADMIN, and include the application messaging (pub/sub) servers.
5. Boot the application server.
6. In Application Designer, perform the following:
  - Confirm that the local node is defined and marked as "local." You do this on the Message Node Properties dialog box, while the Message Node is active.
  - Create a node definition for the target node. Specify the URL of the gateway servlet for the remote node location. For example,

```
https://<web server>/servlets/psft.pt8.gateway.GatewayServlet
```



To use SSL, the URL scheme must be HTTPS.

---

7. Select PeopleTools, Maintain Security, Setup, Digital Certificates, and add a Root CA for the certificate.
  - Create a new Node certificate. If the root certificate for the CA you are going to obtain the node certificate from is not already in the key store, import it.
    - Add a new row
    - Select Root CA for the certificate type
    - Enter the certificate alias
    - Click on the Import link.
    - Paste the base64-encoded, DER-formatted X509 certificate data into the form. It should look something like the following example:

```
-----BEGIN CERTIFICATE-----
```

```
MIICIDCCAcgAwIBAgIQrDVQJKAACLQR0/bIDJMSVDANBgkqhkiG9w0BAQQFADBy
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExEzARBgNVBAcTC1BsZWZzYW50b24x
FzAVBgNVBAoTD1Blb3BsZVNvZnQgSW5jMRMwEQYDVQQLEwpQZW9wbGVUb29sMRMw
EQYDVQQDEwpQZW9wbGVUb29sMB4XDTAwMDMxMDIxMTIzNV0XDTA1MDMxMDIxMTIz
NVowcjELMAkGA1UEBhMCVVMxChAJBgNVBAgTAKNBMRMwEQYDVQQHEwpQbGVhc2Fu
dG9uMRcwFQYDVQQKEw5QZW9wbGVUb29sIEluYzEzMTBEGA1UECzMxKUGVvcGx1VG9v
bDETMBEGA1UEAxMKUGVvcGx1VG9vbDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCy
o44wplb57M272GRP3sC4TtLm/MD1G9osRjG9BwnsjjTij9GNI6Rnf9cNxxj+AGQY
gnE3P7lp9rYN6GQxPlDNagMBAAGjPDA6MA5GA1UdDwQEAwIBxDAMBGNVHRMEBTAD
```

```
AQH/MB0GA1UdDgQWBBSkFZJ1Dtt5uE6muLRN3rwRPsUCsTANBgkqhkiG9w0BAQQF
AANBAJec3hFPS2SLSDtflI9mSA7UL1Vgbxr5zZ4Sj9y4I2rncrTWcBqj7EBp9n/Z
U/EwDEljVbE8SSDYr1Emgoxsr4Y=
-----END CERTIFICATE-----
```

- Click **OK**.
8. Also on the Digital Certificates page, click the **Detail** link for the new root certificate, and perform the following:
    - Confirm that the information is correct.
    - Add a new row.
    - Select *Node* for the certificate type.
    - Enter the name of the local message node for the certificate alias.
    - Enter the root CA alias for the issuer alias, or select one from the drop-down list.
    - Click the **Request** link.
    - Fill in the certificate request form.
    - Click **OK**.
  9. Send the request form to the CA.
    - Copy the generated certificate-signing request. You may want to save it to a file. If you lose this information, you have to delete the certificate and start over.
    - Click **OK**.
    - Submit the certificate-signing request to the CA of your choice. This process varies for each CA.
    - The CA verifies the information in the certificate, signs the certificate with its private key, and returns the signed certificate to you.
  10. When you receive the signed certificate from the CA, go to the Digital Certificates page and perform the following:
    - Click **Import** for the new node certificate.
    - Paste the base64-encoded, DER formatted X509 certificate data into the form.
    - Click **OK**.
    - Click the **Detail** link for the new node certificate, and confirm that the information is correct.

## *Target Node*

The following procedure describes the steps you need to complete for the target node.



---

The following steps need to be completed in Application Designer on the target node.

---

To configure the target node for SSL

1. In Application Designer, confirm that the local node exists.
2. Create a Message Node definition for the source node.
3. In the **Message Node Properties** dialog box, set the Distinguished Name (DN) to reflect the subject DN for the source node certificate.

For example,

```
CN=cdodtx, OU=Appserv, O=My_organization, L=Pleasanton, ST=California, C=US
```

You can obtain the DN information two ways:

- Viewing the certificate information on the Digital Certificates page.
- Importing the source node certificate using your browser. This applies when you do not have access to the application server for the source node. Otherwise, use the Maintain Security interface.

## *Web Server*

To enable SSL security for application messaging you also need to perform the following tasks on your web server:

- Configure SSL for the web server.
- Enable SSL with client authentication.
- Configure the gateway lookup entry for the destination node.

## **Security Processes**

PeopleSoft delivers security batch processes that you run to execute your dynamic role rules or to import LDAP directory information into your PeopleSoft system. The following topics describe the options on the PeopleTools, Maintain Security, Process menu.



---

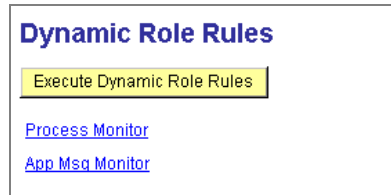
## Execute Role Rules

In the Roles chapter you learned about dynamic and static membership to roles. To manually kick off the DYNROLE\_PUBL Application Engine program, you do so from the Execute Role Rules.



For more information on dynamic roles program, see Roles.

---



PeopleTools, Maintain Security, Process, Dynamic Role Rules

To execute the program, click **Execute Dynamic Role Rules**. To view the status of the program run and/or the generated application message click **Process Monitor** and **App Msg Monitor**, respectively. Keep in mind that not only the program needs to run to completion, but the application message needs to be delivered successfully as well.



This batch program executes the role rules for all of your roles. You can execute rules one-by-one using Maintain Security, Use, Roles, Dynamic Members.

---

To make the program run at a regularly scheduled time, as in once a day, you use the Process Scheduler. This involves creating a process definition for the DYNROLE\_PUBL program, and running the program with your custom recurrence definition.



For more information on using Process Scheduler, see Process Scheduler..

---



---

## Directory Group Import

After you have entered the required values on the Directory Group Import Settings and Attributes pages, you run the LDAPMAP Application Engine program. The values you entered on the Settings and Attributes pages get inserted into the State Record associated with LDAPMAP when the program runs.

**LDAP Map**

Run Control ID: LARD      [Report Manager](#)    [Process Monitor](#)    [Run](#)

Map Name:

PeopleTools, Maintain Security, Process, Directory Group Import

The following procedure describes the steps for invoking LDAPMAP.

To invoke the LDAPMAP program

1. Select PeopleTools, Maintain Security, Process, Directory Group Import.
2. Add a new Run Control ID or select an existing Run Control ID.
3. From the **Map Name** drop-down list on the LDAP MAP page, select the LDAP map that you need to run.
4. Click **Run**.
5. On the **Process Scheduler Request** dialog, specify any options you require, such as **Run Location**, and click **OK**.
6. View the status of the program run by clicking **Process Monitor**, or check the output by clicking **Report Manager**.



For more information on running process requests through Process Scheduler and the Report Manager, see Process Scheduler.

## Other Security Administration Tasks

The following topics describe other tasks related to security that are not included in the Maintain Security interface. For instance there are tasks that you complete in Application Designer, and there are also scripts that you can run outside of Maintain Security through Data Mover.

---

### Setting up Access Profiles

Every user Profile must be assigned to an Access Profile, by way of a Symbolic ID. The Access ID consists of an RDBMS ID and a password, and these IDs must have system administrator privileges. Access profiles provide the necessary IDs and passwords for the behind-the-scenes database logon that occurs. Access IDs are used in the following two situations:

- When an application server boots and connects to the PeopleSoft database.
- When a developer or power user, signs on to the PeopleSoft database directly (two-tier).

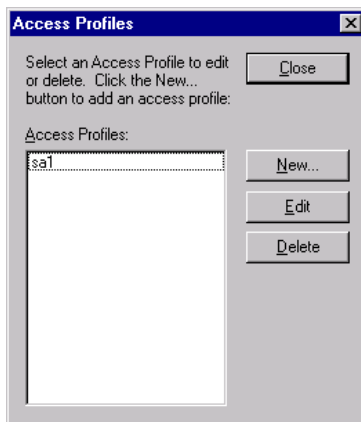
- When batch programs connect to the database.

User's signing onto the system through PIA, take advantage of the Access ID that the application server used for connecting to the database.

Access profiles allow you to minimize the number of Maintain Security users who need to know system administrator passwords. In fact, only one person needs to know these passwords. That person can create the required Access Profiles—by providing the necessary passwords, when prompted—and all other Maintain Security users can simply assign users to the pre-defined Access Profiles. The Access ID and password are encrypted in the database.

Before you begin creating your User Profiles, Roles and Permission Lists, you first need to set up your Access Profiles on the database. Ultimately, the Access Profile is the profile that your users use to connect to your PeopleSoft database. Without being associated with an Access Profile, users can't signon, not even with a test ID.

The ID that you use must be defined at the RDBMS level as a valid RDBMS ID possessing system administrator rights. You don't use PeopleSoft or PeopleTools software to create the RDBMS ID. You need to create it using the utilities and procedures defined by your RDBMS vendor. After you have created the RDBMS ID with system administration authority, then you use the PeopleTools Access Profiles utility to link your RDBMS ID to the Access Profile. You manage Access Profiles using the Access Profiles dialog, which you open from Application Designer by selecting **Tools, Miscellaneous Objects, Access Profiles**.

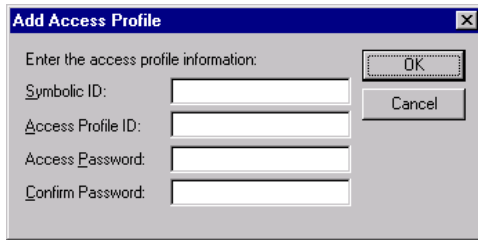


Access Profiles Dialog

This dialog lets you add, modify, and delete Access Profiles. The topics guide you through the tasks you can complete using the Access Profiles dialog box.

## Access Profile Properties

When you create or modify an Access Profile using the Access Profiles dialog, you will need to understand the properties that comprise an Access Profile. After reading this section, you will be familiar with these properties.



Add Access Profile Dialog

The following topics describe the Access Profile properties.

### ***Symbolic ID***

The Symbolic ID is used as the key to retrieve the encrypted ACCESSID and ACCESSPSWD from PSACCESSPRFL. For initial installation we suggest that you set it equal to the Database Name.

### ***Access Profile ID***

The Access Profile ID must be a valid RDBMS ID with system administrator privileges, and the Access Profile ID must match the associated RDBMS ID. PeopleSoft assumes that the RDBMS ID that you choose is the same as the Access Profile ID.




---

For more information on creating RDBMS IDs for your RDBMS, refer to the documentation supplied by your RDBMS vendor.

---

The Access ID also must be a different logon ID than the User ID. There is logic within PeopleTools such that if Access ID = User ID, PeopleTools does not log off and log on again, nor does the system issue a SET CURRENT SQLID = 'owner ID'.




---

**DB2** In DB2 terminology, Access ID is the “primary” ID and Owner ID is a “secondary” Auth ID. If the Access ID does not equal the owner ID, secondary authorization security exists in DB2 to issue a SET CURRENT SQLID command. DB2 will qualify tables (required) with the Owner ID provided by SET CURRENT SQLID statements issued by the PeopleSoft software. If the access ID equals owner ID, then secondary authorization exits are not required. DB2 will qualify the table name with the access ID.

---

### ***Access Password***

The Access Password is the password associated with your RDBMS ID/Access Profile ID. It's the password that the Access ID uses to signon to the database.

## Working with Access Profiles

This section covers the procedures that you complete while adding, modifying, or removing Access Profiles in your PeopleSoft system.

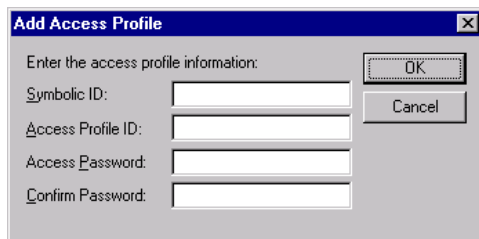
To create a new Access Profile definition

1. In Application Designer, select Tools, Miscellaneous Objects, Access Profiles.

The Access Profiles dialog appears.

2. Click **New**.

The Add Access Profile dialog appears.

The image shows a Windows-style dialog box titled "Add Access Profile". It contains a label "Enter the access profile information:" followed by four text input fields: "Symbolic ID:", "Access Profile ID:", "Access Password:", and "Confirm Password:". To the right of the input fields are two buttons: "OK" and "Cancel".

Add Access Profile Dialog

This dialog prompts you for the Symbolic ID, name, and password of the new Access Profile.

3. Enter a Symbolic ID.

The Symbolic ID is used as the key to retrieve the encrypted ACCESSID and ACCESSPSWD from PSACCESSPRFL.

4. Enter an Access Profile ID.

This ID must be a valid RDBMS ID with system administrator privileges.

5. Enter and confirm a password.

Access Password is the password string for the RDBMS ID/Access Profile ID. Confirm Password is a required field and its value must match that of Access Password.

6. Click **OK**.

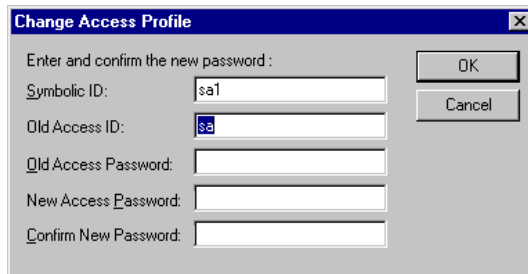
To change an Access Profile password

1. Select Tools, Miscellaneous Objects, Access Profiles.

The Access Profiles dialog appears.

2. In the **Access Profiles:** list, highlight the profile that you want to modify, and click Edit.

The Change Access Profile dialog appears.



Change Access Profile Dialog

This dialog prompts you for the old password then to type and confirm the new password for the Access Profile.

3. Enter and confirm the new a password.

The Access Password is the password string for the ID. Confirm Password is a required field and its value must match that of Access Password.

4. Click **OK**.

To delete an Access Profile

1. Select Tools, Miscellaneous Objects, Access Profiles.

The Access Profiles dialog appears.

2. Highlight the Access Profile that you want to remove, and click Delete.

You are prompted to confirm the deletion.

Click **Yes** at the prompt dialog if you want to delete the selected access profile.

---

## Transferring Users between Databases

In most cases, there will be situations where you need to copy security information from one database to another. Typically, you'd want to do this as part of an upgrade or to transfer security information from your production environment to your development or testing environment. To do this, PeopleTools provides a set of Data Mover (DMS) scripts designed to export and import your security information. The provided scripts transfer user profiles from a source to a target database.



Application Designer's upgrade feature offers upgrade support for both Roles and permission lists.

---

There is one script to export User Profile data from the *source* database. The source database refers to the database that contains the User Profiles that you want to migrate. The target database refers to the database to which you are copying the user information.

After exporting the security information from the source database, you then run the import script against the *target* database. The target database refers to the database to which you want to transfer the security data. The scripts involved in transferring security information from one database to another appear in the following list:

- **USEREXPORT.DMS.** Exports User Profiles from the source database and stores them in a Data Mover DAT file. The output file is named USEREXPORT.DAT.
- **USERIMPORT.DMS.** Reads the file created by USEREXPORT.DMS and copies the User Profile data into the target database.

You will find this set of scripts in PS\_HOME\scripts.

This section describes the procedure for running these scripts, and it outlines what needs to be in place prior to running the scripts. It also presents some items to consider prior to running the scripts.

## Considerations

Prior to running the scripts to export and import your security information, you should read the following sections to avoid any potential problems.

### *Duplicate Rows*

If the target database already contains a row of data with identical keys to a row transferred by the import script, the duplicate row *will not* be transferred to the target. The scripts make no attempt to merge the duplicate row; the row is simply not transferred.

To ensure that you don't have data rows with duplicate keys, you need to make sure that there's not a User Profile in the source database with the same name in the target database.

You should not have data rows with duplicate keys in your source and target database when you begin the copy as this can lead to unexpected results which compromise database integrity.

### *Release Levels*

Because the PeopleTools table structures change between major releases (6.X to 7.X or 7.X to 8.X), you can't transfer users between databases that run different versions of PeopleTools. Before starting the migration process, upgrade your source and target database so the release levels match.

## Running the Scripts

Complete the following procedure to run the user transfer scripts.

To run the scripts

1. Using Data Mover, sign on to the source database and run USEREXPORT.DMS for user definitions.

You can edit this script to specify the location and file name of the output file and the log file.

2. Using Data Mover, sign on to the target database and run USERIMPORT.DMS for user definitions.

You can edit the script to specify the location and file name of the input file and the log file. The name and location of the input file must match the output file you specified in step 2.

3. After copying user and role definitions, it is recommended that you run the PeopleTools audits, such as DDDAUDIT and SYSAUDIT to check the consistency of your database.



## CHAPTER 6

# Object Security

In your development environment, you may not want all developers to have access to every single definition in your database. This is why PeopleTools provides Object Security.

Just as you use Maintain Security to control who can access the various PeopleSoft pages in your system, you use Object Security to control who can access and update the PeopleTools objects. By PeopleTools objects, we are referring to the record definitions, menu definitions, page definitions, and so forth that make up your applications.

In this chapter you'll learn how to use Object Security to restrict the PeopleTools objects that your site's developers can access.

## Understanding Object Security

By controlling page access, Maintain Security dictates which applications and PeopleTools each PeopleSoft user is authorized to use. Object Security enables you to impose similar restrictions on your development staff.

There are only two tasks involved with Object Security: creating Object Groups and linking them to predefined Permission Lists. Object Security leverages the Permission Lists created in Maintain Security to restrict access to individual PeopleTools database objects, which are entities created using a PeopleTools designer utility, such as Application Designer or Tree Manager.

Object types include all of the definitions that appear in the following list. You'll see that most object types are created in Application Designer.

<b><i>Object Type</i></b>	<b><i>Associated Designer Tool</i></b>
Activities	Application Designer
Application Engine Programs	Application Designer
Approval Rule Sets	Application Designer
Business Interlinks	Application Designer
Business Processes	Application Designer
Components	Application Designer
Component Interfaces	Application Designer
Fields	Application Designer

<b>Object Type</b>	<b>Associated Designer Tool</b>
File Layouts	Application Designer
HTML	Application Designer
Images	Application Designer
Import Definitions	Import Manager
Menus	Application Designer
Message Channels	Application Designer
Messages	Application Designer
Message Nodes	Application Designer
Pages	Application Designer
Projects	Application Designer
Queries	PS Query
Records	Application Designer
SQL	Application Designer
Style Sheets	Application Designer
Tree Structures	Tree Manager
Trees	Tree Manager
Translate (X-lat) Tables	Application Designer



You can restrict access to an *entire* object type, such as records or pages, using the Use, Permission Lists, PeopleTools page in Maintain Security. This works by controlling access to the Application Designer functionality that handles a particular object type. For instance, if you don't want a developer to touch Application Engine programs, don't allow them to access Application Engine.

Object Security settings also works at the field level. To change a field on a record, you must be authorized to update *all* record definitions that contain the field. For example, to update or rename the EMPLID field on any record definition, you must have Object Security access to every record definition that contains EMPLID. If you are denied access to the ABSENCE\_HIST record definition, which contains EMPLID, you won't be able to modify any field attributes of EMPLID on any other record that contains the field. This ensures the integrity of your system. In a fast paced development environment, if PeopleTools objects are not well secured, chaos arrives shortly.

Before you start using Object Security, it's a good idea to define the object security needs of your users. For example, should all developers have access to all PeopleTools objects? Should payroll developers have access only to payroll objects? Who will be allowed to access the Application Designer? These are the types of questions you need to consider.

The following topics describe the fundamentals of Object Security.

---

## Object Groups and Permission Lists

You use Object Security to define Object Groups and link them to Permission Lists that you created in Maintain Security. This means that in order to link an Object Group to a Permission List, you must have already created the Permission List in Maintain Security.

An Object Group is a collection of one or more objects that form a logical group for security purposes. For example, let's say you've created a Permission List for analysts that support the PeopleSoft Payroll module. Perhaps this Permission List is called PAYROLL\_DEV. Assume these analysts are allowed to update only payroll objects. Using Object Security, you would create an Object Group containing only payroll objects, give it a name, such as PAYROLL\_OBJ. Then you assign, or link, that Object Group to the corresponding Permission List. In this case you link PAYROLL\_OBJ to PAYROLL\_DEV.

You can assign multiple Object Groups to a single Permission List, and, in most cases, you'll perform this frequently.

You apply Object Security to Object Groups only. For example, you can't declare directly that a particular Permission List can modify a specific object type. However, you can do so "indirectly" by creating an Object Group that consists solely of the desired object type. Also, keep in mind that you can assign an object to multiple groups as needed. To ensure total object security, we recommend that you assign every object to at least one Object Group.



Your PeopleTools databases are delivered with a pre-defined object group called PEOPLETOOLS that contains all the PeopleTools objects. Until you create object groups of your own, the PEOPLETOOLS objects are the only objects that you can secure.

---



---

## Object Security Rules

To set up Object Security properly, it's helpful to understand how the system interprets object security settings. The system has several rules it uses to determine whether a user is authorized to update an object.

The following table presents the rules associated with Object Security.

Rule	Description
1	Is the object type assigned to <i>any</i> Object Group? If not, then <i>anyone</i> has update access to it; access is automatically granted. As stated previously, for this reason we recommend that you have all object types added to at least one Object Group.
2	Is the object type a part of an Object Group assigned to the user's Permission List(s)? If not, the system denies access and displays a message, such as:  <i>&lt;object_name&gt; is not an object that you are authorized to access.</i>

3	<p>Do all of the Object Groups of which the object type is a member have the display-only option enabled? If so, then the system displays the message:</p> <p><code>&lt;object_name&gt; is not an object that you are authorized to update</code></p> <p>The object type would then appear, but with the <b>File, Save</b> option would be disabled.</p>
---	--

If the object passes these system checks, the user is allowed to access and update it—unless it's an Application Designer object, in which case several other security checks are performed first. Application Designer objects are also controlled by the **Application Designer Access** dialog in Maintain Security.



**Important!** It's important to understand that a user gets their object security permissions from their Primary Permission List, not through roles.

## The Object Security Interface

You open Object Security by selecting **Go, PeopleTools, Object Security**. When you first open Object Security, the window is empty.

The following topics describe the menu options specific to Object Security. As you define Object Groups, you'll rely on the options in the following menus:

- File
- Change
- View

We suggest that you review the options on each menu so that it's easier to navigate through the interface as you grant access to your development objects. As you become more familiar with the tool, you'll refer to this section less frequently.

### File Menu

You use the **File** menu to open or create groups of objects that you will use to grant access to permission lists, as well as different options for saving, renaming, or deleting object groups. Print commands for object security profiles are also located in this menu.

The following table presents each menu option with a brief description of its purpose.

<i><b>Menu Option</b></i>	<i><b>Description</b></i>
Open	Allows you to open a predefined Permission List or Object Group.
New Group	Select this option when creating a new Object Group.

Save	Allows you to save any changes made to an Object Group or links made to Permission Lists.
Save As	This option is only available when you have an Object Group open. It enables you to save an Object Group under a new name, or clone it.
Rename	This option is only available when you have an Object Group open. It allows you to specify a new Group ID.
Delete	This option is only available when you have an Object Group open. It allows you to delete a previously created Object Group.
Print	If you want to print an Object Group for better viewing or to share with colleagues, use this option. It invokes the <b>Print Object Security Group</b> dialog.
Printer Setup	To specify a particular printer, page size, and so forth, use this option. It invokes the standard <b>Print Setup</b> dialog.

---

## Change Menu

If you want to grant display-only access to an Object Group, use the **Change** menu.

The following table presents the menu option with a brief description of its purpose.

<i>Menu Option</i>	<i>Description</i>
Display Only	This option is only available when you have a Permission List open in Object Security. It allows you to specify whether or not the Object Groups linked to the Permission List are Display Only.

---

## View Menu

Use the **View** menu to review all of the different types of objects—menu definitions, query definitions and so forth—in an Object Group. The view menu shows every type of definition object to which you can apply Object Security settings.

The view menu is useful when you have an Object Group open. You have two options. You can view all the objects currently added to the Object Group by selecting **View, All Objects**. Or you can opt to view just the objects of a specific object type by selecting **View, <Object Type>**. For example, if you wanted to view only the different Pages that are included in the active Object Group, you would select **View, Pages**.

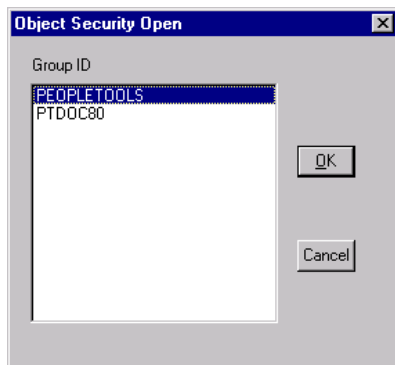
## Working with Object Groups

After reading this section you will be familiar with the fundamental procedures that you'll complete as you create Object Groups.

To open an existing object group

1. Select File, Open, Group.

The **Object Security Open** dialog appears.



Object Security Open (Group) Dialog

You use this dialog to select an Object Group to open.

2. Choose a **Group ID** and click **OK**.

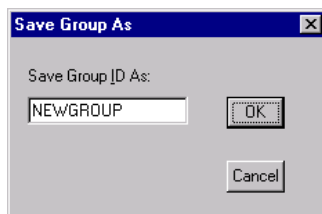
To create a new object group

1. Select File, New Group.
2. Add object to the group.
3. Save the group and give it a name in the Save Group As dialog.

To save an object group as a new group

1. Select File, Save As.

The **Save Group As** dialog appears.



Save Group As Dialog

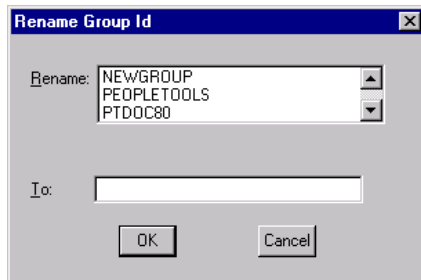
This dialog prompts you to enter a Group ID for the new group that will be created.

2. Enter an ID and click **OK**.

To rename an object group

1. Select File, Rename.

The **Rename Group ID** dialog appears:



Rename Group Id Dialog

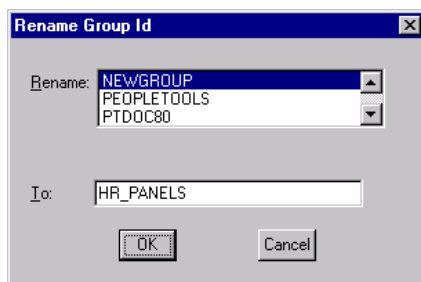
If, after creating an Object Group, you decide it needs a different name, you use this dialog to change it.

2. Select a group from the **Rename** list.



Selecting a Group ID to rename

3. Enter a new Group ID in the **To** edit box.



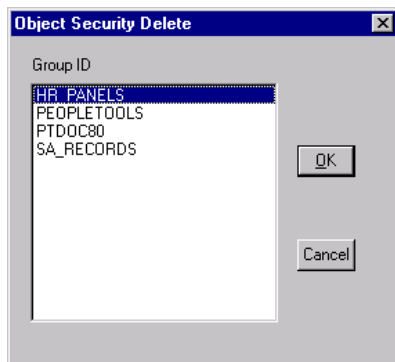
Adding a new Group ID

4. After you've added the new Group ID click **OK**.

To delete an object group

1. Select File, Delete.

The **Object Security Delete** dialog appears:



Object Security Delete Dialog

Occasionally, an Object Group may become obsolete—to the point where it's easier to start a new group from scratch than to redefine the old one. You use this dialog to select and delete unwanted Object Groups.

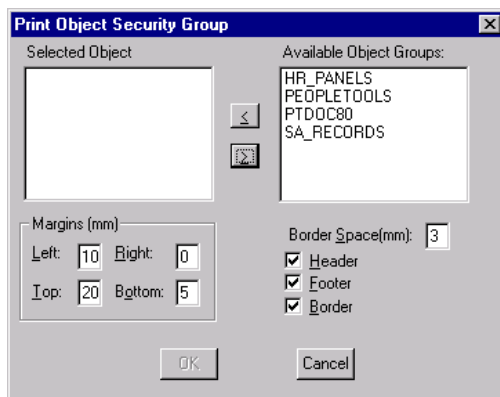
2. Select a **Group ID** and click **OK**.

You will be prompted to confirm the deletion. If you don't want to delete the Object Group don't confirm the delete.

To print an object group definition

1. Select File, Print.

The **Print Object Security Group** dialog appears.



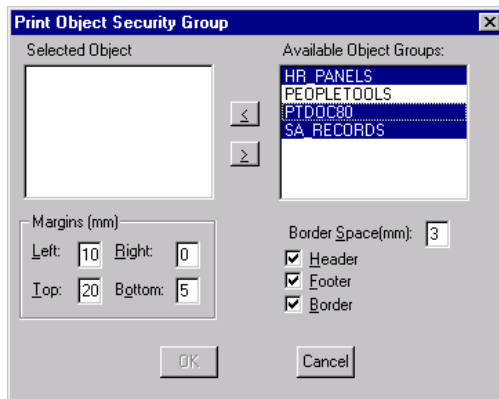
Print Object Security Group Dialog



In this dialog, you select which group definitions you want to print and setup the display options.

2. Select the Object Groups you want to print.

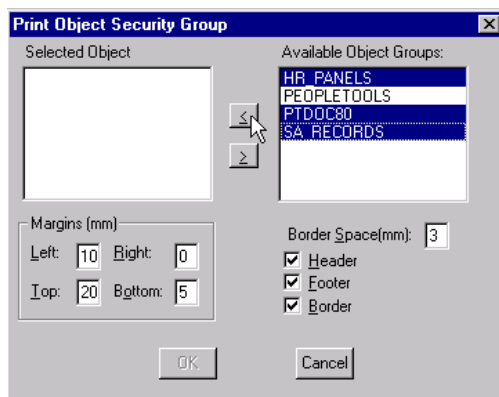
From the list of **Available Object Groups**, select the group(s) to be printed. To select multiple profiles, use Ctrl+click and Shift+click.



Selecting Object Groups to Print

3. Add the groups to the **Selected Objects** box.

To move selected profiles into the box, click the left arrow button. To remove profiles from the box, select them and click the right arrow button. You must select at least one object group in order to print.



Adding Object Groups to the Selected Object List

4. Choose the desired **Margins** and **Border Space** options and click **OK**.

## Viewing Object Groups

You can view an Object Group in one of two ways: with all the objects it includes or with only a single object type displayed. How the Object Group appears depends on the selections you make in the View menu or the drop-down list that appears at the top of the interface.

---

### Selecting a View

You can select how you will view an Object Group by using the View menu, or by selecting an item from the drop-down list that appears at the top of the interface when you have an Object Group open.

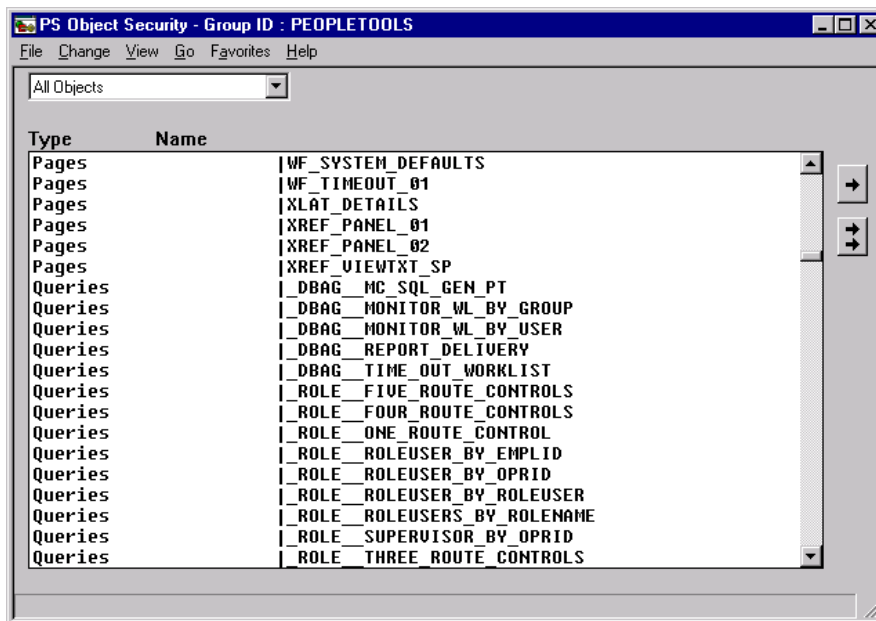
Both methods are identical, and it's up to personal preference to decide which you use.

---

### Viewing All Objects

Rather than looking at particular objects of a particular object type, there are times when you need to get an overview of just what you've added. Viewing by only one object type, obviously, only shows you a fraction of the picture. To see the entire Object Group, view by *All Objects*.

The following example illustrates the PEOPLETOOLS group viewed with *All Objects* displayed.



Viewing an Object Group by *All Objects*

This list box contains every object, regardless of type, assigned to the PEOPLETOOLS Object Group. There are two columns in this display: **Type** and **Name**.

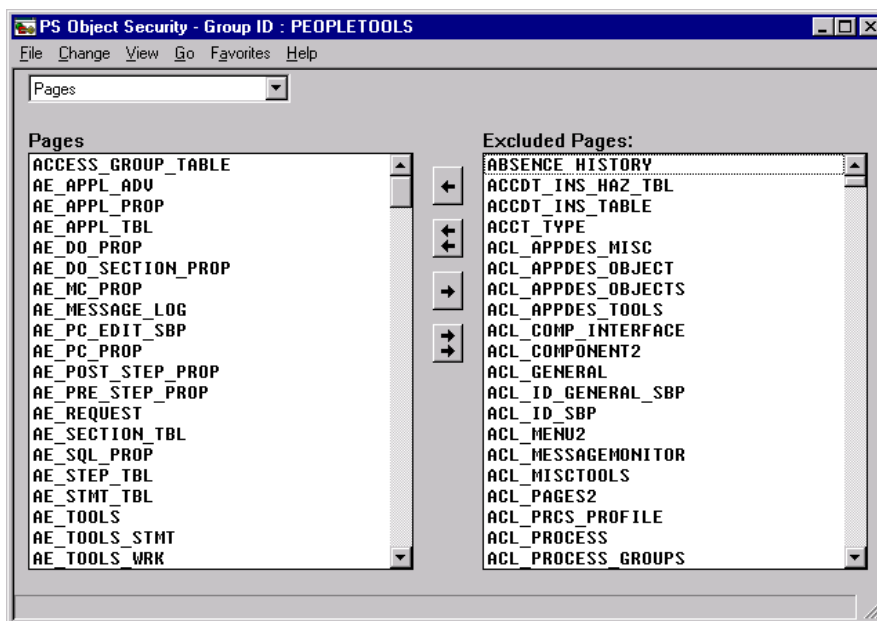
- **Type.** Identifies the object type, as in page, query, and so on.

- **Name.** Shows is the name given to the object when it was created.

## Viewing Objects of a Specific Object Type

Just as there are times when you'll need to observe the entire Object Group and all of its included objects, there are other times when you'll just want to view objects of a particular type that belong to an Object Group. Suppose you just want to view the pages that belong to an Object Group. Instead of selecting **View, All Objects**, you would select **View, Pages**. This allows you to drill down to just the information you currently need.

When you view a group one object at a time, pages in this example, the display looks like this.



Viewing One Object Type (Pages) at a Time

The window is now split vertically into two list boxes. The box on the left contains a list of objects that belong to the Object Group and are of the selected type, pages in this case.

The list box on the right is the **Excluded <Object Type>** list. The label for the object type changes according to the object type you are viewing—when you view pages, the label is **Excluded Pages**, and when you view menus the label reads **Excluded Menus**, and so on. The Excluded <Object Type> list box displays the names of all the objects of the selected type that are not included in the current Object Group.

## Defining Object Groups

Before you can specify the object access for your Permission Lists, you have to create your Object Groups. If an object doesn't belong to a group, it can't be secured.

You can create a new object group in two ways:

- If the Object Group you want to create is similar to an existing group, you can copy, or clone, the existing group and go from there.
- If the Object Group will be unlike any existing groups, or if there are no existing groups, create the new group from scratch.





For each object type in your system, you choose which objects to add or remove from the group until you're satisfied the group contains the necessary object access.

---

## Adding and Removing Objects

To add object types to an Object Group, you may not view by All Objects; you'll need to view by the type of object that you want to add. If you wanted to add pages to an Object Group, select View, Pages.

You use the arrow buttons that appear between the two list boxes (<Object Type> to <Excluded Object Type> and to move objects into and out of an Object Group. The following table describes the purpose of each button.

<b>Button</b>	<b>Description</b>
	The single left arrow moves a selected object or objects from the <b>Excluded...</b> box into the left box, adding it to the group.
	The double left arrow button adds all excluded objects into the group.
	Conversely, the single right arrow button moves a selected object from the group into the <b>Excluded...</b> box, removing it from the group.
	The double right arrow button removes all objects from the group.



You'll see two arrow buttons in the All Objects view. These are for removing any unwanted objects from the Object Group. You can only use these buttons to remove objects from the group; you can't add new objects while viewing by All Objects.

---

To add objects to an Object Group

1. Open the Object Group you want to modify.

Select **File, Open, Group**, and select the appropriate Object Group from the **Object Security Open** dialog.

2. Select the desired object type by which to view.

Use the **View** menu or the drop-down list at the top of the interface.

3. Select the objects to be added.

In the **Excluded <Object Type>** list box, select the object(s) you want to add to the active Object Group. To select multiple objects, use CTRL+click and Shift+click. If you want to add all of the items in the **Excluded <Object Type>** list, go to the following step.

4. Click one of the left arrow buttons to move the objects into the group.

To move just the selected objects, use the single left arrow. To move all excluded objects into the group, use the double left arrow.

To remove objects from an Object Group

1. Open the Object Group you want to modify.

Select **File, Open, Group**, and select the appropriate Object Group from the **Object Security Open** dialog.

2. Select the desired object type by which to view.

Use the **View** menu or the drop-down list at the top of the interface.

3. Select the object(s) to be removed in the list box on the left.

To select multiple objects, use CTRL+click.

4. Click one of the right arrow buttons to move the objects out of the group.

To move just the selected objects, use the single right arrow. To remove all objects from the group, use the double right arrow.

## Assigning Object Groups to Permission Lists

After you define your Object Groups, you implement object security by assigning them to Permission Lists that you've already created in Maintain Security. So to link an Object Group to a Permission List, that Permission List must already exist.

This section covers the procedures and concepts involved with linking your Object Groups with your Maintain Security Permission Lists.



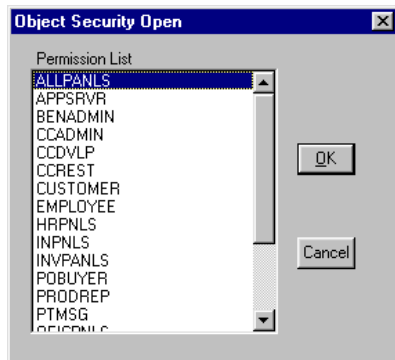
For more information on creating Permission Lists, see Working with Permission Lists.

---

To link Object Groups to a Permission List

1. Select File, Open, Permission List.

The **Object Security Open** dialog appears.

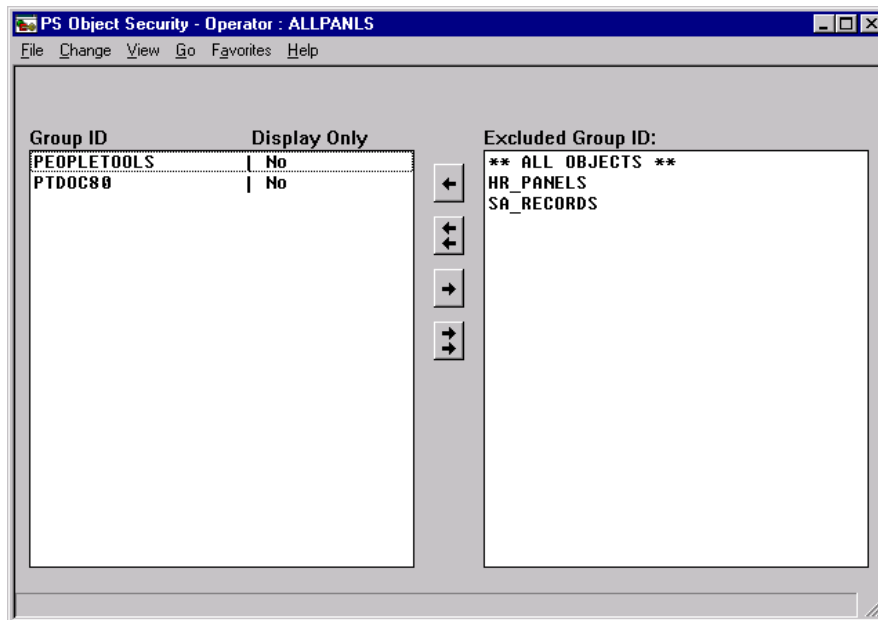


Object Security Open Dialog

You use this dialog to select the Permission List to which you want to link Object Groups.

2. Select a permission list and click **OK**.

The window displays two list boxes.



Viewing Group ID Assignments

When working with security profiles in Object Security, the display looks similar to the single-type view you see when adding objects to an Object Group. The arrow buttons in this display work the same way as in the left buttons move selections into the left box, the right buttons move selections in the right box.

Instead of moving *objects* into and out of the box on the left—as you do when defining an Object Group—here, you move Group IDs. The Group ID is the ID, or name, that you

specified when saving an Object Group. The list box on the right shows the existing Object Groups that are not currently linked to the active Permission List. The list box on the left shows the Group IDs that the Permission List is currently authorized to access.

### 3. Specify the included and excluded groups.

To enable access to an Object Group, select it in the **Excluded Group ID** list box on the right and move it into the list box on the left. To restrict access to a group, select it on the left and move it into the **Excluded Group ID** list box on the right. To move just the selected groups, use the single arrows. To move all groups, use the double left arrows.



The **\*\*ALL OBJECTS\*\*** group is a default “super group,” maintained by the system, that includes all system objects. You can use it to grant total unrestricted access to all database. On the other hand, restricting access to **\*\*ALL OBJECTS\*\*** has no security effect. To be able to restrict access to an object, it must belong to at least one object group.

---

### 4. Enable/disable the **Display Only** mode for included groups, as desired.

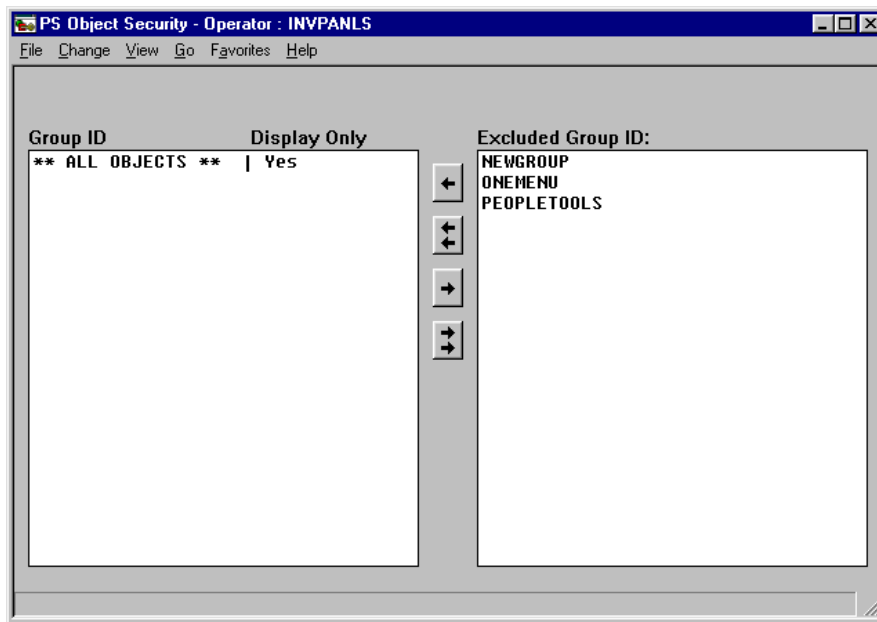
### 5. Select **File, Save** to save your changes.

## Display Only Mode

Enabling display-only access to an Object Group means the objects in that group can be viewed but not modified. You can toggle it off and on for Object Groups that you have linked to a particular Permission List. You need to add the Object ID to the linked list first before you specify a Display Only value.

The Display Only option for the **\*\*ALL OBJECTS\*\*** super group doesn’t work the same way it does for regular Object Groups. When you enable the Display Only mode for **\*\*ALL OBJECTS\*\***, it applies only to the Object Groups in the **Excluded Group ID** list.

The following example shows a Permission List (INVPANLS) with access to all objects, or **\*\*ALL OBJECTS\*\*** status. Notice that Display Only is activated. However, it only applies to those groups in the Excluded Group ID list: the NEWGROUP, ONEMENU, and PEOPLETOOLS groups. To translate, this means that INVPANLS Permission List has read/write access to *all* objects in the system except for those that appear in the **Excluded Group ID** list. For those objects, INVPANLS only has read, or Display Only, access.

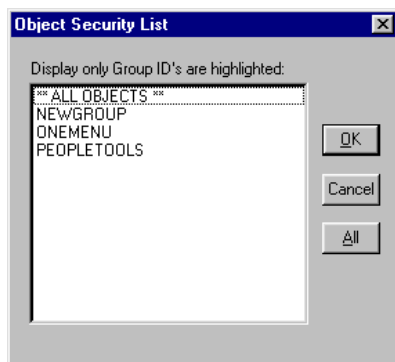


Applying Display Only Access to **\*\*ALL OBJECTS\*\***

To enable/disable Display Only

1. Select Change, Display Only.

The **Object Security List** dialog appears.



Object Security List Dialog

This dialog lists all the Object Groups assigned to the current Permission List and allows you to specify the Object Groups that should provide display-only access. Object Groups with a **Display Only** setting of *Yes* are highlighted, and Object Groups with a **Display Only** setting of *No* are not.

2. Select (highlight) the groups in the list that you want to make display-only; deselect those that should not be display-only.

You can use the **All** button to select all the groups in the list.



3. After you have selected and deselected the appropriate Object Groups, click **OK**.



## CHAPTER 7

# Security Configuration Alternatives

The PeopleSoft security system provides ample flexibility so that you can integrate with other security utilities, such as an LDAP directory server, that may be in use at your site. A PeopleSoft integration technology such as business interlinks and component interfaces enable you to exchange information with practically any system, and you can use them to integrate your security implementation.

The following topics describe using Signon PeopleCode, LDAP directory servers, and security user exits.

## Integrating with an LDAP Directory

PeopleSoft delivers three technologies that you use for authentication against an LDAP V3 compliant directory server and reuse your existing user profiles stored within LDAP. The three technologies are:

- Directory Business Interlink
- User Profile Component Interface
- Signon PeopleCode

The Directory Business Interlink exposes the Lightweight Directory Access Protocol (LDAP) to PeopleCode. The system uses it for all communication with the LDAP server process running on a directory server.

The User Profile Component Interface exposes the User Profile Component to PeopleCode. The system uses it to programmatically manage a local cache of User Profiles.

Signon PeopleCode is PeopleCode that executes when a user signs on to the system—similar to the login scripting of most network systems. Signon PeopleCode uses the Directory Business Interlink and the User Profile Component Interface to verify directory-based credentials and programmatically create a local User Profiles cache.

The combination of these three technologies provides a flexible way to configure PeopleSoft for integration with your directory server. No set schema is required in the directory. Instead, you are free to customize and extend the Signon PeopleCode to work with any schema implemented in your directory server.

The following topics are related to setting up the LDAP integration technology on your site. These tasks assume that there is already an LDAP V3 compliant directory service installed, and that you are intending to import LDAP group values and apply them to PeopleSoft roles. These

topics also assume that you are familiar with the Maintain Security interface, especially the pages related to configuring LDAP.

The sections are arranged in the order that you should perform each task when configuring LDAP integration. Many of the components and pages are also documented within the Maintain Security documentation.



When you enable LDAP Authentication the password column on the PSOPRDEFN record is no longer used. Also, LDAP Authentication requires an application server; it does not work for two-tier signon.

## Testing LDAP Connectivity

Before configuring PeopleSoft for LDAP Authentication you must verify that your Directory Server properly responds to LDAP client requests. Both Internet Explorer 5 and Netscape 4.7 have built-in LDAP clients that you can use for testing LDAP connectivity.

To establish an LDAP connection from a browser use the LDAP protocol specifier `ldap://` when entering the URL. For example, the syntax of an LDAP URL is as follows:

```
ldap://<hostname>:<ldap_port>/<base_dn>?<attributes>?<scope>?<filter>
```

The following table describes the components of an LDAP URL:

Component	Description
<hostname>	Name (or IP address in dotted format) of the LDAP server. For example, <code>ldap.peoplesoft.com</code> or <code>192.202.185.90</code> .
<port>	Port number of the LDAP server, as in, 696). If no port is specified, the standard LDAP port (389) or LDAPS port (636) is used.
<base_dn>	Distinguished name (DN) of an entry in the directory. This DN identifies the entry that is starting point of the search. If this component is empty, the search starts at the root of the directory tree.
<attributes>	The attributes to be returned. To specify more than one attribute, use commas to delimit the attributes (for example, "cn,mail,telephoneNumber"). If no attributes are specified in the URL, all attributes are returned.
<scope>	The scope of the search, which can be one of these values:  <i>base</i> retrieves information only about the distinguished name (<base_dn>) specified in the URL.  <i>one</i> retrieves information about entries one level below the distinguished name (<base_dn>) specified in the URL. The base entry is not included in this scope.  <i>sub</i> retrieves information about entries at all levels below the

	distinguished name (<base_dn>) specified in the URL. The base entry is included in this scope. If no scope is specified, the server performs a base search.
<filter>	Search filter to apply to entries within the specified scope of the search. If no filter is specified, the server uses the filter (objectClass=*).



**Note.** The components <attributes>, <scope>, and <filter> are identified by their positions in the URL. If you do not want to specify any attributes, you still need to include the question marks delimiting that field.

## Enabling Signon PeopleCode for LDAP Authentication

LDAP Authentication runs as Signon PeopleCode that must be enabled and configured to execute with proper permissions.

You don't need to select the Enabled checkbox to enable the Signon PeopleCode. When you elect to use directory authentication on the Setup, Directory Authentication page, the system automatically enables the Signon PeopleCode for LDAP authentication.

Home > PeopleTools > Utilities > Use > Signon PeopleCode

☐ Invoke as user signing in  
☒ Invoke as User ID:  Password:

*Sequence	Enabled	*Record	*Field Name	Event Name	Function Name	Exec Auth Fail	
1	<input type="checkbox"/>	FUNCLIB_PWL	PWDCNTL	FieldDefault	PASSWORD_CONTROLS	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/>
2	<input checked="" type="checkbox"/>	FUNCLIB_LDAP	LDAPAUTH	FieldDefault	LDAP_AUTHENTICATION	<input checked="" type="checkbox"/>	<input type="button" value="+"/> <input type="button" value="-"/>

PeopleTools, Utilities, Use, Signon PeopleCode

To enable Signon PeopleCode

1. Select PeopleTools, Utilities, Use, Signon PeopleCode.
2. On the Signon PeopleCode page, click the **Invoke As** radio button that applies to your configuration.

Do you want to use a default user ID, or do you want the Signon PeopleCode to be invoked by whoever the user ID is that happens to be signing on the system. Either way, the value for the User ID and the password must be a valid PeopleSoft User ID and password. For LDAP authentication, you need to use “Invoke As” because the user signing in (most likely) won’t exist in the local system, until Signon PeopleCode runs and updates the local cache of user profiles.



The User ID entered—whether it is Invoke as user signing in or a default user—must be able to access the User Profile Component in a permission list.

---

3. Locate the row for the LDAP\_Authentication function on the Record FUNCLIB\_LDAP.
4. Check the **Enabled** checkbox (if it is not already checked automatically by the system).
5. Check the **Exec Auth Fail** checkbox is checked.

This refers to if PeopleSoft authorization fails, then execute the Signon PeopleCode. PeopleSoft authorization always fails if you are using LDAP authentication.

6. Click **Save** at the bottom of the page.
7. Reboot any application servers running against the local database.

---

## Configuring Directory Authentication

The Directory Authentication component enables you to turn on directory authentication and configure PeopleSoft for your directory server, DIT, and schema.

It also enables you to configure how the system creates a User Profile in the cache of user profiles at signon time. Prior to using Directory Authentication you must configure the Mandatory User Properties page to specify how mandatory properties of the User Profile are populated.

### Setting up the Directory

This section describes the steps required for setting up the directory connect information.

Home > PeopleTools > Maintain Security > Setup > Directory Authentication

Directory Setup Mandatory User Properties Optional User Properties

### Directory Information

☒ Use Directory Authentication

#### Directory Connect Information

Server name:

Port:

User DN:

Password:

#### User Search Information

Scope

☒ SUB ☐ ONE ☐ BASE

Search Base:

Search Attribute:

[Directory Setup](#) | [Mandatory User Properties](#) | [Optional User Properties](#)

To configure Directory Authentication

1. Navigate to Maintain Security, Setup, Directory Authentication.
2. Choose the appropriate settings on the **Directory Setup** tab:
  - **Use Directory Authentication:** Check this box to enable directory-based authentication into PeopleSoft. (Note: This checkbox also toggles the Enabled checkbox for the LDAP\_Authentication row on the Signon PeopleCode page).
  - **Server name:** Name (or IP address in dotted format) of the LDAP server (for example, ldap.peoplesoft.com or 192.202.185.90).
  - **Port:** Port number of the LDAP server. The standard LDAP port is 389.
  - **User DN:** The Distinguished Name of directory based account with “Browse” rights to ObjectClass=Person entries and “Read” rights to the needed attributes.
  - **Password:** The password for directory-based account specified in User DN.
  - **Scope:** The scope of the search, which can be one of these values:
    - **base** retrieves information only about the distinguished name (<base\_dn>) specified in the URL.
    - **one** retrieves information about entries one level below the distinguished name (<base\_dn>) specified in the URL. The base entry is not included in this scope.
    - **sub** retrieves information about entries at all levels below the distinguished name (<base\_dn>) specified in the URL. The base entry is included in this scope. If no scope is specified, the server performs a base search.
  - **Search Base:** Distinguished name (DN) of an entry in the directory. This DN identifies the entry that is starting point of the search.

- **Search Attribute:** Attribute of ObjectClass=Person to which the provided User ID should be matched.

## Specifying User Properties

After you enable directory authentication and specify the connect information, you need to specify mandatory and optional user properties.

- **Symbolic ID:** A valid symbolic ID for your database.

Home > PeopleTools > Maintain Security > Setup > Directory Authentication

Directory Setup Mandatory User Properties Optional User Properties

### Directory User Attribute

\*User ID Attribute:

---

\*Symbolic Id:

\*Role Name:

**ID Type**

\*ID Type:  Employee

\*ID Type Attribute:

**Language**

☒ Use Default Language Code      Language Code:

LangCD Attribute:

Save   Previous tab   Next tab

[Directory Setup](#) | [Mandatory User Properties](#) | [Optional User Properties](#)

### User Properties

To set user properties

#### 1. Choose the appropriate settings for the **Mandatory User Properties**

- **User ID Attribute:** The name of the LDAP attribute containing the value that should be used as the PeopleSoft UserID.
- **Role Name:** A default Role for newly created users.
- **ID Type:** A default ID Type for newly created users. In the example above, the ID Type should read Employee ID in a real world example.
- **ID Type Attribute:** The name of the LDAP attribute containing valid data for the given ID Type.
- **Use Default Language Code:** Check this box if you do not maintain language codes in the directory.



- **Language Code:** Default language code to use if not taken from the directory.
- **Language Code Attribute:** The name of the LDAP attribute containing a valid language code. The value retrieved from the attribute must be a valid PeopleSoft language code.



For customers using the Microsoft Active Directory, the UID attribute is named sAMAccountName.

---

## 2. Choose the appropriate settings for Optional User Properties.

For each of the User Profile Properties listed on the page click the checkbox if there is appropriate data stored in the directory and then enter the LDAP name of the corresponding directory attribute.

---

## Importing Directory Groups

Membership in PeopleSoft Roles can be synchronized with Directory Group membership using the Directory Group Import process and a Directory Rule for Dynamic Members.

### Configure Directory Group Import

The following procedure outlines the steps you need to complete to import directory groups into PeopleSoft.

To configure the Directory Group Import

1. Navigate to Maintain Security, Setup, Directory Group Import to open the Directory Group Import Setup.
2. Use the **Settings** tab to specify the following parameters:
  - **Server:** Name (or IP address in dotted format) of the LDAP server (for example, ldap.peoplesoft.com or 192.202.185.90).
  - **Port:** Port number of the LDAP server. The standard LDAP port is 389.
  - **User DN:** The Distinguished Name of directory based account with “Browse” rights to entries retrieved by <Filter>.
  - **Password:** The password for account specified in User DN
  - **Scope:** The scope of the search, which can be one of these values:
    - **base** retrieves information only about the distinguished name (<base\_dn>) specified in the URL.
    - **one** retrieves information about entries one level below the distinguished name (<base\_dn>) specified in the URL. The base entry is not included in this scope.

- **sub** retrieves information about entries at all levels below the distinguished name (<base\_dn>) specified in the URL. The base entry is included in this scope. If no scope is specified, the server performs a base search.
  - **Search Base:** Distinguished name (DN) of an entry in the directory. This DN identifies the entry that is starting point of the search. Scope – Scope of the search; 0 = Base, 1 = One Level, 2 = Sub Tree
  - **Filter:** Search filter to apply to entries within the specified scope of the search. For example, (objectClass=groupOfNames).
  - **Message:** The Message that takes the results of the directory search.
3. Next click the **Attributes** tab to specify how the attributes of the found directory entries will be mapped to the fields of the message.

### Run the Directory Group Import Process

Once a Directory Group Import Map has been created, run the Directory Group Import process to populate the database with names of the directory groups.

To run the Directory Group Import process

1. Choose Maintain Security, Process, Directory Group Import.
2. When prompted for the name of the Directory Group Import Map, choose the appropriate map name.
3. Click the **Run**.

---

### Assigning Imported Directory Groups to PeopleSoft Roles

To assign the imported directory groups to PeopleSoft Roles

1. Choose Maintain Security, Use, Roles.
2. Choose the Role that will be assigned the group.
3. Click the **Dynamic Members** tab.
4. Click the **Directory Rule Enabled** checkbox to enable the Assign Directory Groups link.
5. Then click Assign Directory Groups.
6. Click on the **Search** button next to the Directory Group field to display a list of valid directory group names.
7. Click the **OK** button at the bottom of the page and save the changes to the Role.

8. Repeat this task for each Role that requires a Directory Rule.

## Signon PeopleCode

Signon PeopleCode executes whenever a user signs onto PeopleSoft. The main purpose of Signon PeopleCode is to copy user profile data from a directory server to the local database whenever a user signs on. This ensures that the local database has a current copy of the user profile. Because Signon PeopleCode runs at each signon, you are not required to maintain the local copy of the user information.

Signon PeopleCode is not limited to LDAP integration. You can also use Signon PeopleCode and business interlinks to synchronize a local copy of the user profile with any data source when a user signs on. Because the signon program is written in PeopleCode, you are able to customize it any way that suits your site requirements.

The basic process flow of Signon PeopleCode is as follows:

- A user enters user ID and password on signon page.
- PeopleTools attempts to authenticate a user with the local PeopleSoft password.
- Signon PeopleCode executes. It verifies the user and password, and then updates the local cache of user profiles stored in the PeopleSoft database.

Signon PeopleCode only runs when a user is logging through PIA, the portal, or a three-tier Windows workstation.



If you are using LDAP authentication, of course the PeopleSoft authentication process is going to fail because the user Password is not stored within the PeopleSoft database. Because of this, if you are using LDAP authentication, you set your Signon PeopleCode program to execute when PeopleSoft authentication fails.

---

---

## Modifying Signon PeopleCode

Signon PeopleCode is Record PeopleCode, and you view and edit the PeopleCode on the record with which the program is associated. PeopleSoft delivers a PeopleCode program for directory authentication. It is intended for production use but it can also be used as a sample that shows many of the technologies you can include within a Signon PeopleCode program. You can find the delivered PeopleCode program on the following record: FUNCLIB\_LDAP.LDAPAUTH (FieldDefault). You are free to customize it as needed for testing or production use.

Open the record in Application Designer, and view the PeopleCode with the PeopleCode Editor. The delivered PeopleCode was written to accommodate as many different directory scenarios as possible; it demonstrates use of the business interlink and component interface technologies. You may want to modify the authentication PeopleCode to improve log in performance or to accommodate any special directory authentication needs. The delivered program that ships with PeopleTools has the following general flow:

- Searches the directory server for the user profile of the user signing in.
- Using the password the user entered at the signon page, the program attempts to bind (or connect) to the directory server. If the connect succeeds, then the password is valid.
- Retrieves the user profile of the user signing in. The program gets the profile from the directory server and creates a local cache copy within the PeopleSoft database. This improves performance by allowing the PeopleSoft applications to access the user profile locally, rather than making a call to the LDAP server every time they need user profile data. If a locally cached copy already exists for the user signing in, the local cache is updated according to the current user in the directory server.



**Tip.** To see what the Signon PeopleCode program performs, it is helpful to use the PeopleCode debugger. This enables you to step through the program step-by-step. You must debug the Signon PeopleCode program while connected to a local application server. For more information refer to the Enable Debugging parameter described in the PIA Administration PeopleBook.

The following table presents the key PeopleCode constructs that you use with Signon PeopleCode. Click the function to view more details in the PeopleCode documentation.

<b><i>PeopleCode Function</i></b>	<b><i>Description</i></b>
<code>%PSAuthResult</code>	Returns the result (boolean) of PeopleSoft authentication.
<code>SetAuthenticationResult</code>	Used to verify customers that log on to the system even if the PeopleSoft authentication fails.
<code>%SignonUserId</code>	User ID value the user entered at the Signon page. This applies to PIA and Windows signon.
<code>%SignOnUserPswd</code>	User Password value the user entered at the Signon page. This value is encrypted. This applies to PIA and Windows signon.
<code>%Request</code>	The HTML request that comes from the browser. In the case of security, this includes any information submitted at the Signon page, such as User ID, password, and any additional fields if you have extended the Signon page. This only applies to PIA.



Do not use `%SwitchUser` in Signon PeopleCode.

## Enabling Signon PeopleCode

Signon PeopleCode is different from other PeopleCode in that you specify which Signon PeopleCode you want to run from its own Signon PeopleCode page. To access the Signon PeopleCode page select **PeopleTools, Utilities, Signon PeopleCode**. Notice that the PeopleSoft Password Controls program, which is written in PeopleCode, is also on this page.

By default, both programs are disabled. You enable them on this page, or you can also enable these programs by enabling password controls on the Password Controls page or by enabling directory authentication on the Directory Authentication component. After enabling each option on the appropriate page, the system enables the associated PeopleCode program on the Signon PeopleCode page.



Using PeopleSoft password controls is only valid if you are *not* using LDAP authentication. When you are using LDAP authentication the directory server, not PeopleSoft, controls the password.

You can add your own PeopleCode programs, but you need to add them to another record, and then add them to this page. You add and remove rows from the grid using the plus and minus buttons.

<input checked="" type="radio"/> <b>Invoke as user signing in</b>						
<input type="radio"/> <b>Invoke as</b> User ID: <input type="text"/> Password: <input type="password"/>						
*Sequence	Enabled	*Record	*Field Name	Event Name	Function Name	Exec Auth Fail
1	<input type="checkbox"/>	FUNCLIB_PWL	PWDCNTL	FieldChange	Password_Controls	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	FUNCLIB_LD#	LDAPAUTH	FieldDefault	LDAP_Authentication	<input checked="" type="checkbox"/>

PeopleTools, Utilities, Signon PeopleCode

The list describes the controls on this page:

- Invoke as...** When a PeopleCode program runs, it has to have a context of a user. This is how you indicate to the system who the user is executing the program. This is important because the user ID provided needs to have access to all of the objects that your signon program uses. For instance, if you are using LDAP the signon peoplecode, you'll notice that it contains a business interlink and a component interface. If the user ID provided does not have the appropriate authority to business interlinks or component interfaces, the program fails. Whether you use the value of the user signing in or you create a default user ID for all signon attempts depends on your implementation. For example, if your signon PeopleCode creates local copies of users, you'll have to configure that program to be "Invoked as" an existing user in the system. In this case, you should create a new user within PeopleSoft that only has authority to access the objects required within your PeopleCode program. You should then enter this user as the "Invoke As" user.
- Sequence.** The sequence column shows you the sequence in which your signon programs execute. You can change the sequence by changing the numerical value in the edit box. The application server executes all programs in the ascending order in which they appear.

- **Enabled.** To enable a program to run at signon, check the **Enabled** checkbox. If it is not checked, then the system ignores the program at signon.
- **Record.** Specify the record on which you record PeopleCode exits.
- **Field Name.** Add the specific field that contains the PeopleCode.
- **Event.** Add the event that triggers a particular program.
- **Function Name.** Add the name of the function to be called.
- **Exec Auth Fail.** This column means "execute if PeopleSoft authentication fails." In other words, if PeopleSoft does not successfully authenticate the user based on the password within the PeopleSoft database, you still want the program to run. For instance, you want the LDAP authentication program to run after PeopleSoft denies access so that your program can authenticate the user instead. Also, you can leave this option unchecked to further secure your system. For instance, if you are *not* using LDAP authentication, leaving this option unchecked prevents any program or script from running if your PeopleSoft authorization fails.

---

## Permissions

Signon PeopleCode scripts run with full permissions of the User they're invoked as. This includes access to the database via SQL, access to the file system, business interlinks, component interfaces application messaging, and so on. A malicious developer could conceivably write a signon PeopleCode program that exposed or corrupted sensitive information. To minimize this risk, you should follow these guidelines:

- You should limit access to the Signon PeopleCode setup page to only trusted administrators. This will prevent people from configuring un-trusted PeopleCode programs to execute at signon time.
- If you aren't implementing external authentication at your site (all your users are authenticated based on an existing User ID and password with the PeopleSoft database, you should not have the "Exec Auth Fail" column checked for any Signon PeopleCode scripts.
- After a trusted administrator configures the list of functions that should execute at signon time, you should use Object Security to restrict access to the Record objects that contains the programs. Only trusted developers should be allowed to modify the PeopleCode on these records.
- Even for trusted developers, it is a good idea to have a second person review the code before testing and moving to production.
- No developer or Administrator should have access to the Signon PeopleCode setup page, or the Records that contain the signon PeopleCode functions in a production system.



The password the user types in at the signon page is never visible to the signon PeopleCode developer. It is impossible to write a script that captures user passwords as they type them in, and store them in a file or database table.

---

## Using Security Exits

PeopleSoft enables you to maintain security information outside of the PeopleSoft system. Many sites prefer to do this so that they can maintain all of their user information from a central location. This reduces maintenance costs and possible errors attributed to duplicated data. If you opt to maintain user information required by PeopleSoft in an external source, you can employ the following options to facilitate this implementation.



The exits described here are offered in addition to the Signon PeopleCode running on the application server, which in and of itself provides integration. With PeopleTools 8.10, there are no psuser exits on the application server; Signon PeopleCode replaces that functionality. On the client side, the functionality is the same as previous releases. PeopleSoft encourages you to use Signon PeopleCode for signon integration, but if you have a previous implementations, you can use the options described in this section.

---

### Web Server Exit

Part of the integration technology PeopleSoft delivers is to ensure that our security/authentication system is open and flexible. Because the PeopleSoft applications are now designed for internet deployment, many sites need to take advantage of the authentication services that exist at the web server level.

This section describes a procedure that enables you to configure your implementation so that PeopleTools authentication logic "trusts" the authentication performed at the web server level. The following list presents examples of some of the third party authentication technologies you may want to integrate with:

- Web single-signon/authorization/authentication solutions.
- Client-side SSL authentication provided by web servers.
- Public Key Infrastructures, either stand-alone or embedded as part of the network operating system environment.



The previous list is not a list of certified integration points; it merely shows examples of authentication technologies that exists in the industry.

For this configuration to work successfully, PeopleSoft assumes the following:

- You want to authenticate the user at the web server level only, and not within the PeopleSoft Application Server. (The configuration discussed in this section enables you to authenticate users within the web server instead of the default configuration, where the application server controls the authentication logic).
- You need to have a web server environment that includes a mechanism to identify and authenticate a user. For example, this may be through a signon page with a User ID and

password, through a digital certificate, or through one of several industry-standard authentication methods.

- Your web server has the capability of passing the user ID to the application server through the HTTP request object. For this you can use an HTTP header variable, cookie, or a form field.



Configuring the following authentication system is not an "out-of-the-box" feature. It requires development outside of the realm of PeopleSoft, and because of that, PeopleSoft assumes that you have the appropriate level of internet development expertise to make sure that you are passing the appropriate information to the PeopleSoft system. As with all security development, being extremely careful is of the utmost importance.

---

## Configuring the System

The following section outlines the steps that you need to complete in order to provide signon authentication at the web server level.

### Creating a Default User

Create a default User ID using Maintain Security.

This user ID does not require any roles or permission lists. PeopleSoft recommends creating a long and difficult-to-guess password.

For this example, we create the following user profile and password:

- **User ID.** default\_user
- **Password.** ekdJl3838\*\*&^%kdjflsdkjfJHJK

As you can see, the password is long and difficult to guess.



For more information on creating user profiles, see User Profiles.

---

## Modifying the configuration.properties File

With the default user created, you then modify the configuration.properties file to include the default user signon information.

Within the properties file, you first need to disable the PeopleSoft signon page. By default, PeopleSoft prompts an unauthenticated user for a User ID and Password with the signon page. You disable the signon page by setting the byPassSignOn parameter to a value of true.

```
byPassSignOn=true
```



If set to true, the PeopleSoft system does not display the password page to the user. Instead, the web server uses the defaultUSERID (default user ID) and defaultPWD (default password) parameters to initiate a secure session with the application server.



As you'll notice in the following discussion, the user is never actually signed on as "default\_user". The "default\_user" ID is just a temporary value used to initiate a secure connection to the application server. The application server then determines the real user ID using Signon PeopleCode. The real user ID is contained in the request object, and all the other user information, such as language code, roles, and so on, is already stored in PeopleSoft or an LDAP server.

Besides modifying the byPassSignOn parameter, you also need to set the defaultUSERID and defaultPWD parameters to the user ID created in the previous step. For example,

```
defaultUSERID=default_user
```

and

```
defaultPWD=ekdJl3838**&^%kdjflsdkjfJHJIK
```

Because you hardcode the signon values in the properties file, no end user ever needs to know them—their use is transparent.

PeopleSoft recommends limiting the access to and knowledge of the defaultUSERID and defaultPWD values. You can do this by sharing this information only with a small number of trusted security administrators. Also, you should make sure that only these select few have read access to the configuration.properties file.



The web server process needs read access to the configuration.properties file.

Even if somebody does discover the defaultUSERID and defaultPWD, they won't be able to sign on to PeopleSoft. Recall that the "default\_user" doesn't have any roles or permission lists. On the other hand, an extremely sophisticated hacker could attack the application server directly by sending it a connection request formatted in the Tuxedo/Jolt protocol and potentially assume the identity of a user. PeopleSoft recommends using network and firewall products to restrict the origin of requests sent to the application server.

## Writing a Signon PeopleCode Program

In addition to creating a default user and modifying the configuration.properties file, you also need to write a Signon PeopleCode program that performs the following:

- Uses data within the HTTP request to determine the real user ID. Your web server authentication system should be configured to insert the USERID of an authenticated user into the HTTP request as a header, a form field, or cookie.
- Creates or updates the local copy of the user profile within the PeopleSoft database.

The programs developed to perform this task will vary depending on where the web server inserted the user ID in the HTTP request and where the user profiles are stored. For example, some systems use an HTTP header to store the user ID, while others use cookies or form fields.

If the web server security product uses LDAP as a backend data store for user profiles, you can reuse some of the LDAP authentication PeopleCode to copy the profile from LDAP to the local database. The user profile may also be stored in another database, or a Windows NT domain registry. In either case, you need to write PeopleCode to retrieve the value and make a local copy.



For more information on setting up LDAP Authentication, see Integrating with an LDAP Directory.

---



You can't use the LDAP Authentication PeopleCode program as delivered. This program performs LDAP authentication and copies the user profile from an LDAP directory to the local database. You can, however, use the code that copies the profile from the directory, as a template for the code you need in this case.

---

The following is sample PeopleCode with the External\_Authentication function. It is a simple example of retrieving the user ID from a form field named "UserID".

```

/*//////////////////////////////////////
////////////////////////////////////*/

Function External_Authentication()

    /* This application server "trusts" the authentication done in the web
    server */

    /* grab the USERID from the HTTP request and pass it to
    SetAuthenticationResult */

    &UserID = %Request.GetParameter("UserID");

    SetAuthenticationResult( True, &UserID, "", False);

End-Function;

```

After you have written the program, you need to set the Signon PeopleCode program to execute only if authentication is successful. On the Signon PeopleCode page, you set the execution as follows:

Home > PeopleTools > Utilities > Use > Signon PeopleCode New Window

### Signon PeopleCode

Signon

☐ Invoke as user signing in

☒ Invoke as 

User ID:

Password:

Sequence	Enabled	Record	Field Name	Event Name	Function Name	Exec Auth Fail
1	<input checked="" type="checkbox"/>	FUNCLIB_EXTAUTH	EXTAUTH	FieldDefault	External_Authentication	<input type="checkbox"/>

PeopleTools, Utilities, Use, Signon PeopleCode



For more information on the Signon PeopleCode page, see Signon PeopleCode.

The Exec Auth Fail checkbox must *not* be checked. You want this PeopleCode to run only if the connection to the application server originates from a web server that presents a valid user ID and password. In this case, the user ID is default\_user and the associated password. You should only enable Exec Auth Fail when the PeopleCode authenticates the user itself, not when the program relies on the web server to perform authentication.

You should also set Invoke as to a user profile that has the appropriate roles and permissions to do all the operations in the External\_Authentication function. For example, if External\_Authentication creates a local copy of the user profile using the User Profile component interface, “signon\_peoplecode\_user” must have permission to use this component interface. The Signon PeopleCode program runs under the “signon\_peoplecode\_user” User ID.



Before executing the PeopleCode, the application server authenticates the defaultUSERID and defaultPWD.

### Signing on through the Web Server

This section provides step-by-step example of what occurs within the system once you have it configured to trust authentication performed at the web server level.

Step	Component	Description
1	Browser	User clicks on a link to the PeopleSoft application, as in http://serverXYZ/servlets/psportal/peoplesoft8/?cmd=start.

<b>Step</b>	<b>Component</b>	<b>Description</b>
2	Web Server	<p>The Web server receives the request for the URL, authenticates the user, and adds the User ID to the HTTP request for the resource.</p> <p>How the system authenticates the user and how the web server adds the user ID to the HTTP request depends on your implementation. For example, it could be a web security product like SiteMinder, or PKI/ digital certificate, or SSL with client-side authentication.</p>
3	Servlet	<p>The PeopleSoft servlet receives the HTTP request, which includes the user ID in a header, cookie, or form field, and connects to the application server using the defaultUSERID and defaultPWD values from configuration.properties.</p>
4	Application Server	<p>The Application server authenticates the connection from the web server by checking the defaultUSERID and defaultPWD against the values stored in PSOPRDEFN. The user ID and password must be valid in order for the connection to succeed and for Signon PeopleCode to execute.</p> <p><b>Note.</b> The password check prevents a sophisticated hacker from connecting to the application server directly and executing service requests.</p>
5	Signon PeopleCode	<p>Signon PeopleCode executes, under the context of the "signon_peoplecode_user". When Signon PeopleCode runs, it has all the permissions of this user. It grabs the "real" user ID from the HTTP request and creates a copy of the user profile in the local database (if appropriate). It also calls the PeopleCode built-in SetAuthenticationResult and passes the user ID, and "true" for AuthResult. The PeopleCode program always passes "true" for AuthResult because the application server is "trusting" the authentication logic of the web server.</p> <p>The PIA session is set to the user ID of whatever you pass into SetAuthenticationResult. For example,</p> <pre>SetAuthenticationResult( True, "TSAWYER", "", False);</pre> <p>In this case, the system sets the session to "TSAWYER". The user can access all the pages "TSAWYER" to which TSAWYER has access.</p>

---

## Windows Exits

The following sections discuss the security exits provided for the Windows environment. Most end users will access PeopleSoft using a browser, so you may not need to implement any client-side Windows exits. However, in the event that you need to provide this functionality, PeopleSoft provides the option.

### Overview

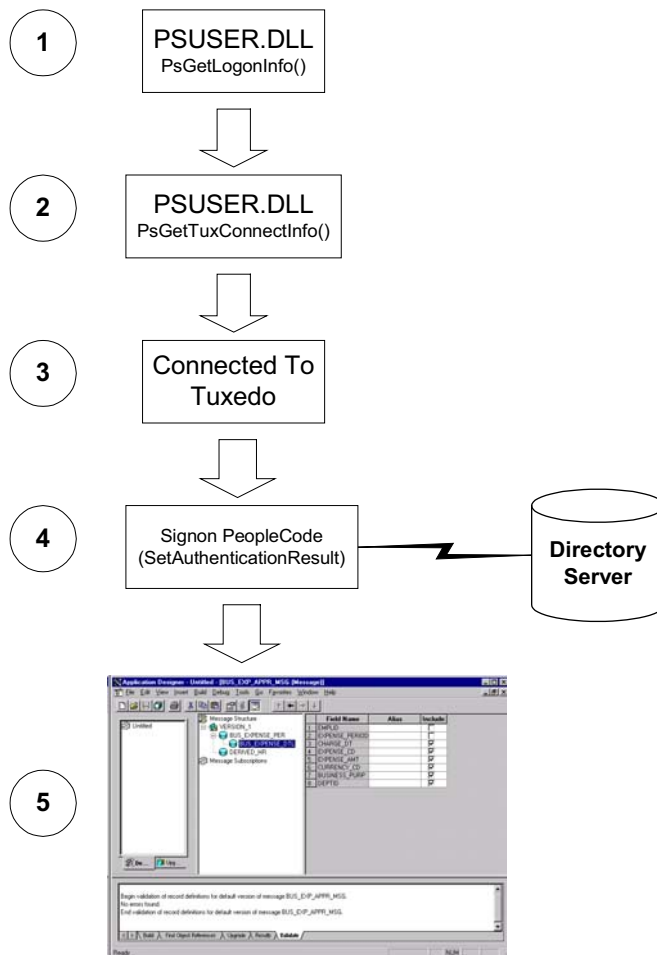
The Windows client-side exits are:

- **PsGetTuxConnectInfo()**. Used only for three-tier Windows workstations running Application Designer or Query, for instance.
- **PsGetLogonInfo()**. Used for Windows workstations in both a two-tier and three-tier environment.

You use these functions to create a customized PSUSER.DLL. These exits are used primarily for the PeopleTools Development Environment, Query users, or Tree Manager users. Unless you intend to deploy PeopleSoft applications to Windows workstations, the Windows exits are seldom used.

PsGetLogonInfo was used for the Windows Client in previous releases to fill in the signon screen programmatically without displaying it to the user.

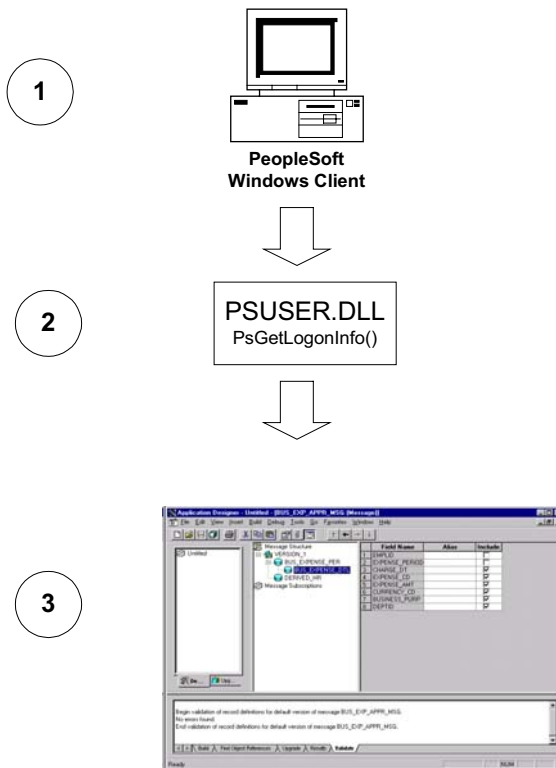
With the three-tier Windows Client signon you can also skip the PeopleSoft Signon window by modifying the PsGetLogonInfo() function as with the two-tier connection. But since you are connecting to the database through Tuxedo, there are some other authorizations that need to occur.



### Windows Client Three-Tier Signon Exits

- The PsGetLogonInfo() function must specify APPSERV as the szDBType parameter to bypass the PeopleSoft Signon window.
- To connect to the Tuxedo application server, the PsGetTuxConnectInfo() function retrieves authentication information from directory server.
- If the authentication information is valid, Tuxedo allows connection.
- Now Tuxedo needs to connect to the database server. The application server verifies the authentication information passed by the PsGetTuxConnectInfo() function.
- If the authentication is successful, the user is connected to PeopleTools.

The following example illustrates the results produced by customizing the PSUSER.DLL PsGetLogonInfo() function to bypass the PeopleSoft Signon dialog.



Two-Tier Windows Client Signon Using PsGetLogonInfo()

- From the workstation the user executes PSTOOLS.EXE. PSTOOLS.EXE calls the PSUSER.DLL.
- The PsGetLogonInfo() function supplies user signon information. If information is validated by the RDBMS, user is connected as User ID or Connect ID, and then after the security profile is retrieved and validated the user is connected as Access ID.
- If the signon information is valid, PeopleSoft connects the user to the specified PeopleTool.

## Customizing PSUSER.DLL

If your site has implemented a security system external to PeopleSoft, you can use that external system to validate your Windows Client PeopleSoft users as well. This is done through our User Exit (PSUSER.DLL), which also provides the capabilities to specify your own encryption for use in encrypting passwords.

To enable these options you'll need to modify several procedures in the PSUSER.C, and recompile to create a new PSUSER.DLL. Then you need to install the new DLL file wherever users run their PeopleSoft executables, such as PS\_HOME on the file server.

In this section, we show you the security functions that we provide and how you can tailor them for use in your own system. To successfully complete any customizations with these functions, you will need to be familiar with the C programming language.

## ***PsGetLogonInfo()***

The PsGetLogonInfo() function is always called when PeopleSoft is launched. If you're already controlling which users can access the PeopleSoft applications—through a DCE or other security solution—you may want to use this function to let those users start PeopleSoft directly without being prompted for PeopleSoft signon information. This function can also be overridden to provide information to the three-tier exit, PSGetTuxConnectInfo().

As delivered, PsGetLogonInfo() returns a FALSE value and is ignored. However, if it returns a TRUE value, the PeopleSoft signon dialog will be bypassed and the information that you've coded into the function will be used as the signon parameters.

You'll find this function in your <PS\_HOME>\SRC\PSUSER\PSUSER.C file. The code initially looks like this:

```

/*****

* Function:      PsGetLogonInfo                                *
*
*
* Description:   Sample routine to get logon information.      *
*
*
* Returns:      TRUE if logon information returned            *
*
*               FALSE to ignore                               *
*
*****/

PS_EXPORT(BOOL) PsGetLogonInfo(LPSSLGINFOP lpPsLogInfo)
{

/*----- BEGIN SAMPLE CODE -----

// ask for user input only when it is the first signon
if (!lpPsLogInfo->bSubsequentSignon)
{
    // test auto logon

    strcpy(lpPsLogInfo->szDBChange, "NO");

    strcpy(lpPsLogInfo->szDBType, "DB2");

    strcpy(lpPsLogInfo->szDBName, "C9442A");

```



```

strcpy(lpPsLogInfo->szServerLogonSec, "NO");

strcpy(lpPsLogInfo->szOprId, "C944201");

strcpy(lpPsLogInfo->szOprPswd, "C944201");

return(TRUE);

}

```

```

----- END SAMPLE CODE -----*/

```

```

return(FALSE);

```

```

}

```

To activate the automated signon feature you need to comment out the “false” return and uncomment the “true” return line. The return value is historical and ignored. The user exit bypasses the screen only if it receives enough information.

Then you will need to code the appropriate logic to fill in the values for the parameters to the PSGetLogonInfo routine. If you provide all of the appropriate field values, the system will proceed directly to your default initial window specified in the Configuration Manager’s Startup tab. Your procedure might look something like this:

```

PS_EXPORT(BOOL) PsGetLogonInfo(LPSSLGINF0 lpPsLogInfo)
{
/* test auto logon */

//strcpy(lpPsLogInfo->szDBChange, "NO");

strcpy(lpPsLogInfo->szDBType, "ORACLE");

strcpy(lpPsLogInfo->szDBName, "PSORADB");

strcpy(lpPsLogInfo->szServerLogonSec, "NO");

strcpy(lpPsLogInfo->szOprId, "MGR2");

strcpy(lpPsLogInfo->szOprPswd, "password");

return(TRUE);

//return(FALSE);
}

```



If any required signon parameters are omitted, our signon screen will appear and the missing values will default to the settings found in the registry. One way to control whether the signon dialog displays is to have PSUSER.DLL provide (or not provide) the user's password.

All parameters except bSubsequentSignon, which is Boolean, are of the data type CHAR and are defined as follows:

<b>Variable Name</b>	<b>Description</b>	<b>Values</b>
BSubsequentSignon	This is this an initial or a subsequent signon	FALSE = Initial signon. User just started PeopleSoft. TRUE = Subsequent Signon. User probably selected Go->PeopleTools from the PeopleSoft menu.
szDBChange	change database name/type	TYPE = allow to change type and name YES = allow to change name only NO = do not allow to change either
szDBType	database type	DB2 = IBM DB2 through Centura Gateway DB2ODBC = DB2 through ODBC DB2UNIX = DB2/UNIX INFORMIX = Informix MICROSFT = Microsoft SQL Server ORACLE = Oracle Server SYBASE = Sybase SQL Server APPSERV = Application Server
szDBName	database name or application server name	
szServerLogonSec	Refers to the Change Password feature.	YES = enabled NO = disabled
szOprId	User ID	
szOprPswd	User Password	

### ***PsGetTuxConnectInfo()***

When operating in three-tier mode, PsGetTuxConnectInfo() is called after PsGetLogonInfo() and just before connecting to Tuxedo. You can use this function to pass authentication data (key) to the server. This can either be used to supplement or to replace PeopleSoft's standard authentication process.

You'll find this function in your <PS\_HOME>\SRC\PSUSER\PSUSER.C file. The delivered code looks like this:

```

/*****

* Function:      PsGetTuxConnectInfo      *
*
*
* Description:   This function is called from PeopleTools just prior to *
*                connecting to Tuxedo.  The PeopleTools client sends *
*                the data in *ppData to the PeopleSoft Tuxedo *
*                authentication service (PSAUTH), where it can be used *
*                as an alternative or supplement to the default *
*                PeopleTools authentication (see PsTuxAuthExit in *
*                pssite.c). *
*
* TO DO:        Add logic to obtain client authentication information. *
*                An example might be NT or DCE signon information. *
*
* Returns:      TRUE if logon information returned *
*                FALSE to ignore *

*****/

PS_EXPORT(BOOL) PsGetTuxConnectInfo(NETEXTAUTH *pExtAuth)
{

/*----- BEGIN SAMPLE CODE -----

// set the auth information size and allocate space for auth information
pExtAuth->nLen = 25;
pExtAuth->pData = (unsigned char *) malloc(pExtAuth->nLen);

// set your authentication string

```

```

memcpy(pExtAuth->pData, "NATHAN HORNE\0\0PEOPLESOFT\0", pExtAuth->nLen);

return(TRUE);

----- END SAMPLE CODE -----*/

return(FALSE);

}

```

## Implementing a Customized PSUSER.DLL

In the following procedure, we explain how to recompile your modified source files and to implement the new version of PSUSER.DLL.

To rebuild and implement PSUSER.DLL

### 1. Compile PSUSER.C and create PSUSER.DLL

To do this for Windows platforms, run NMAKE while in the <PS\_HOME>\SRC\PSUSER\WINX86 directory. You must use a Microsoft Visual C++ 6.x compiler.

On UNIX, run the shell script psuser.sh in pshome\src\psuser.

The resulting file, PSUSER.DLL, is used by PeopleTools (PSTOOLS.EXE), as well as the Windows COBOL interfaces. For Windows NT, you'll need to copy this file into your COBOL directory.

### 2. Distribute PSUSER.DLL to workstations

If your workstations run the PeopleSoft executables from a common file server, you'll need to ensure that your new PSUSER.DLL is copied to that file server. If any of your workstations run the PeopleSoft executables locally, PSUSER.DLL will have to be distributed to such workstations.





# Index

## A

- Access Groups
  - security 2-24
- Access ID 1-10
  - definition of 1-11
- Access Password 5-34
- Access Profile ID 5-34
- Access Profiles
  - Access Password 5-34
  - Access Profile ID 5-34
  - changing password 5-35
  - creating 5-32, 5-35
  - deleting 5-36
  - properties 5-33
  - Symbolic ID 5-34
  - working with 5-35
- Account Lockout 5-5
- Alternate User ID 4-7
- Application Data
  - security 1-4
- Application Designer
  - SQL build access 2-13
  - Tools menu access 2-14
- Application Message Monitor
  - granting access to 2-22
  - permissions 2-22
- Application Messaging
  - security 5-27
  - SSL 5-23
- Application Server
  - who can start 2-5
- Audit
  - security information 2-31
  - user profile changes 4-9
- Authentication
  - LDAP 1-15
  - options 1-15
  - PeopleSoft 1-15
- Authentication
  - configuring directory-based 7-4
  - configuring LDAP 7-4
  - directory-based 5-8, 7-4
  - enabling LDAP 5-8
  - enabling Signon PeopleCode 7-11
  - enabling Signon PeopleCode for LDAP 7-3
  - importing directory groups 5-12
  - LDAP 5-8
  - LDAP setup 7-1
  - modifying Signon PeopleCode 7-9

- user exits 7-13
- user properties 7-6
- Authorization IDs 1-10

## B

- Batch programs
  - security 2-14
- Build and Data Administration
  - security 2-13

## C

- CD-ROM
  - ordering ii
- Change Control
  - security 2-12
- Component Interfaces
  - permissions 2-21
- Connect ID
  - Definition of 1-10
- Connectivity
  - LDAP 7-2
- Currency Code 4-4

## D

- Digital Certificates 5-23
  - managing 5-25
- Directory Groups
  - assigning to roles 7-8
  - importing 7-7
- Directory Server
  - integration 1-13
- Dynamic role rules
  - role members 3-4

## E

- Email ID 4-4
- Exits
  - security user exits 7-13

## F

- Field-level security 1-5
- Form ID 4-7
- Functional security 1-2

## H

### Hints

forgotten password 5-7

## I

### Integration

security 7-1

## L

### Language Translations

security 2-13

### LDAP

- authentication 5-8
- configuring 5-8, 7-1
- connect information 5-9
- defining LDAP map 5-12
- directory information 5-8
- importing directory groups 5-12, 7-7
- importing LDAP directory groups 5-31
- integration 1-13, 7-1
- mandatory user properties 5-9
- optional user properties 5-11
- running LDAPMAP program 5-32
- search information 5-9
- testing connectivity 7-2
- user properties 7-6

### Logging on

single signon 5-16

### Logon Attempts

maximum 5-5

## M

### Maintain Security

- processes 5-30
- window 1-18

### Maintain Security

- interface 1-17
- Process menu 1-20
- Setup menu 1-19
- Use menu 1-18

### Mass Change

- security 2-29
- template permissions 2-30

### Menu

- permissions 2-6
- security 2-6

### Migrating Users

running the scripts 5-37

### My Profile 4-14

## O

### Object Groups 6-3

- adding 6-12
- adding objects to 6-11
- assigning to a class 6-13
- assigning to permission lists 6-13
- creating 6-6
- defining 6-11
- deleting 6-8
- display only 6-16
- linking to Permission Lists 6-3
- opening 6-5
- printing definitions 6-8
- removing 6-12, 6-13
- removing objects from 6-11
- renaming 6-7
- rules for 6-3
- saving as a new group 6-6
- selecting a view 6-10
- viewing 6-10
- viewing specific types 6-11
- working with 6-5

### Object Security 1-4, 6-1

- assigning object groups 6-13
- Change menu 6-5
- display only 6-15
- File menu 6-4
- interface 6-4
- object group rules 6-3
- object groups 6-3, 6-5. *See* Object Groups
- overview 6-1
- view menu 6-5
- viewing all objects 6-10
- viewing object groups 6-10
- window 6-4

### Online Security 1-2

### Options

security 1-15

## P

### Pages

security/permissions 2-6

### Password

requesting new 4-17

### Passwords

- age 5-4
- changing 4-14
- character requirements 5-6
- configuring forgotten password site 5-7
- controlling length 5-5
- controls 5-3
- creating hints 5-7
- email new password 4-17
- enabling controls 5-4



- forgotten password questions 5-6
  - forgotten password setup 4-15
  - length 5-5
  - managing 5-3
  - Password Controls dialog 5-4
- PeopleBooks
  - CD-ROM, ordering ii
  - printed, ordering iii
- PeopleCode
  - Signon 1-13
  - Signon PeopleCode *See* Signon PeopleCode
- PeopleCode Debugger
  - security 2-14
- PeopleSoft security 1-1
- PeopleTools
  - granting access to 2-9
  - object permissions 2-10
  - Object Security 6-1
  - permissions 2-12
- Permission Lists 2-1
  - assigning to roles 3-3
  - auditing changes 2-31
  - cloning 2-3
  - creating 2-3
  - definition 1-8
  - deleting 2-3
  - emailing passwords 2-5
  - general 2-4
  - links 2-30
  - menus 2-6
  - objects 2-10
  - PeopleTools 2-9
  - process group attributes 2-15
  - process security 2-14
  - time-out minutes 2-6
  - working with 2-1
- PIA
  - security 1-6
- Process Groups
  - security 2-15
- Process Profile
  - client destinations 2-17
  - job controls 2-18
  - permissions 2-16
  - process request options 2-18
  - security 2-16
  - server destinations 2-17
- Process Profiles
  - editing 2-16
- Process Request Options
  - allow requester to 2-19
  - override output 2-19
  - override parameters 2-19
  - recurrence 2-20
  - update by 2-18
  - update servers 2-19
  - view by 2-18
  - view servers 2-19

- Process Scheduler
  - security 1-3
- PS\_TOKEN 5-21
- PsGetLogonInfo() 7-19, 7-22
- PsGetTuxConnectInfo() 7-19, 7-24
- PSUSER.DLL 7-21
  - customizing 7-21, 7-26

## Q

- Query
  - granting security access 2-26
  - securing output 2-29
  - securing use 2-28
  - security 1-5, 2-24
- Query profiles
  - defining 2-27

## R

- Reporting
  - security 1-4
- Role rules
  - PeopleCode 1-17
  - query 1-16
- Role Rules
  - executing 5-31
- Roles 3-1
  - assigning 1-15
  - assigning a Query rule 3-4
  - assigning an LDAP/directory rule 3-5
  - assigning directory groups to 7-8
  - assigning permission lists 3-3
  - definition 1-7
  - definition of 3-1
  - dynamic 1-16
  - dynamic members 3-4, 7-8
  - dynamic rules 5-31
  - executing rules 4-6
  - extending 3-11
  - general attributes 3-2
  - static 1-16
  - testing rules 4-6
  - viewing a user's roles 4-5
  - viewing members 3-3
  - workflow options 3-11
- Roles rules
  - LDAP 1-16
- Routing Preferences 4-8

## S

- Security
  - access IDs 1-11
  - Access Profiles 5-32

- adding links 5-15
- administrative tasks 5-32
- application data 1-4
- Application Designer 2-10
- Application Message Monitor 2-22
- auditing definition modification 2-31
- authentication options 1-15
- change control 2-12
- changing passwords 4-14
- Component Interfaces 2-21
- Connect ID 1-10
- creating access profiles 5-32
- creating LDAP map 5-12
- definition synchronization 1-17
- deleting user profiles 4-18
- deleting users 5-3
- dialog 1-3
- directory server integration 1-13
- email new password 4-17
- emailing passwords 2-5
- exits 7-13
- extending Maintain Security 2-30
- extending the interface 5-15
- field-level 1-5
- functional 1-2
- general permissions 2-4
- implementation options 1-15
- importing directory groups 7-7
- importing LDAP information 5-12
- integration 7-1
- interface 1-17
- LDAP integration 1-13
- Maintain Security 1-17
- Mass Change 2-29
- Mass Change templates 2-30
- menus, components, and pages 2-6
- migrating users between databases 5-36
- My Profile 4-14
- object groups 6-3
- object level 1-4
- object types 2-10
- objects *See* Object Security
- online 1-2
- options 5-1
- pages 1-3
- password management 5-3
- PeopleSoft definitions 1-6
- PeopleTools permissions 2-9
- permission lists 2-1. *See* Permission Lists
- process 1-3
- process groups
  - granting access to 2-15
- Process Scheduler 1-3, 2-14
- processes 5-30
- PS/Query 2-24
- Query access groups 2-24
- Query output 2-29
- Query use 2-28
- reporting 1-4
- roles *See* Roles
- Row 1-5
- running LDAPMAP program 5-32
- self-service 4-14
  - alternate user 4-17
  - passwords 4-14
  - preferences 4-15
- setup options 5-1
  - user profiles 5-1
- signon 1-2, 1-12
- Signon PeopleCode 1-13
- single signon 1-14
- single signon setup 5-16
- single-signon 7-21
- skip tables for user delete 5-3
- special features 5-1
- SQL build 2-13
- SSL 5-23
- strategy 1-11
- Symbolic IDs 1-11
- time-out minutes 2-6
- understanding 1-1
- user exits 7-13
- user profile types 5-1
- user profiles *See* User Profiles
- Web Libraries 2-23
- Security processes
  - executing dynamic role rules 5-31
  - importing directory groups 7-8
  - importing LDAP directory groups 5-31
- Signon
  - customizing 7-21
  - single signon setup 5-16
  - single-signon 7-21
- Signon PeopleCode 7-9
  - enabling 7-11
  - enabling for LDAP 7-3
  - modifying 7-9
  - permissions 7-12
- Signon security 1-12
- Signon Time
  - authorizing 2-20
- Single Signon
  - authentication tokens 5-16
  - cookies 5-16
  - interface 5-18
  - PS\_TOKEN 5-21
  - token expiration 5-18
  - trusted nodes 5-19
- Single-Signon
  - implementing 7-26
  - PSUSER.DLL 7-21

SQL Editor  
     security 2-14

SSL  
     digital certificates 5-23  
     managing certificates 5-25  
     source node 5-27  
     target node 5-27, 5-30

Symbolic ID 4-3, 5-34  
     Definition of 1-11

System Administrator  
     user profile 4-9

## T

Time-out minutes  
     specifying 2-6

## U

Upgrade  
     security 2-14

User ID 1-10  
     definition of 1-10

User IDs  
     transferring 5-36

User Profile  
     account lockout 5-5  
     deleting 4-18  
     self-service 4-14  
         alternate user 4-17  
         passwords 4-14  
         preferences 4-15  
     skip tables for user delete 5-3

User profiles

    setup options 5-1

User Profiles 4-1  
     adding permission lists 4-5  
     adding roles 4-5  
     additional links 4-9  
     administrative tasks 4-10  
     alternate user 4-7  
     auditing changes to 4-9  
     currency code 4-4  
     definition 1-7  
     dynamic role rules 4-6  
     Email ID 4-4  
     form ID 4-7  
     general attributes 4-3  
     ID 4-2, 4-3  
     ID type 4-2  
     language preference 4-4  
     My Profile 4-14  
     reassign work 4-8  
     roles 4-5  
     routing preferences 4-8  
     Symbolic ID 4-3  
     system administrator profile 4-9  
     types 5-1  
     workflow 4-7  
     workflow attributes 4-7  
     working with dynamic roles rules 4-6

## W

Web Libraries  
     permissions 2-23

Workflow  
     query routings 3-11  
     reassigning work 4-8  
     user profile settings 4-7

