PeopleSoft®

Enterprise PeopleTools 8.45 PeopleBook: Security Administration

June 2004

Enterprise PeopleTools 8.45 PeopleBook: Security Administration
SKU PT845SEC-B 0604

Open Source Disclosure

PeopleSoft takes no responsibility for its use or distribution of any open source or shareware software or documentation and disclaims any and all liability or damages resulting from use of said software or documentation. The following open source software may be used in PeopleSoft products and the following disclaimers are provided.

Apache Software Foundation

This product includes software developed by the Apache Software Foundation (http://www.apache.org/). Copyright (c) 1999-2000 The Apache Software Foundation. All rights reserved.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL

Copyright (c) 1998-2003 The OpenSSL Project. All rights reserved.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

SSLeay

Copyright (c) 1995-1998 Eric Young. All rights reserved.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Loki Library

Copyright (c) 2001 by Andrei Alexandrescu. This code accompanies the book:

Alexandrescu, Andrei. "Modern C++ Design: Generic Programming and Design Patterns Applied". Copyright (c) 2001. Addison-Wesley. Permission to use, copy, modify, distribute and sell this software for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation.

Contents

About This PeopleBook

PeopleBooks provide you with the information that you need to implement and use PeopleSoft applications.

This preface discusses:

- PeopleSoft application prerequisites.
- PeopleSoft application fundamentals.
- Related documentation.
- Typographical conventions and visual cues.
- Comments and suggestions.
- Common elements in PeopleBooks.

Note. PeopleBooks document only page elements that require additional explanation. If a page element is not documented with the process or task in which it is used, then either it requires no additional explanation or it is documented with common elements for the section, chapter, PeopleBook, or product line. Elements that are common to all PeopleSoft applications are defined in this preface.

PeopleSoft Application Prerequisites

To benefit fully from the information that is covered in these books, you should have a basic understanding of how to use PeopleSoft applications.

See *Enterprise PeopleTools 8.45 PeopleBook: Using PeopleSoft Applications*.

You might also want to complete at least one PeopleSoft introductory training course.

You should be familiar with navigating the system and adding, updating, and deleting information by 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.

These books do not review navigation and other basics. They present the information that you need to use the system and implement your PeopleSoft applications most effectively.

PeopleSoft Application Fundamentals

Each application PeopleBook provides implementation and processing information for your PeopleSoft database. However, additional, essential information describing the setup and design of your system appears in a companion volume of documentation called the application fundamentals PeopleBook. Each PeopleSoft product line has its own version of this documentation.

The application fundamentals PeopleBook consists of important topics that apply to many or all PeopleSoft applications across a product line. Whether you are implementing a single application, some combination of applications within the product line, or the entire product line, you should be familiar with the contents of this central PeopleBook. It is the starting point for fundamentals, such as setting up control tables and administering security.

Related Documentation

This section discusses how to:

- Obtain documentation updates.
- Order printed documentation.

Obtaining Documentation Updates

You can find updates and additional documentation for this release, as well as previous releases, on the PeopleSoft Customer Connection website. Through the Documentation section of PeopleSoft 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 that is delivered on your PeopleBooks CD-ROM.

Important! Before you upgrade, you must check PeopleSoft Customer Connection for updates to the upgrade instructions. PeopleSoft continually posts updates as the upgrade process is refined.

See Also

PeopleSoft Customer Connection, https://www.peoplesoft.com/corp/en/login.jsp

Ordering Printed Documentation

You can order printed, bound volumes of the complete PeopleSoft documentation that is delivered on your PeopleBooks CD-ROM. PeopleSoft makes printed documentation available for each major release shortly after the software is shipped. Customers and partners can order printed PeopleSoft documentation by using any of these methods:

- Web
- Telephone
- Email

Web

From the Documentation section of the PeopleSoft Customer Connection website, access the PeopleBooks Press website under the Ordering PeopleBooks topic. The PeopleBooks Press website is a joint venture between PeopleSoft and MMA Partners, the book print vendor. Use a credit card, money order, cashier's check, or purchase order to place your order.

Telephone

Contact MMA Partners at 877 588 2525.

Email

Send email to MMA Partners at peoplesoftpress@mmapartner.com.

See Also

PeopleSoft Customer Connection, https://www.peoplesoft.com/corp/en/login.jsp

Typographical Conventions and Visual Cues

This section discusses:

- Typographical conventions.
- Visual cues.
- Country, region, and industry identifiers.
- Currency codes.

Typographical Conventions

This table contains the typographical conventions that are used in PeopleBooks:

Typographical Convention or Visual Cue	Description
Bold	Indicates PeopleCode function names, method names, language constructs, and PeopleCode reserved words that must be included literally in the function call.
Italics	Indicates field values, emphasis, and PeopleSoft or other book-length publication titles. In PeopleCode syntax, italic items are placeholders for arguments that your program must supply. We also use italics when we refer to words as words or letters as letters, as in the following: Enter 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 the W key.
`Monospace font`	Indicates a PeopleCode program or other code example.
" " (quotation marks)	Indicate chapter titles in cross-references and words that are used differently from their intended meanings.
. . . (ellipses)	Indicate that the preceding item or series can be repeated any number of times in PeopleCode syntax.
{ } (curly braces)	Indicate a choice between two options in PeopleCode syntax. Options are separated by a pipe (|).

Typographical Convention or Visual Cue	Description
[ ] (square brackets)	Indicate optional items in PeopleCode syntax.
& (ampersand)	When placed before a parameter in PeopleCode syntax, an ampersand indicates that the parameter is an already instantiated object. Ampersands also precede all PeopleCode variables.

Visual Cues

PeopleBooks contain the following visual cues.

Notes

Notes indicate information that you should pay particular attention to as you work with the PeopleSoft system.

Note. Example of a note.

If the note is preceded by *Important!*, the note is crucial and includes information that concerns what you must do for the system to function properly.

Important! Example of an important note.

Warnings

Warnings indicate crucial configuration considerations. Pay close attention to warning messages.

Warning! Example of a warning.

Cross-References

PeopleBooks provide cross-references either under the heading "See Also" or on a separate line preceded by the word *See*. Cross-references lead to other documentation that is pertinent to the immediately preceding documentation.

Country, Region, and Industry Identifiers

Information that applies only to a specific country, region, or industry is preceded by a standard identifier in parentheses. This identifier typically appears at the beginning of a section heading, but it may also appear at the beginning of a note or other text.

Example of a country-specific heading: "(FRA) Hiring an Employee"

Example of a region-specific heading: "(Latin America) Setting Up Depreciation"

Country Identifiers

Countries are identified with the International Organization for Standardization (ISO) country code.

See *About These PeopleBooks*, "ISO Country and Currency Codes," ISO Country Codes.

Region Identifiers

Regions are identified by the region name. The following region identifiers may appear in PeopleBooks:

- Asia Pacific
- Europe
- Latin America
- North America

Industry Identifiers

Industries are identified by the industry name or by an abbreviation for that industry. The following industry identifiers may appear in PeopleBooks:

- USF (U.S. Federal)
- E&G (Education and Government)

Currency Codes

Monetary amounts are identified by the ISO currency code.

See Appendix A, “ISO Country and Currency Codes,” ISO Currency Codes.

Comments and Suggestions

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

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

Or send email comments to doc@peoplesoft.com.

While we cannot guarantee to answer every email message, we will pay careful attention to your comments and suggestions.

Common Elements in These PeopleBooks

As of Date	The last date for which a report or process includes data.
Business Unit	An ID that represents a high-level organization of business information. You can use a business unit to define regional or departmental units within a larger organization.
Description	Enter up to 30 characters of text.
Effective Date	The date on which a table row becomes effective; the date that an action begins. For example, to close out a ledger on June 30, the effective date for the ledger closing would be July 1. This date also determines when

	you can view and change the information. Pages or panels and batch processes that use the information use the current row.
Once, Always, and **Don't Run**	Select Once to run the request the next time the batch process runs. After the batch process runs, the process frequency is automatically set to Don't Run. Select Always to run the request every time the batch process runs. Select Don't Run to ignore the request when the batch process runs.
Report Manager	Click to access the Report List page, where you can view report content, check the status of a report, and see content detail messages (which show you a description of the report and the distribution list).
Process Monitor	Click to access the Process List page, where you can view the status of submitted process requests.
Run	Click to access the Process Scheduler request page, where you can specify the location where a process or job runs and the process output format.
Request ID	An ID that represents a set of selection criteria for a report or process.
User ID	An ID that represents the person who generates a transaction.
SetID	An ID that represents a set of control table information, or TableSets. TableSets enable you to share control table information and processing options among business units. The goal is to minimize redundant data and system maintenance tasks. When you assign a setID to a record group in a business unit, you indicate that all of the tables in the record group are shared between that business unit and any other business unit that also assigns that setID to that record group. For example, you can define a group of common job codes that are shared between several business units. Each business unit that shares the job codes is assigned the same setID for that record group.
Short Description	Enter up to 15 characters of text.

See Also

Enterprise PeopleTools 8.45 PeopleBook: PeopleSoft Process Scheduler

Enterprise PeopleTools 8.45 PeopleBook: Using PeopleSoft Applications

Security Administration Preface

This preface provides a general overview of the contents discussed in the PeopleTools Security Administration PeopleBook.

Security Administration

This PeopleBook describes the interface, tables, and 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. Remember that your application documentation also contains security topics that are more specific to the applications you have purchased.

CHAPTER 1

Getting Started with Security Administration

This chapter provides overviews of security administration and security administration integrations and discusses security administration implementation.

Security Administration Overview

This section discusses:

- User security.
- Lightweight Directory Access Protocol.
- Authentication and single signon.
- Pluggable cryptography.
- Query and definition security.
- PeopleSoft personalizations.

User Security

The core functionality of security administration in PeopleSoft applications is user security, which you administer using several basic elements.

To establish appropriate user access:

1. Define permission lists.

   Permission lists are the building blocks of user security authorization. A permission list grants a particular degree of access to a particular combination of PeopleSoft elements, specifying pages, development environments, time periods, administrative tools, personalizations, and so on.

   This level of access should be appropriate to a narrowly defined and limited set of tasks, which can apply to a variety of users with a variety of different roles. These users might have overlapping — but not identical — access requirements.

   You typically define permission lists before you define roles and user profiles. When defining permission lists, however, consider the roles that you will use them with.

   See Chapter 3, “Setting Up Permission Lists,” page 23.

2. Define roles.

   A *role* is essentially a collection of permission lists. You can assign one or more permission lists to a role. The resulting combination of permissions can apply to all users who share those access requirements. However, the same group of users might also have other access requirements that they don’t share with each other. You can assign a given permission list to multiple roles.

You typically define roles after first defining their permission lists, and before defining user profiles. You use roles to assign permissions to users dynamically.

See Chapter 4, "Setting Up Roles," page 51.

3. Define user profiles.

   A *user profile* is a definition that represents one PeopleSoft user. Each user is a unique; the user profile specifies a number of user attributes, including one or more assigned roles. Each role that's assigned to a given user profile adds its permission lists to the total that apply to that user.

   You typically define user profiles after defining their roles. You can assign a given role to multiple user profiles. It's worthwhile to define a set of roles that you're confident can be assigned to user profiles that you'll create in the future.

   See Chapter 5, "Administering User Profiles," page 65.

Lightweight Directory Access Protocol (LDAP)

LDAP is an internet protocol used to access a directory listing. Organizations typically store user profiles in a central repository, a *directory server*, that serves user information for all of the programs that require it. If your existing computer network uses an LDAP V3 compliant directory server, PeopleSoft supports the use of that server for managing user profiles and authenticating users. PeopleSoft enables you to integrate your authentication scheme for PeopleSoft with your existing infrastructure.

You always maintain permission lists and roles using PeopleSoft security. However, you can maintain user profiles in PeopleSoft security or reuse user profiles and roles that are already defined within an LDAP directory server. 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 synchronization.

You can configure and extend your signon PeopleCode to work with any schema implemented in your directory server. You can assign roles to users manually or assign them dynamically. When assigning roles dynamically, you use PeopleCode, LDAP, and PeopleSoft Query rules to assign user profiles to roles programmatically.

See Chapter 6, "Employing LDAP Directory Services," page 93.

Authentication and Single Signon

PeopleSoft delivers the most common authentication solutions and packages them with your PeopleSoft application. This saves you the trouble of developing your own solutions and saves you time with your security implementation. These prepackaged solutions include PeopleCode that supports basic sign-in through secure sockets layer (SSL), LDAP authentication, and single signon.

Because PeopleSoft applications are designed for internet deployment, many sites must take advantage of the authentication services that exist at the web server level. PeopleSoft takes advantage of HTTPS, 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 business-to-business processing) over the internet.

PeopleSoft supports *single signon* within PeopleSoft applications. 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 different applications and databases, the user navigates seamlessly through the system. Recall that each suite of PeopleSoft applications, such as HCM or CRM, resides in its own database.

See Chapter 7, "Employing Signon PeopleCode and User Exits," page 117 and Chapter 8, "Setting up Digital Certificates and Single Signon," page 139.

Pluggable Cryptography

Data security comprises the following elements:

- Privacy — keeping data hidden from unauthorized parties.

  Privacy is normally implemented with some type of *encryption*. Encryption is the scrambling of information such that no one can read it unless they have a piece of data known as a key.

- Integrity — keeping transmitted data intact.

  Integrity can be accomplished with simple checksums or, better, with more complex cryptographic checksums known as *one-way hashes*, and often with *digital signatures* as well.

- Authentication — verifying the identity of an entity that's transferring data.

  Authentication can be accomplished using passwords, or with digital signatures, which are by far the most popular and most reliable method of authentication.

PeopleSoft *pluggable encryption technology* (PET) provides a way for you to use hashes and digital signatures to secure critical PeopleSoft data and communicate securely with other businesses. It enables you to extend and improve cryptographic support for your data in PeopleTools, giving you strong cryptography with the flexibility to change and grow, by incrementally acquiring stronger and more diverse algorithms for encrypting data. PeopleSoft delivers pluggable encryption technology with support for the *OpenSSL* and *PGP* encryption libraries.

To implement pluggable cryptography:

1. Load an encryption library's algorithms into the PET database.
2. Generate accompanying encryption keys, and insert them into the PET keystore
3. Define a sequence, or *chain* of algorithms by selecting from all the algorithms in the database.
4. Define an encryption profile, which is an instance of an algorithm chain applicable to a specific encryption task.
5. Write PeopleCode to invoke the encryption profile.

See Chapter 9, "Securing Data with Pluggable Cryptography," page 159.

Query and Definition Security

You use PeopleSoft Query to build SQL queries and retrieve information from application tables. For each PeopleSoft Query user, you can specify the records the user is allowed to access when building and running queries. You do this by creating query access groups in PeopleSoft Tree Manager, and then assigning users to those groups with PeopleSoft Query security. PeopleSoft Query security is enforced only when using PeopleSoft Query; it doesn't control runtime page access to table data.

Use Definition Security to govern access to database object definitions, such as record definitions, field definitions, and page definitions, and to protect particular object definitions from being modified by developers.

See Chapter 10, "Implementing Query Security," page 181 and Chapter 11, "Implementing Definition Security," page 189.

PeopleSoft Personalizations

PeopleSoft offers a variety of options that enable end users, especially power users, to configure certain aspects of their PeopleSoft environment to produce a more personalized interface. These options improve a user's navigation speed through the system and enable users to select international preferences, such as date and time formats.

You define, group, and categorize personalization options, then use permission lists to control access to them. Users with access to a personalization option can control it through the My Personalizations menu.

See Chapter 12, "Managing PeopleSoft Personalizations," page 199.

Security Administration Integrations

This section identifies the Security integration points using:

- Component interfaces.
- Messages.
- Application Engine programs.

Component Interfaces

The following are the delivered component interfaces designed for security integration.

DELETE_ROLE

This Component Interface is based on the Delete Role Component, and it is used to purge roles. It is keyed by RoleName, and has the Get, Find, Save, Cancel methods. The DELETE_ROLE Application Message calls this Component Interface.

DELETE_USER_PROFILE

This Component Interface is based on the Delete User Profile Component, and it is used to purge User Profiles. It is keyed by User ID, and has the Get, Find, Save, Cancel methods. The Delete_User_Profile Application Message, and the PURGEOLDUSERS Application Engine program call this Component Interface.

ROLE_MAINT

This Component Interface is based on the Roles Component. It is keyed by RoleName and has the Cancel, Create, Find, and Get methods.

USERMAINT_SELF

This Component Interface is based on the My Profile Component. It allows only the current user to access it.

This CI is used with the following components: Forgot My Password, Change Password, and Change Expired Password.

USER_PROFILE

This Component Interface is based on the User Profiles Component. It is keyed by User ID.

This CI is used in User Profile Save As, and with LDAP authentication.

Messages

The following are the delivered messages designed for security integration.

DELETE_ROLE

This message is called from the Delete Role component. It is used to the delete the role from subscribing databases. The message requires that the DELETE_ROLE Component Interface be authorized.

Note. Currently the PeopleCode that publishes this message from the Delete Role component is commented out. If you would like to publish deletes to another database, you will need to uncomment the following PeopleCode found on the PURGE_ROLEDEFN.GBL SavePostChange Component PeopleCode.

```
/*****************************************************************
The PeopleCode to publish new User IDs, and changes made to User IDs, has been
commented out to prevent unnecessary publishing.
If you would like to take advantage of the DELETE_ROLE message, un-comment
the following peoplecode.
*****************************************************************/
/*
If %Mode = "U" Then
   &ROLECHANGE = GetLevel0();
   &MSG = CreateMessage(Message.DELETE_ROLE);
   &MSG.CopyRowsetDelta(&ROLECHANGE);
   &MSG.Publish();
End-If;
*/
```

DELETE_USER_PROFILE

This message is called from the Delete User Profile Component. It is used to delete the user profile from subscribing databases. This message requires that the DELETE_USER_ PROFILE Component Interface be authorized.

Note. PeopleSoft delivers the PeopleCode to publish this message from the Delete User Profile component, however, it is currently commented out. If you would like to publish deletes to another database, you will need to uncomment the following PeopleCode found on the PRG_USR_PROFILE.OPRID SavePostChange (Record PeopleCode).

```
/*****************************************************************
The PeopleCode to publish deleted User IDs, has been
commented out to prevent unnecessary publishing.
If you would like to take advantage of DELETE_USER_PROFILE message, un-comment
the following peoplecode.
*****************************************************************/
/*&RS_DELETE = GetLevel0();
&MSG = CreateMessage(Message.DELETE_USER_PROFILE);
&MSG.CopyRowsetDelta(&RS_DELETE);
&MSG.Publish();
*/
```

ROLESYNCH_MSG

This message is published when a Dynamic Role Rule is run. It is called after the DYNROL_PUBL Application Engine program successfully finishes.

ROLE_MAINT

This Application Message publishes new Roles, and updates to existing Roles made in the Roles Component.

Currently, the PeopleCode to publish this Message is commented out. If you would like to take advantage of the ROLE_MAINT message, you need to uncomment the PeopleCode found on ROLEMAINT.GBL SavePostChange Component PeopleCode.

```
/*****************************************************************
PeopleCode to publish new Roles, and changes made to Roles has been
commented out to prevent unnecessary publishing.
If you would like to take advantage of ROLE_MAINT message, uncomment
the following peoplecode.
*****************************************************************/

/*If %Mode = "A" Then
   &ROLECHANGE = GetLevel0();
   &MSG = CreateMessage(Message.ROLE_MAINT);
   &MSG.CopyRowset(&ROLECHANGE);
   &MSG.Publish();
Else
   &ROLECHANGE = GetLevel0();
   &MSG = CreateMessage(Message.ROLE_MAINT);
   &MSG.CopyRowsetDelta(&ROLECHANGE);
   &MSG.Publish();
End-If;*/
```

USER_PROFILE

This Application Message publishes new User Profiles, and updates to existing User Profiles when using the User Profile Component, the User Profile Save As Component, the My Profile Component, the Distributed User Profile Component, the USER_PROFILE Component Interface and the USERMAINT_SELF Component Interface.

Currently, the PeopleCode to publish this Message is commented out. If you would like to take advantage of the USER_PROFILE message, you need to uncomment the following PeopleCode:

USERMAINT.GBL SavePostChange Component PeopleCode:

```
/*****************************************************************
The PeopleCode to publish new User IDs, and changes made to User IDs, has been
commented out to prevent unnecessary publishing.
If you would like to take advantage of USER_PROFILE message, un-comment
the following peoplecode (if statment only).
*****************************************************************/
/*
If %Mode = "A" Then
   &USERPROFILECHANGE = GetLevel0();
   &MSG = CreateMessage(Message.USER_PROFILE);
```

```
   &MSG.CopyRowset(&USERPROFILECHANGE);
   &MSG.Publish();
Else
   &USERPROFILECHANGE = GetLevel0();
   &MSG = CreateMessage(Message.USER_PROFILE);
   &MSG.CopyRowsetDelta(&USERPROFILECHANGE);
   &MSG.Publish();
End-If;*/
```

USERMAINT_SELF.GBL SavePostChange Component PeopleCode:

```
rem call USER_PROFILE application message to synch user changes;
/*********************************************************************
The PeopleCode to publish changes made to User IDs has been
commented out to prevent unnecessary publishing.
If you would like to take advantage of USER_PROFILE message, un-comment
the following peoplecode
*********************************************************************/
/*
If %Mode = "U" Then
   &USERPROFILECHANGE = GetLevel0();
   &MSG = CreateMessage(Message.USER_PROFILE);
   &MSG.CopyRowsetDelta(&USERPROFILECHANGE);
   &MSG.Publish();
End-If;
*/
```

USERMAINT_DIST.GBL SavePostChange Component PeopleCode:

```
/*********************************************************************
The PeopleCode to publish new User IDs, and changes made to User IDs, has been
commented out to prevent unnecessary publishing.
If you would like to take advantage of USER_PROFILE message, un-comment
the following peoplecode (if statment only).
*********************************************************************/
/*
If %Mode = "A" Then
   &USERPROFILECHANGE = GetLevel0();
   &MSG = CreateMessage(Message.USER_PROFILE);
   &MSG.CopyRowset(&USERPROFILECHANGE);
   &MSG.Publish();
Else
   &USERPROFILECHANGE = GetLevel0();
   &MSG = CreateMessage(Message.USER_PROFILE);
   &MSG.CopyRowsetDelta(&USERPROFILECHANGE);
   &MSG.Publish();
End-If;
*/
```

Application Engine Programs

The following are the delivered Application Engine programs designed for security integration.

DYNROLE

Application Engine Program that is called when Dynamic Role Rules are published from the User Profile.

DYNROLE_PUBL

Application Engine Program that is called when the Dynamic Role Rules are published from the Role.

PURGEOLDUSERS

Application Engine Program that deletes users that have not signed on within a period specified on Password Controls.

LDAPSCHEMA

Application Engine Program that puts the LDAP Schema definition into the PeopleSoft database.

Security Administration Implementation

This section discusses:

- Preparing to use PeopleSoft security.
- Administering security from applications.

Preparing to Use PeopleSoft Security

The functionality of security administration for your PeopleSoft applications is delivered as part of the standard installation of PeopleTools, which is provided with all PeopleSoft products.

To start administering security, install your PeopleSoft application according to the installation guide for your database platform.

Other Sources of Information

This section provides information to consider before you begin to manage your data. In addition to implementation considerations presented in this section, take advantage of all PeopleSoft sources of information, including the installation guides, release notes, and PeopleBooks.

See Also

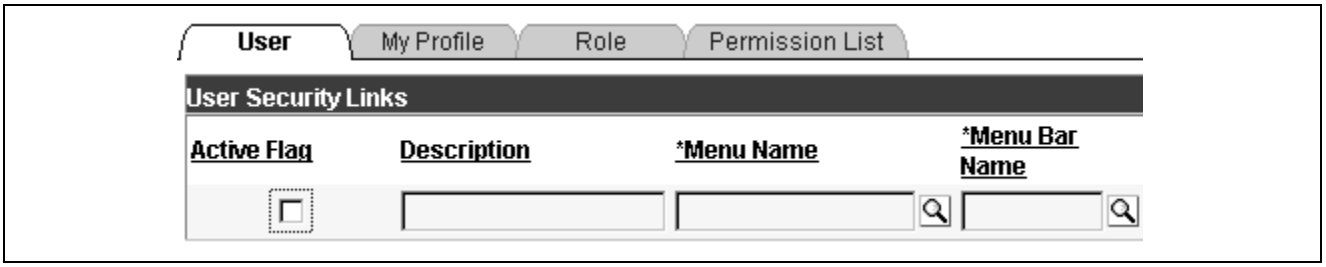
"Security Administration Preface," page xix

Enterprise PeopleTools 8.45 PeopleBook: Getting Started with Enterprise PeopleTools

Administering Security from Applications

If you administer security information outside of the PeopleSoft security interface, for example using application-specific pages to define application security, you have the option of modifying the PeopleSoft security menus to include links to those pages. This provides administrators a convenient way to access application-specific security pages without having to spend time navigating to them.

You add the extra security links from a browser by selecting PeopleTools, Security, Security Objects, Security Links. You can add links to the User Profile component, My System Profile page, 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.



Security Links - User page (1 of 2)

Security Links - User page (2 of 2)

Active Flag Enables you to activate and deactivate links. Only those links with the Active Flag checked appear for system users.

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, My Profile, and Permission List.

Test After you have added all the appropriate information, use this link to test the security link. If it does not work correctly, double check your selections for the previous options.

To add a Security Link

1. Select PeopleTools, Security, Security Objects, Security Links.
2. Select the security profile type (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 appropriate link information (Menu Name, Menu Bar name, and so on) information.
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.

Note. 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.

CHAPTER 2

Understanding PeopleSoft Security

This chapter discusses:

- Security basics.
- PeopleSoft online security.
- PeopleSoft authorization IDs.
- PeopleSoft sign-in.
- Implementation options.

Security Basics

Security is especially critical for core business applications, such as PeopleSoft applications. Typically, you do not want every department in your company to have access to all your applications. Nor do 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 customize your applications with PeopleTools.

PeopleSoft provides security features, including components and PeopleTools applications, to ensure that your sensitive application data, such as employee salaries, performance reviews, or home addresses, does not fall into the wrong hands. Most likely, you use other security tools for your network and relational database management system (RDBMS). These tools work together to protect the PeopleSoft system from unauthorized access.

As you implement the PeopleSoft Internet Architecture (PIA), you 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.

The PeopleSoft security approach is tailored for the internet. It enables you to easily create and maintain security definitions, and you can perform many maintenance tasks programmatically.

You can apply security to all users, including employees, managers, customers, contractors, and suppliers. You group your users according to roles to give them different degrees of access. For instance, there might be an Employee role, a Manager role, and 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.

You must also secure the objects and definitions in your PeopleSoft development environment. Just as you restrict sets of end users from accessing particular pages and components, you also restrict the definitions that your site's developers can access using PeopleSoft Application Designer. A *definition* refers to any of the definitions that you create within PeopleSoft Application Designer, such as records, pages, or components. Each object definition may have individual security needs. For example, you may have a large development staff, but perhaps you want only a few developers to have access to specific record definitions.

PeopleSoft Security Definitions

Because deploying your applications to the internet significantly increases the number of potential users your system must accommodate, you need an efficient method of granting authorization to different user types. PeopleSoft security definitions provide a modular means to apply security attributes in a scalable manner.

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

- User profiles.
- Roles.
- Permission lists.

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

User Profiles

User profiles define individual PeopleSoft users.

Each user has an individual user profile, which in turn is linked to one or more roles. You add one or more permission lists, which ultimately control what a user can and can't access, to each role. A few permission types are assigned directly to the user profile.

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.

Roles

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, and Student.

A manager is also an employee, and may also be a student. Roles enable you to mix and match access appropriately.

You have two options when assigning roles: assign roles manually or assign them dynamically. When assigning roles dynamically, you use PeopleCode, LDAP, and PeopleSoft Query rules to assign user profiles to roles programmatically.

Permission Lists

Permission lists are groups of authorizations that you assign to roles. Permission lists store sign-in 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.

A user profile inherits most of its permissions through roles, but you apply some permission lists, such as process profile or row-level security (data permissions), directly to a user profile.

See Also

The PeopleSoft Customer Connection website

PeopleSoft Online Security

The PeopleSoft system has many components, such as batch processes, object definitions, and application data. Use PeopleTools security tools to control access to most of these components. To secure other elements, you use application-specific interfaces, such as Administer Security.

This section discusses:

- Sign-in and time-out security.
- Page and dialog box security.
- Batch environment security.
- Definition security.
- Application data security.
- PeopleSoft Internet Architecture security.

Sign-in and Time-out Security

When a user attempts to sign in to PeopleSoft, he or she enters 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 sign in during an invalid sign-in time, as defined in the user's security profile, he or she is not allowed to sign on. A sign-in time is an adjustable interval during which a user is allowed to sign in to PeopleSoft. For example, if a given sign-in time is Monday through Friday from 7 a.m. to 6 p.m. for a set of users, those users cannot access a PeopleSoft application on Saturday or on Friday at 6:05 p.m. If a user is signed in when the sign-in period expires, PeopleSoft signs the user out automatically.

After a user signs on, he or she can stay connected as long as the sign-in time allows and as long as the browser doesn't sit idle for longer than the timeout interval. A timeout interval specifies how long the user's machine can remain idle—no keystrokes, no SQL—before PeopleSoft automatically signs the user out of the application.

You specify both the sign-in times and time-out interval using PeopleTools Security.

Note. Other timeout intervals, unrelated to security, are controlled by your web server and by PeopleSoft Internet Architecture components.

Page and Dialog Box Security

You can restrict access to PeopleSoft menus. You can set the access rights to the entire menu, such as Administer Workforce or PeopleTools Security, or just a specific item on that menu. Because the only normal 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.

You can also restrict access to specific actions or commands on a page. For example, you may want a clerk in your sales office to be able to access contract data, but not be able to update the data. In this case, you grant access to the set of pages, but you allow display only access only. In this case, the clerk cannot update or correct any data. This approach enables users to get their work done while maintaining the security and integrity of your business data.

Batch Environment Security

If a particular user must run batch processes using PeopleSoft Process Scheduler, assign the appropriate process profile to the user profile and create process groups for your processes. A user receives both process group and process profile authorizations through permission lists. A user gets permission to process groups through roles, and they get a process profile through the process profile permission list.

Note. 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, make sure that you are running your batch processes in a secure environment.

There are three levels of security for batch programs:

- Each batch program has a run control that you define before you can run the batch program.

  Run controls are set up using PeopleSoft Process Scheduler

- Also using PeopleSoft Process Scheduler, you set up process groups, which are groups of batch processes.

  In PeopleTools Security you add process groups to a security profile. Users can run processes that belong to the process groups assigned to their security profile.

- In your RDBMS environment, you can restrict offline access to batch processes using the security tools described in your platform manuals.

Reporting Security

PeopleSoft Report Manager uses a logical space on a web server called the Report Repository. PeopleSoft Report Manager enables you to generate and distribute reports over the internet, and it stores the output in the Report Repository. Wherever you decide to situate your repository, make sure that the server is protected from outside access. Ensure that only PeopleSoft can access and distribute the generated reports. The Report Repository servlet gets items from the web server and puts them in the browser. With report distribution, you distribute reports and view them according to your role.

PeopleSoft delivers the following roles for the specific use in reporting:

- ReportDistAdmin
- ReportSuperUser

Definition Security

Use Definition Security to govern access to database object definitions, such as record definitions, field definitions, and page definitions, and to protect particular object definitions from being modified by certain developers.

Application Data Security

Definition security is a form of data security—you use it to control access to particular rows of data (object definitions) in PeopleTools tables. PeopleSoft also provides other methods 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.

Table-Level Security

You use PeopleSoft Query to build SQL queries and retrieve information from application tables. For each PeopleSoft Query user, you can specify the records the user is allowed to access when building and running queries. You do this by creating query access groups in PeopleSoft Tree Manager, and then assigning users to those groups with PeopleSoft Query security. PeopleSoft Query security is enforced only when using PeopleSoft Query; it doesn't control runtime page access to table data.

Row-Level Security

You can design special types of SQL views—security views—to control access to individual rows of data stored within application database tables. Row-level security enables you to specify the 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, PeopleSoft Human Resources security tables enable you to restrict user access to employee rows of data according to organizational roles. You could also permit users to view and update rows for employees in their departments only. Similarly, in PeopleSoft Financials, you can use security views to determine access to 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.

See the documentation for your application for details about implementing row-level security for your applications.

Field Security

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

PeopleSoft Internet Architecture Security

PeopleSoft Internet Architecture security is also known as runtime security. Only authorized users can connect to the web and application server, and only authorized application servers can connect to a given database.

PeopleSoft uses authentication tokens embedded in browser cookies to authorize users and enable single sign-in throughout the system. To secure links between system components, including browsers, web servers, application servers, and database servers, PeopleSoft incorporates a combination of Secure Sockets Layer (SSL) security and BEA Tuxedo and BEA Jolt encryption.

SSL is a protocol developed by Netscape that defines an interface for data encryption between network nodes. To establish an SSL-encrypted connection, the nodes must complete the SSL handshake. The simplified steps of the SSL handshake are as follows:

1. Client sends a request to connect.
2. Server responds to the connect request and sends a signed certificate.
3. Client verifies that the certificate signer is in its acceptable certificate authority list.
4. Client generates a session key to be used for encryption and sends it to the server encrypted with the server's public key (from the certificate received in step 2).
5. Server uses a private key to decrypt the client generated session key.

Establishing an SSL connection requires two certificates: one containing the public key of the server (server certificate or public key certificate) and another to verify the certification authority that issued the server certificate (trusted root certificate). The server needs to be configured to issue the server certificate when a client requests an SSL connection and the client needs to be configured with the trusted root certificate of the certificate authority that issued the server certificate.

The nature of those configurations depends on both the protocol being used and the client and server platforms. In most cases you replace HTTP with Lightweight Directory Access Protocol (LDAP). SSL is a lower level protocol than the application protocol, such as HTTP or LDAP. SSL works the same regardless of the application protocol.

Note. Establishing SSL connections with LDAP is not related to web server certificates or certificates used with PeopleSoft integration.

The system uses SSL encryption in the following locations:

- Between the browser and the web server.
- Between the application server and the integration gateway.
- Between the integration gateway and an external system.

The system uses BEA Tuxedo and BEA Jolt encryption in these locations:

- Between the web server and the application server.
- Between the integration gateway and a PeopleSoft system (BEA Jolt only).

Security between the application server and database is supplied by RDBMS connectivity.

PeopleSoft Integration Broker and portal products have additional security concerns, which are addressed in the documentation for those products.

See Also

Enterprise PeopleTools 8.45 PeopleBook: PeopleSoft Integration Broker

Enterprise PeopleTools 8.45 PeopleBook: Internet Technology

PeopleSoft Authorization IDs

The PeopleSoft system uses various authorization IDs and passwords to control user access. You use PeopleTools Security to assign two of these IDs: the user ID and the symbolic ID.

This section discusses:

- User IDs.
- Connect ID.
- Access IDs.
- Symbolic IDs.
- Administrator access.

See Also

Chapter 2, “Understanding PeopleSoft Security,” PeopleSoft Sign-in, page 18

User IDs

A PeopleSoft user ID is the ID you enter at the PeopleSoft sign-in dialog box. You 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 the key used to identify the user profile definition.

Connect ID

The connect ID performs the initial connection to the database.

Note. PeopleSoft no longer creates users at the database level.

A connect ID is a valid user ID that, when used during sign-in, takes the place of PeopleSoft user IDs. Using a connect ID means you don’t have to create a new database user for every PeopleSoft user that you add to the system.

Note. A connect ID is required for a direct connection (two-tier connection) to the database. Application servers and two-tier Microsoft Windows clients require a connect ID. You specify the connect ID for an application server in the Signon section of the PSADMIN utility. For Microsoft Windows clients, you specify the connect ID in the Startup tab of PeopleSoft Configuration Manager. You can create a connect ID by running the Connect.SQL and Grant.SQL scripts.

Warning! Without a connect ID specified, the system assumes that workstation is accessing PeopleSoft through an application server. The option to override the database type is disabled.

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 applications are ultimately connected to your database after the PeopleSoft system connects using the connect ID and validates the user ID and password. An access ID typically 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.

Users do not know their corresponding access IDs. They just sign in with their user IDs and passwords. Behind the scenes, the system signs them into the database using the access ID.

If users try to access the database directly with a query tool using their user or connect IDs, they have limited access. User and connect IDs only have access to the few PeopleSoft tables used during sign-in, and that access is Select-level only. Furthermore, PeopleSoft encrypts all sensitive data that resides in those tables.

Note. Access profiles are used when an application server connects to the database, when a Microsoft 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 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 sign in to the database.

Note. PeopleSoft suggests that you only use one access ID for your system. Some RDBMS do not permit more than one database table owner. If you create more than one access ID, it may require further steps to ensure that this ID has the correct rights to all PeopleSoft system tables.

Symbolic IDs

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, must be retrieved or referenced, the query selects the appropriate access ID by using the symbolic ID as a search key.

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 need to update only the reference of the access ID to the symbolic ID in the PSACCESSPRFL table. You do not need to update every user profile in the PSOPRDEFN table.

Administrator Access

As an administrator, you must customize your own user definition. PeopleSoft delivers at least one full-access user ID with each delivered database. Your first task should be to sign in 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. You should change the passwords of all delivered IDs as soon as possible.

Note. PeopleSoft-delivered IDs and passwords are 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, set up the others before creating any new PeopleSoft security definitions. Most sites only use one access profile.

The number of database-level IDs you create is up to your site requirements. However, in most cases, having fewer database-level IDs reduces maintenance issues.

For example, if you implement pure LDAP authentication, at a minimum you need two database-level IDs—your access ID and your connect ID. With this scenario, in PeopleSoft you need to maintain only a symbolic ID to reference the access ID and maintain a user ID that the application server uses during sign-in. 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.

PeopleSoft Sign-in

This section discusses:

- PeopleSoft sign-in.
- Directory server integration.
- Authentication and sign-in PeopleCode.
- Single signon.

PeopleSoft Sign-in

The most common direct sign-in to the PeopleSoft database is the application server sign-in, so let's examine how the application server signs in to the database.

The basic steps in a PeopleSoft sign-in are:

1. Initial connection.

   The application server starts, and uses the connect ID and user ID specified in its configuration file (PSAPPSRV.CFG) to perform the initial connection to the database.

2. The server performs a SQL Select statement on security tables.

   After the connect ID is verified, the application server performs a Select statement on PeopleTools security tables, such as PSOPRDEFN, PSACCESSPRFL, and PSSTATUS. From these tables, the application server gathers such items as the user ID and password, symbolic ID, access ID, and access password. After the application server has the required information, it disconnects.

3. The server reconnects with the 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 in using a Microsoft Windows workstation are developers using PeopleSoft Application Designer or end users who need to access PeopleSoft Query or Tree Manager.

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

PeopleSoft recommends that all connectivity be made through either a three-tier Microsoft Windows client or through the browser. A two-tier connection is no longer necessary other than for the application server, PeopleSoft Process Scheduler, or for a user who will be running upgrades or PeopleSoft Data Mover scripts.

Sign-in 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 recognizes 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.

Organizations typically store 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.

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 synchronization.

You always maintain permission lists and roles using PeopleTools Security. However, you can maintain user profiles in PeopleTools Security or with an external LDAP server.

See Also

Chapter 6, "Employing LDAP Directory Services," page 93

Authentication and Signon PeopleCode

You can store PeopleSoft passwords within PeopleTools, in the PSOPRDEFN table. You can also store and maintain 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 sign-in PeopleCode.

If you decide 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 PeopleTools Security.

Signon PeopleCode copies the most recent user profile data from a directory server to the local database whenever a user signs in. 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 in, signon PeopleCode checks to see to see if the row in the user profile cache needs to be updated.

The sign-in process occurs as follows:

1. The user enters a user ID and password on the sign-in page.
2. PeopleTools attempts to authenticate the user against the PSOPRDEFN table.
3. Signon PeopleCode runs.

   The default signon PeopleCode program updates the user profile based on the current data stored in the directory server.

You can use signon PeopleCode and business interlinks to synchronize the local copy of the user profile with any data source at sign-in time—the program that ships with PeopleTools is designed to synchronize the user profile with an LDAP directory server only. Because the sign-in program is PeopleCode, you can modify it, 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 sign-in PeopleCode program need to have a good understanding of PeopleCode and the integration features it offers.

Note. Only users who signon through PIA or three-tier Microsoft Windows clients take advantage of sign-in PeopleCode.

Single Signon

PIA uses browser cookies for seamless single signon across all PeopleSoft nodes. A node refers to a database and the application servers connected to it. For example, a user can complete a PeopleSoft Human Resources transaction, and then click a link for a PeopleSoft 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.

See Also

Chapter 8, "Setting up Digital Certificates and Single Signon," page 139

Implementation Options

By using our integration technologies, you can configure PeopleSoft security to work with numerous schemes.

This section discusses:

- Authentication.
- Role assignments.
- Cross-system synchronization.

Authentication

Consider how you plan to authorize users as they sign in 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 existing user profiles in an external directory server?

PeopleSoft-based Authentication

This option is, generally, the way PeopleSoft customers have authorized users in previous releases. PeopleSoft user passwords are stored and maintained solely within PeopleSoft. Although this method does not require a large amount of storage, it does add administration issues, mainly because PeopleSoft passwords are yet another password users 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

You can also use a central repository for user information in a directory server that uses the LDAP protocol.

The advantage of this option is that a user has one user ID and password that allows access to numerous software systems.

Role Assignments

Consider how you plan to assign authorizations to your users. Recall that users inherit permissions through the roles to which they are assigned. When you plan your authorization assignment, you are really planning how you intend to assign roles to users. There are two ways to assign roles to users: the static approach and the dynamic approach.

Static

You assign users to roles manually. The static approach is not scalable to the thousands of users that are likely to use 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

The system assigns roles based on business rules. You can manually run the rule, but typically, you run the rules from a scheduled batch process.

Suppose an employee changes jobs and 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 adds the appropriate roles required for the new position. In addition, you can have the rule publish a message to other nodes, such as a PeopleSoft Financials node, that might subscribe to changes in the PeopleSoft Human Resources database.

You can use PeopleSoft Query, LDAP, or PeopleCode to define dynamic role assignment. If necessary, you can use a combined 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. For example, a Manager role could be derived partially from an LDAP rule and partially from a PeopleSoft Query rule. As the following list describes, where the information that drives your role assignments is stored determines the types of role rules you use:

- If the membership data for your roles resides in your PeopleSoft database, use PeopleSoft Query to construct your role rules.

  One query could be MANAGER, another EMPLOYEE, and so on. When the rule runs, 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.

- If you already have LDAP directory server groups organized by region, department, position, and so on, base your rules on the existing LDAP structure.

  Based on the directory setup and hierarchy, your rule assigns PeopleSoft users to the appropriate roles. PeopleSoft uses your existing LDAP configuration. You should use this role rule type in conjunction with LDAP authentication.

- If you have user information in other third-party systems, such as legacy mainframe applications or UNIX account groups, use PeopleCode.

  You can 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, consider how to keep user information synchronized. 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 PeopleSoft Human Resources, a user may click a link that takes her directly to PeopleSoft Financials.

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 example, suppose PeopleSoft Financials system needs a list of managers for a particular transaction. Because the manager information resides in PeopleSoft Human Resources, the PeopleSoft Human Resources system publishes any changed information to PeopleSoft Financials to keep the data synchronized.

PeopleSoft also publishes a message when a user profile changes. This is most useful if you are 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.

You can upgrade permission lists and roles using the PeopleSoft Application Designer upgrade features. For user information, PeopleSoft Data Mover scripts migrate user profiles between systems for upgrades or bulk loads.

CHAPTER 3

Setting Up Permission Lists

This chapter provides an overview of permission lists and discusses how to:

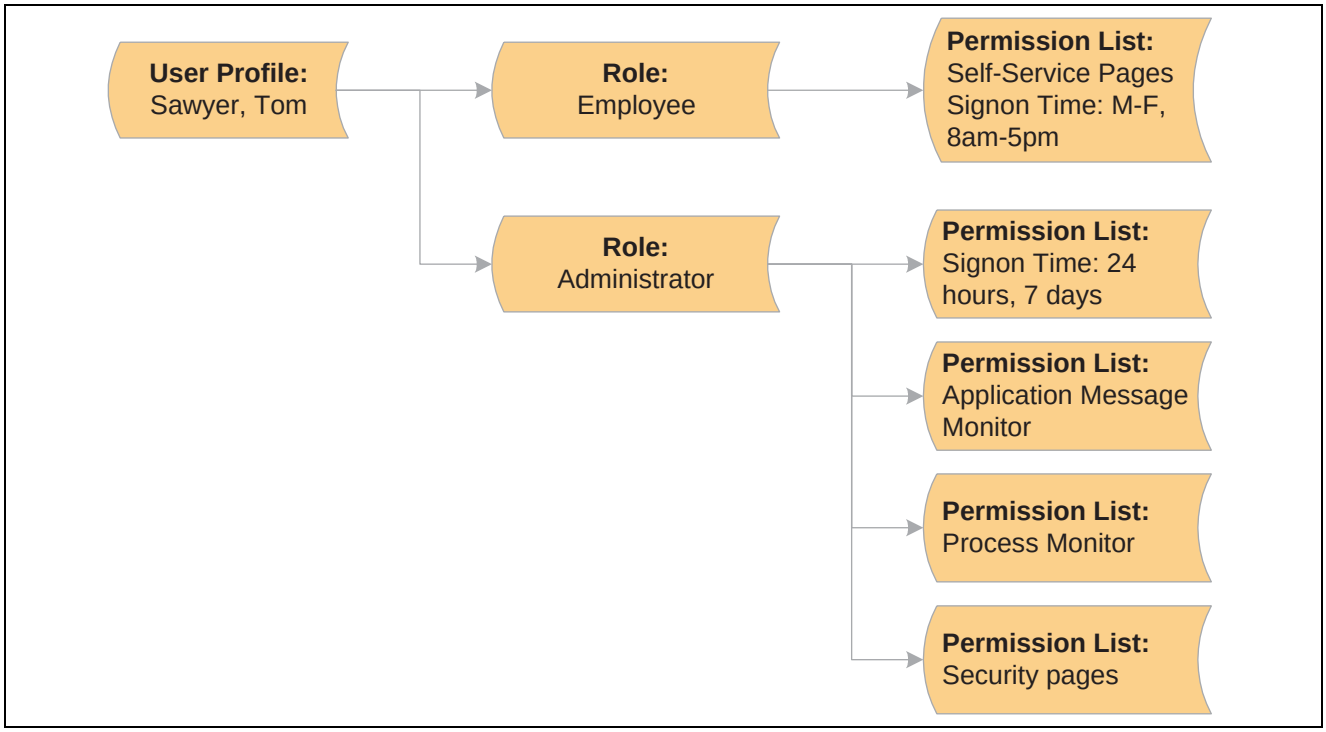
- Manage permission lists.
- Define permissions.

Understanding Permission Lists

Permission lists are the building blocks of user security authorizations. You typically create permission lists before you create user profiles and roles. When defining permission lists, however, consider the roles and user profiles with which you will use them. Recall that roles are intermediary objects between permission lists and users. You use roles to assign permissions to users dynamically.

Permission lists may contain any number of permissions, such as sign-in times, page permissions, and component interface permissions. Permission lists are more flexible and scalable when they contain fewer permissions.

The following diagram illustrates how 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. A user inherits all permissions assigned to each role to which the user belongs. User access is determined by the combination of all assigned roles.



Security definition hierarchy

The diagram represents the security authorizations of Tom Sawyer. Mr. Sawyer inherits the five permission lists that are assigned to the two roles that are assigned to his user profile. In this example, he has access to the employee self-service pages, the message monitor, PeopleSoft Process Monitor, and PeopleTools Security. If Tom were to become a manager, then the permission lists assigned to the Manager role would be added to his profile.

Theoretically, you could create a permission list tailored for every role, and that permission list could contain a permission for every category, from General to Web Libraries. However, permission lists like this do not scale to encompass roles that might be similar, but not exactly alike. For a similar role, you'd have to create a new role from the beginning. This kind of approach is not efficient for larger, more complicated implementations.

Alternatively, you can use a more modular, or mix-and-match, approach. In this approach, you create numerous, generic permission lists that you can add and remove to role definitions. Suppose you have three 8-hour shifts at your site. Using the modular approach, you could create three different versions of sign-in permissions: one for 6 a.m. to 2 p.m., one for 2 p.m. to 10 p.m., and another for 10 p.m. to 6 a.m. Then, depending on the shift for a particular role, you can easily apply or remove the appropriate permission as needed without affecting any other permissions.

Although how you decide to implement Permission Lists depends on your site's security scheme and your security administrator, the modular approach provides increased scalability. As a general rule, your permission lists should be assigned to roles so that the common user has between 10 to 20 lists. This range represents the best balance of 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 sacrifice flexibility.

Managing Permission Lists

This section discusses how to:

- Create new permission lists.
- Copy permission lists.
- Delete permission lists.
- View related content references.
- Add links.
- Run permission list queries.

Creating New Permission Lists

To create a new permission list:

1. Select PeopleTools, Security, Permissions & Roles, Permission Lists.
2. On the search page, click Add a New Value.
3. In the Permission List edit box, enter the name of permission list to create.

   Note. Permission list names have a 30-character limit. PeopleSoft HCM requires certain naming conventions for permission lists, but PeopleTools does not enforce these application-specific requirements. Therefore, when creating permission lists, keep in mind that PeopleSoft HCM requires primary permission lists to start with PP, and data permission lists to start with DP.

4. From the pages in the Permission List component, select the appropriate permissions.
5. Save your permission list.

Copying Permission Lists

To copy a permission list:

1. Select PeopleTools, Security, Permissions & Roles, Copy Permission Lists.
2. In the search page, search for the permission list that you want to copy (clone), and then click it.

   The Permission List Save As page appears.
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 copy.
4. Click Save.

Note. When copying a permission list, you also copy the access specified for content references by the original permission list. When deleting a permission list, you also remove access to the content references associated with that permission list.

Deleting Permission Lists

To delete a permission list:

1. Select PeopleTools, Security, Permissions & Roles, Delete Permission Lists.
2. On the search page, locate the permission list that you want to delete and click it.

   The Delete Permission List page appears.
3. Click Delete Permission List.

4. Click OK to confirm the deletion, or click Cancel to end without deleting.

Note. This deletes content reference permissions and all references to the permission list (even where referenced in application data).

Viewing Related Content References

This section discusses:

- Viewing content references.
- Synchronizing content references.

Viewing Content References

Select PeopleTools, Security, Permissions & Roles, Permission Lists, Pages to access the Pages page, then click the Edit Components link to access the Component Permissions page.

See Chapter 3, "Setting Up Permission Lists," Setting Page Permissions, page 30.

When you set component permissions and web library permissions, use the View Content References link to view the content references pointing to a given component or script. PeopleTools automatically propagates changes to permission lists to the content references.

When you click the link, the Content References page appears, showing the following:

- Name of the portal.
- Name of the content reference.
- The label.
- Whether or not it is accessible.
- The path.

Synchronizing Permission Lists and Content References

Use the PORTAL_CSS application engine program to synchronize permission lists with content references for the portal. By default, the system synchronizes changes in permission lists with content references; however, after an upgrade or any time when you want to make sure, you can run the PORTAL_CSS program. There is a process definition of the same name.

See *Enterprise PeopleTools 8.45 PeopleBook: Internet Technology*, "Administering Portals," Administering Content References.

Adding Links

Select PeopleTools, Security, Permissions & Roles, Permission Lists, Links to access the Links page.

Use this page to add links 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. If this application-specific setting appears on a page not in PeopleTools, Security, add a link to that page so that anyone updating the permission list can easily navigate to it.

You create your inventory of links to security settings that exist outside of PeopleTools Security using the Security Links page. After being created and assigned to a security definition, such as a permission list, then the links appear in the security definition's list of links.

See Also

Chapter 1, “Getting Started with Security Administration,” Administering Security from Applications, page 8

Running Permission List Queries

Select PeopleTools, Security, Permissions & Roles, Permission Lists, Permission List Queries to access the Permission List Queries page.

Permission list queries enable you to run queries that provide detailed information regarding a permission, such as the user IDs and roles associated with a permission list. The available queries are documented on the page.

To run a permission list query:

1. Click the link associated with the query you want to run.

   This invokes a new browser window.

2. View the information the query returns, or select a download option.

   For downloading, you have the following options:

   • Microsoft Excel spreadsheet.

     Downloads the query results as a MicrosoftExcel spreadsheet (.XLS) file.

   • CSV text file.

     Downloads the query results as a comma-separated values (CSV) file.

Defining Permissions

This section discusses how to:

- Set general permissions.
- Set page permissions.
- Set PeopleTools permissions.
- Set process permissions.
- Set sign-in time permissions.
- Set component interface permissions.
- Set message monitor permissions.
- Set web library permissions.
- Set personalization permissions.
- Set query permissions.
- Set mass change permissions.
- View when a permission list was last updated.

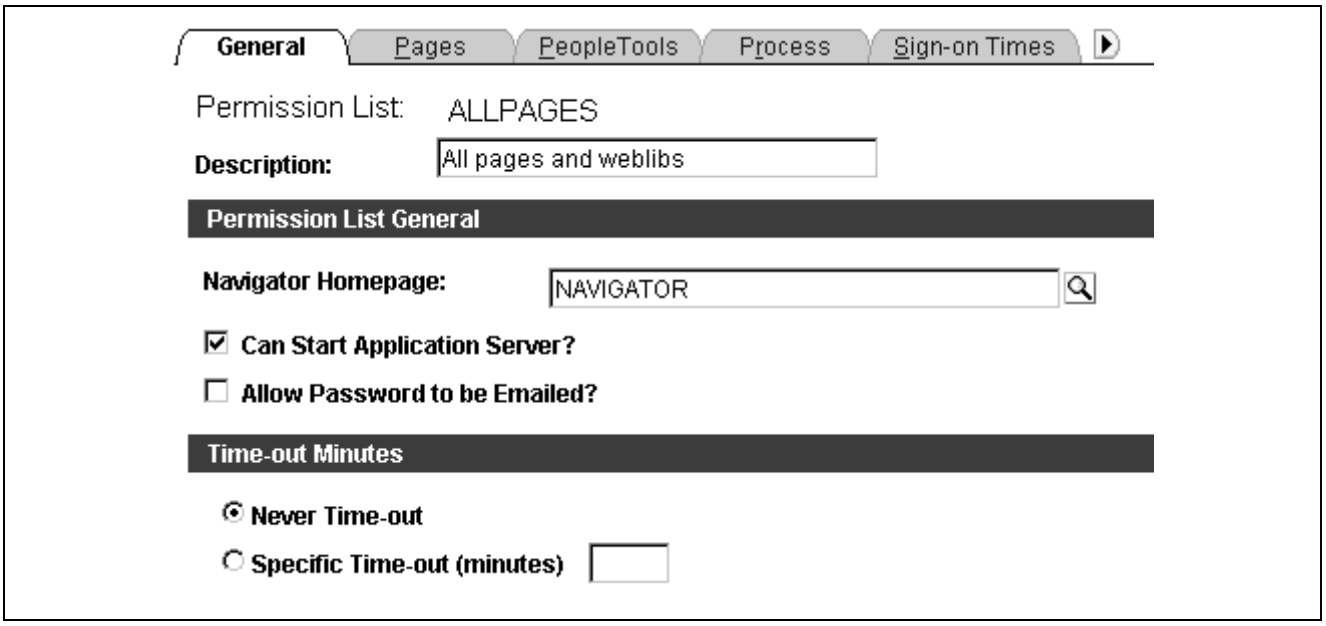
Pages Used to Define Permission Lists

Page Name	Object Name	Navigation	Usage
General	ACL_GENERAL	PeopleTools, Security, Permissions and Roles, Permission Lists, General	Set general or miscellaneous attributes and system defaults.
Pages	ACL_MENU2	PeopleTools, Security, Permissions and Roles, Permission Lists, Pages	Set page permissions.
PeopleTools	ACL_MISCTOOLS	PeopleTools, Security, Permissions and Roles, Permission Lists, PeopleTools	Grant access to PeopleTools applications, such as PeopleSoft Application Designer, and grant access for specific operations within PeopleTools.
Process	ACL_PROCESS	PeopleTools, Security, Permissions and Roles, Permission Lists, Process	Specify to what capacity a user or role can modify PeopleSoft Process Scheduler settings.
Sign-on Times	ACL_SIGNON2	PeopleTools, Security, Permissions and Roles, Permission Lists, Sign-on Times	Specify when users are authorized to sign in to the PeopleSoft system. If users are signed in to the system when the sign-in time expires, they are automatically signed out.
Component Interface	ACL_COMP_INTERFACE	PeopleTools, Security, Permissions and Roles, Permission Lists, Component Interface	Grant access to any component interfaces that a user may need to use to complete business transactions.
Message Monitor	ACL_MESSAGEMONITOR	PeopleTools, Security, Permissions and Roles, Permission Lists, Message Monitor	Set permissions for administrators to monitor the messages and components involved in the application messaging system.
Web Libraries	ACL_WEBLIBS	PeopleTools, Security, Permissions and Roles, Permission Lists, Web Libraries	Set web library permissions.
Personalizations	PLIST_OPTN	PeopleTools, Security, Permissions and Roles, Permission Lists, Personalizations	Set which personalizations your users can use and which they can customize.
Query	PERMLIST_QUERY	PeopleTools, Security, Permissions and Roles, Permission Lists, Query	Control the query operations a user can perform and the data they can access while using PeopleSoft Query.

Page Name	Object Name	Navigation	Usage
Mass Change Operator Security	MC_OPR_SECURITY	PeopleTools, Security, Mass Change Operator Security	Set mass change security permissions.
Audit	PERMLIST_AUDIT	PeopleTools, Security, Permissions and Roles, Permission Lists, Audit	Inquire when a permission list was last updated and by whom.

Setting General Permissions

Access the Permission Lists - General page.



Permission Lists - General page

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

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

Can Start Application Server? Select to enable user profiles with this permission list to start PeopleSoft application servers.

Note. This setting also applies to starting PeopleSoft Process Scheduler servers.

Typically, you'll create a user profile that's dedicated to starting application servers. When you define an application server domain, one of the parameters you specify in PSADMIN is the PeopleSoft user ID (and password) for that profile, which must be associated with at least one permission list that has this option enabled. The user ID and password are stored in the Startup section of the PSAPPSRV.CFG file, which BEA Tuxedo reads when the application server is started.

In many installations, an application server starts with an automated process. A user profile with this property enabled shouldn't be used

by an actual user who signs in to the application server and starts it by submitting the appropriate commands.

Note. Password controls don't apply when a password is used for two-tier activities like starting application servers. They apply only when the password is used to sign in over three-tier connections.

Important! For a given user profile, the password controls that you set for account lockout (maximum logon attempts) and age (expiration) apply to three-tier and web sign-in only, and don't apply if the user profile is used just for two-tier activities like starting an application server or process scheduler.

However, make sure that you don't use the same user profile for both types of activities. When you use it for three-tier and web sign-in, it becomes subject to the account lockout and age controls, which will prevent it from completing the two-tier activities.

Allow Password to be Emailed? Select to allow users to receive forgotten passwords through email. At some sites, the security administrator may not want passwords appearing unencrypted in anyone's email. You implement this feature by permission list. None can use it, some can use it, or all can use it depending upon your implementation. Users who do not have the proper authority receive an error message if they attempt to have a new password emailed to them.

Never Time-Out and **Specific Time-out (minutes)** Select the number of minutes of inactivity allowed at a terminal before the system automatically signs the user out of the PeopleSoft online system. Inactivity means no mouse clicks, keystrokes, import, file print, or SQL activity. The default time-out minutes setting is Never Time-out.

Note. Time out limits are also controlled at the web server and application server level.

If you select Never Time-out, an inactive user is never automatically signed out. Otherwise, select Specific Time-out (minutes) and enter the appropriate value in minutes. Keep the following in mind while entering a custom time-out interval:

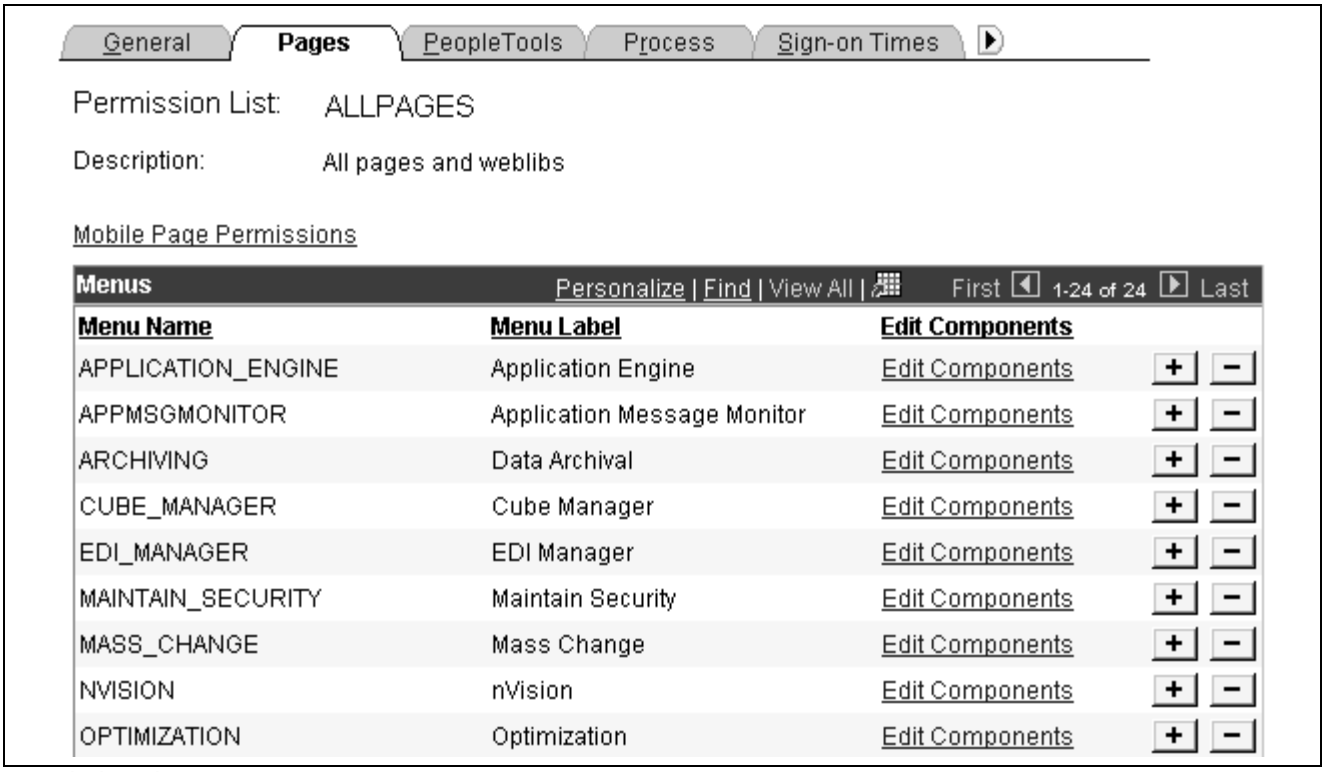
- It must be a positive integer.
- It must not contain edit characters, such as commas or a $.
- It must be a SMALLINT in the valid range allowed for this field (0-32767).
- Entering a value of zero (0), is equivalent to selecting Never Time-out.

To comply with the Americans with Disabilities Act (ADA), you might have most permission lists set up to time out in 20 minutes, but have a special ADA permission list for some users where timeout only occurs after 60 minutes.

Note. Keep in mind that you'll need to set higher web server timeouts.

Setting Page Permissions

Access the Permission Lists - Pages page.



Permission Lists - Pages page

Mobile Page Permissions Click to grant access to mobile application pages.

Menu Name Displays all menu names in the database. Add new rows to add more menu names. The name reflects the definition name in PeopleSoft Application Designer.

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

Edit Components Click to grant access to specific pages.

Page permissions refer to the pages to which a user has access. Pages are contained within components, which are ultimately contained within a menu name. To grant access to a particular page, determine the component it is in and the menu name the component falls under. This enables you to drill down to the appropriate page.

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

Granting access to PeopleTools and PeopleSoft applications requires serious considerations. For each role, carefully consider what the members of that role must access to complete their jobs and to what degree they need access. Then make the appropriate permission lists.

After you add a menu name, you grant access to its components and pages on an item-by-item basis. In PeopleSoft applications, menu items represent components. If a component consists of more than one page, then selecting the menu item opens another layer with more items—individual pages. For example, if you added the UTILITIES menu name to a permission list, you could then 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 make some items display only.

There are two categories of components to which you grant access permission:

- All PeopleSoft applications.
- Page-driven PeopleTools.

Note. With PeopleTools programs, the process of editing menu items varies. With page-based PeopleTools, such as PeopleSoft Process Scheduler, you can grant access to menu items just as you can for PeopleSoft applications. However, the other 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. PeopleSoft Application Designer is an exception; you can restrict access to it at the definition level.

Granting Access to Components and Pages

The following procedure describes how to set access permissions to your PeopleSoft applications and your page-driven PeopleTools. You begin at the component level and drill down to the page level making the appropriate selections as you go.

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

To add access to PeopleSoft components and pages:

1. Locate the menu name of the component to which you want to add access.
2. Click Edit Components.

   This takes you to the Components page.
3. Locate the component to which you want to grant access.

   By default, when adding a new permission list, no components are authorized.
4. 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 determine the actions that a user can complete on the page. You have the following options for each page that appears in the Page column:

   - Authorized?

     Select to enable a user to access the page. 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.

     Select to enable the user to view the information provided by the page, but not to alter any data.
   - Actions.

     Determine how users can alter information on a page, such as Add, Update/Display, and Correction. The options that are available depend upon the options selected when the page was initially developed in PeopleSoft Application Designer.

     To grant access to all pages and all actions for each page, click Select All.
5. When you have finished making the appropriate selections, click OK on the Page Permissions page and then again on the Component Permissions page.

   For each menu name, repeat each step.

Note. After you delete access to a component or iScript, you must clear the browser cache or wait for 20 minutes (default time) for the deletion to appear on the menu.

Granting Access to Mobile Pages

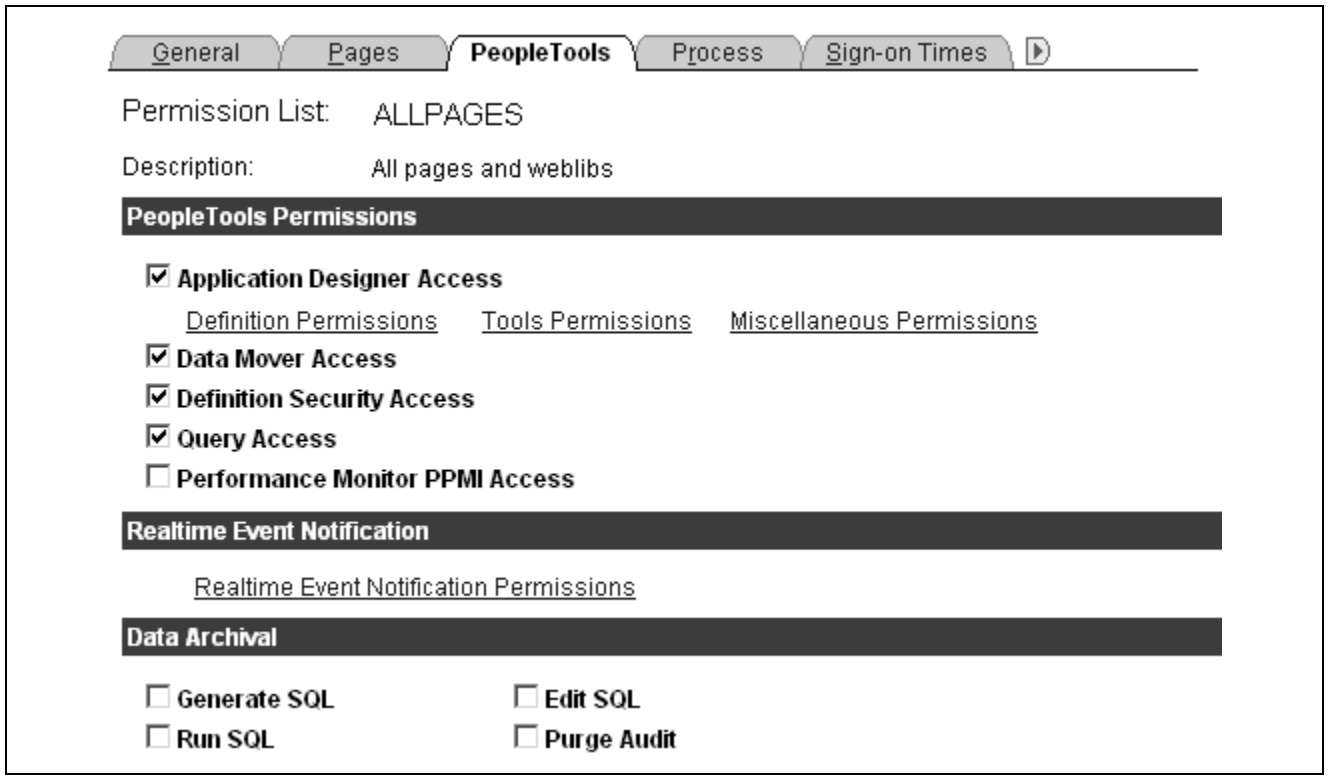
To add access to mobile pages:

1. Select PeopleTools, Security, Permissions & Roles, Permission Lists, and select the Pages page.
2. Click the Mobile Page Permissions link.

   This takes you to the Mobile Page Permissions page.
3. To add a new mobile page to the permission list, click the plus sign.
4. For the Mobile Page Name edit box, click the search button.
5. Search for and select the mobile page for which you need to grant access.
6. Click OK.
7. Save the permission list.

Setting PeopleTools Permissions

Access the Permission Lists - PeopleTools page.



Permission Lists - PeopleTools page

The PeopleTools Permissions section of this page applies to standalone PeopleTools applications. They aren't PIA-based, but are Windows programs that weren't developed using PeopleSoft Application Designer. They include:

- PeopleSoft Application Designer
- PeopleSoft Data Mover
- PeopleSoft Definition Security

• PeopleSoft Query (Windows interface, not the browser interface)

The Performance Monitor PPMI Access check box doesn't control access to an application; rather, it enables PeopleSoft Performance Monitor data collators to insert performance data into the database, which enables you to view the data.

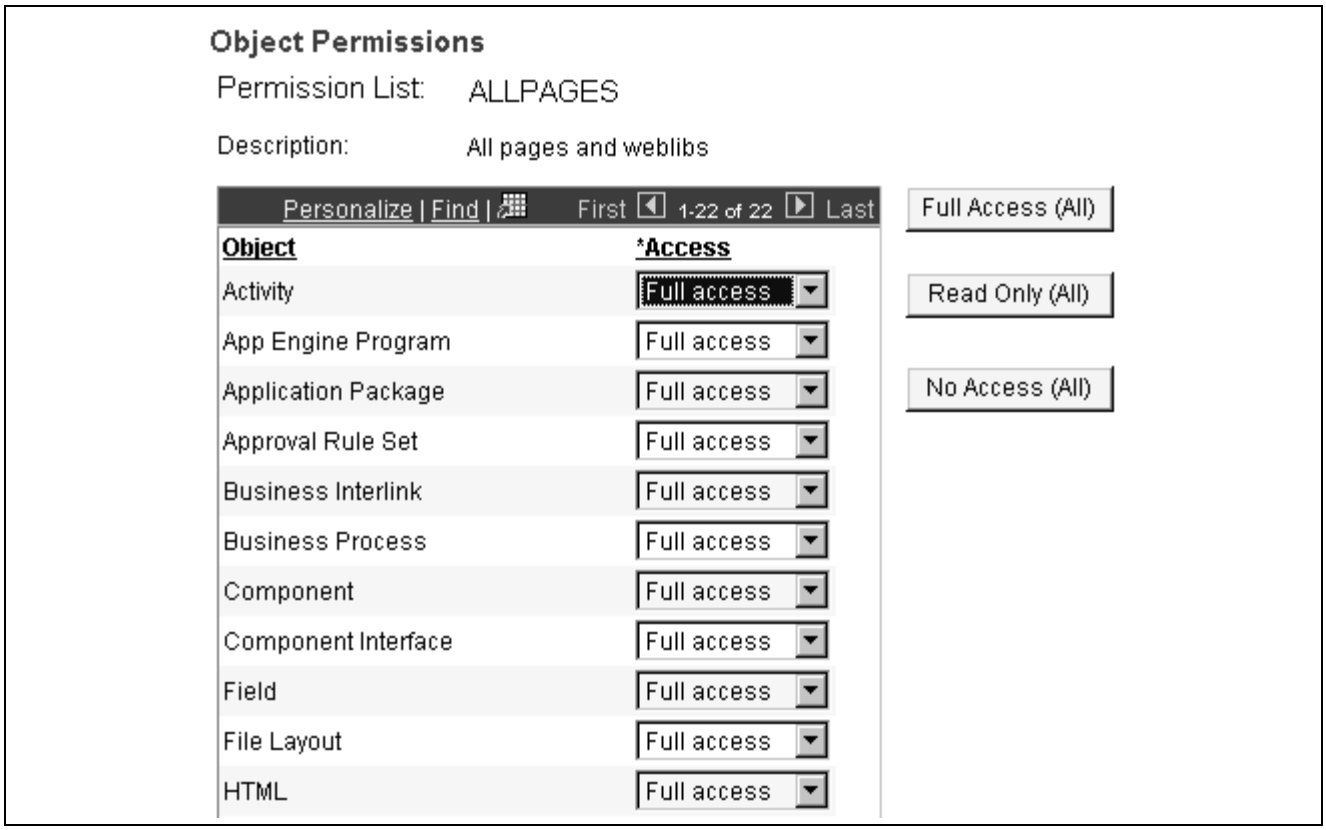
See *Enterprise PeopleTools 8.45 PeopleBook: PeopleSoft Performance Monitor*.

To grant access to these PeopleTools features, select the check box next to the appropriate item.

With PeopleSoft Application Designer, the procedure for applying permissions is slightly more complex, because security for PeopleSoft Application Designer also controls what object definition types can be accessed and what degree of modifications can be made. The links on this page (Definition Permissions, Tools Permissions, and Miscellaneous Permissions) enable you to provide more detail to PeopleSoft Application Designer access permissions.

Definition Permissions

Select Definition Permissions to access the Object Permissions page.



Object Permissions page

Grant access to the definitions that developers create using PeopleSoft Application Designer. Each type of object that you define with PeopleSoft Application Designer appears in the object permissions list.

Note. Here, you add permissions to an object type, such as application engine programs. You grant access to specific objects, such as PeopleSoft Payroll application engine programs, using Definition Security.

Access Select the appropriate access level. Options are:

Full Access: Definitions of the specified type can be modified. For records, this setting allows access to the Build dialog box.

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 applies only to fields. This allows a user to modify only Translate table values.

Data admin only: This level applies only to records. It allows a user to modify only those record attributes found in the Tools, Data Administration menu (tablespaces, indexes, and record DDL).

Full Access (ALL), Read Only (ALL) and **No Access (ALL)** — Click to set all object types in the list to the same access level.

Note. If change control locking is enabled, the Change Control access setting on the Tools Permissions page can override object types settings.

See *Enterprise PeopleTools 8.45 PeopleBook: PeopleSoft Application Designer*, "Using PeopleSoft Application Designer," Building and Maintaining Data.

Tools Permissions

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

The tools within PeopleSoft Application Designer include the following:

- Build/Data Admin (select Build, Project and Tools, Data Administration).
- Change Control (select Tools, Change Control).
- Language Translations (select Tools, Translations).
- PeopleCode Debugger (select Debug, PeopleCode Debugger Mode).
- SQL Editor (the PeopleSoft Application Designer utility for adding SQL objects and statements to applications and application engine programs).
- Upgrade (select Tools, Upgrade).

  This includes Copy Project, Compare and Report, and so on.

You can set the access level individually for the Tools Permissions page options or your can use the (ALL) buttons to set across the board settings. Remember that every button affects every access level for the tools.

Build/Data Admin — Control access to the Build and Tools, Data Administration menu items. Select from:

- No access. The 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 box options, but the Execute SQL now and Execute and build script options are disabled. The Tools, Data Administration menu items are not available.

  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 not available

  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.

Change Control The change control access levels are valid only when change control is enabled. You enable change control locking using PeopleSoft Application Designer. Select from:

- Restricted access. Restricts users from locking or unlocking objects. When change control locking is enabled, users with restricted access can only view PeopleSoft Application Designer definitions—they cannot create, modify, or delete them.

  Note. With locking enabled, this setting overrides any *Full Access* settings on the Object Permissions page or Miscellaneous Permissions page.

- Developer access. The user can lock any unlocked objects and unlock any objects that he or she has locked.
- Supervisor access. The user can unlock any locked objects, regardless of who has locked them.

Language Translations Set only two levels of access, No access and Full access. Enable this set of menu options for people involved in translating or globalizing your applications.

PeopleCode Debugger Restrict access to the PeopleCode Debugger.

SQL Editor Restrict developers from modifying the SQL in your applications.

Upgrade Select No access to make all the Upgrade menu items on the Tools menu unavailable. Developers can still access the Upgrade view and modify upgrade settings in the project definition, but they cannot run any the upgrade processes.

With Read-only access, users can run compare reports against the database, but they cannot copy objects into the database.

The following table shows the relationship between the permissions that are set up within the source and the target databases, which you should consider in upgrade situations.

Source DB	Target DB	Compare?	Copy?	Export?	Import?
No Access	No Access	No	No	No	No
No Access	Read-only Access	No	No	No	No
No Access	Full access	No	No	No	No
Read-only Access	No Access	No	No	Yes	No
Read-only Access	Read-only Access	Yes	No	Yes	No
Read-only Access	Full access	Yes	Yes	Yes	No
Full access	No Access	No	No	Yes	Yes
Full access	Read-only Access	Yes	No	Yes	Yes
Full access	Full access	Yes	Yes	Yes	Yes

Miscellaneous Permissions

Set access levels for the Miscellaneous Definitions items that appear in the PeopleSoft Application Designer Tools menu, including Access Profiles, Color, Field Format, Style, and Tool Bar.

Each of the miscellaneous definitions can be set for No access, Read-only, or Full access. You can select the (ALL) buttons to grant the same permissions to each item.

Realtime Event Notification Permissions

Select this link to access the REN Permissions (Realtime Event Notification Permissions) page.

See *Enterprise PeopleTools 8.45 PeopleBook: PeopleSoft MultiChannel Framework*, "Configuring REN Servers," Configuring REN Server Security.

Data Archival

Use the PeopleSoft Data Archive Manager application to archive your data as part of regular database maintenance. The security options in this group relate specifically to actions a system administrator would make while using PeopleSoft Data Archive Manager. The actions that a system administrator can perform within PeopleSoft Data Archive Manager are controlled by permission lists. Before you grant any permissions to these actions, read the PeopleSoft Data Archive Manager documentation.

Note. PeopleSoft Data Archive Manager is a page-driven PeopleTools application, but on this page you enable specific operations used within the archiving process.

See Also

Enterprise PeopleTools 8.45 PeopleBook: Data Management, "Using PeopleSoft Data Archive Manager"

Setting Process Permissions

Just as you define permissions for the pages a user can access, it is also critical to specify the batch (and online) processes that users can invoke through PeopleSoft Process Scheduler. Typically, process groups are arranged by department or task. For example, the batch programs having to do with your payroll department probably all belong to the PAYROLL process group, or something similar.

When you create a process permission list, you add the appropriate process groups so that a user belonging to a particular role can invoke the proper batch programs to complete their business transactions. You do this using the Process Group Permission page.

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

Note. The Process Profile is granted to the user by way of the user profile, and the Process Group is granted to the user by way of a permission list.

Process Group Permissions

Access the Process Groups page.

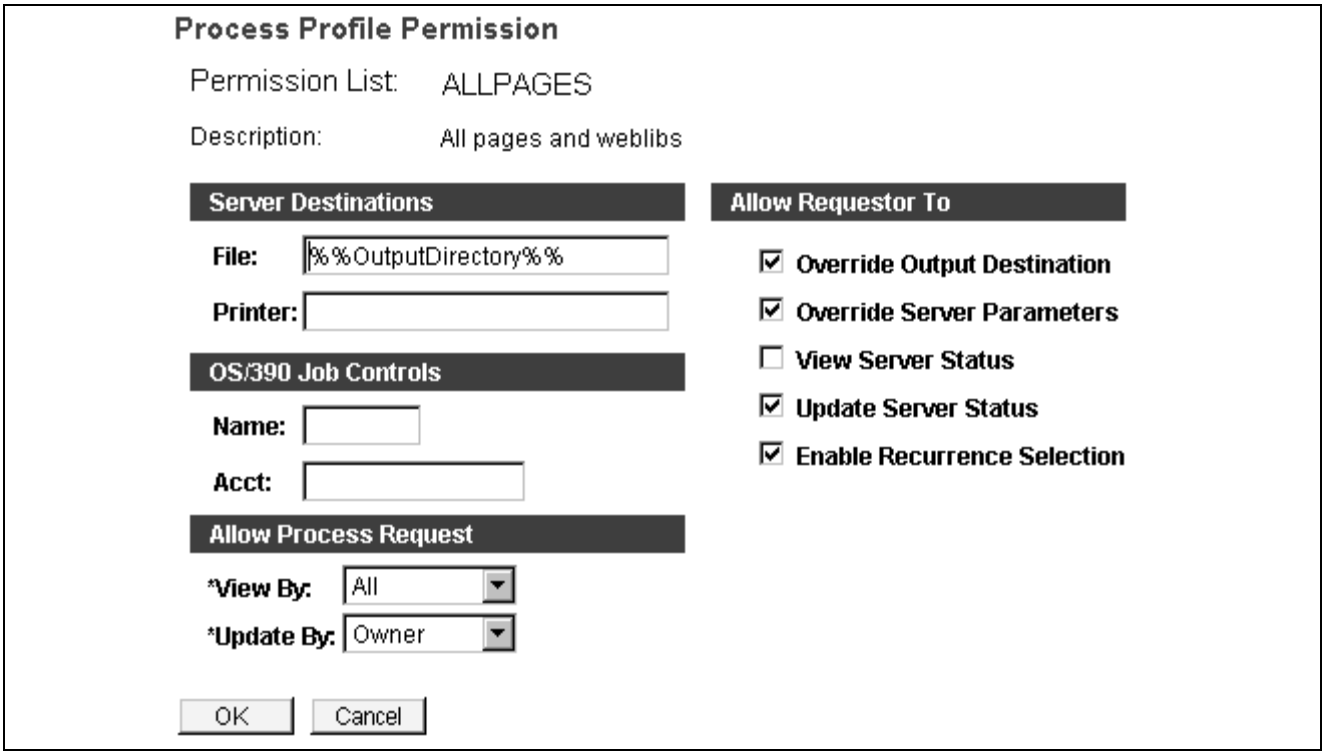
This page lists the process groups associated with a permission list. Process groups are collections of process definitions that you create using PeopleSoft Process Scheduler.

Typically, you group process definitions according to work groups within your organization, and typically that work group has a particular role associated with it. Regardless of how you organize process definitions, you must assign process groups to a permission list.

Users can run only the processes that belong to process groups assigned to their roles. For instance, you may have a set of process definitions that relate to your Human Resources department and another set for your Manufacturing department.

Process Profile Permissions

Access the Process Profile Permission page.



Process Profile Permission page

Server Destinations

You can specify output variables when running processes or jobs on a server. You have the following options:

- File.

  If the output is going to a 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 must explicitly specify the printer; there are no meta-variables available for this value.

OS/390 Job Controls

Note. This group of options applies only to DB2 for OS/390 and z/OS.

All PeopleSoft Process Scheduler shell JCLs use meta-strings to pass data stored in the database. PeopleSoft 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%*.

See your relational database management system documentation and the PeopleSoft installation guides for details about JCL meta-variables and strings.

Allow Process Request

These options apply to using PeopleSoft Process Monitor. You can restrict which users are permitted to view or update a given process, based on the user who launched (and owns) the process. You can specify restrictions as follows:

- View by.

  Specify who can view processes that are launched by users who have this permission list assigned as their process profile permission list on the User Profile - General page.

  Select from the following options:

  - *Owner:* For a process that's launched by a user who has this process profile permission list assigned, only the user who launched the process can view it.
  - *All:* All users can view processes that are launched by a user who has this process profile permission list assigned.
  - *None:* No one can view processes that are launched by a user who has this process profile permission list assigned.

- Update By.

  Specify who can update the status of processes that are launched by users who have this permission list assigned as their process profile permission list on the User Profile - General page. For example, you decide whether users can restart or cancel a request.

  Note. Updates are made using the PeopleSoft Process Monitor Process Detail page in the Update Process component.

  Select from the following options:

  - *Owner:* For a process that's launched by a user who has this process profile permission list assigned, only the user who launched the process can update it.

    For example, nobody else can restart a request that this user submitted. However, this user might still be able to update another user's processes.
  - *All:* All users can update processes that are launched by a user who has this process profile permission list assigned.
  - *None:* No one can update processes that are launched by a user who has this process profile permission list assigned.

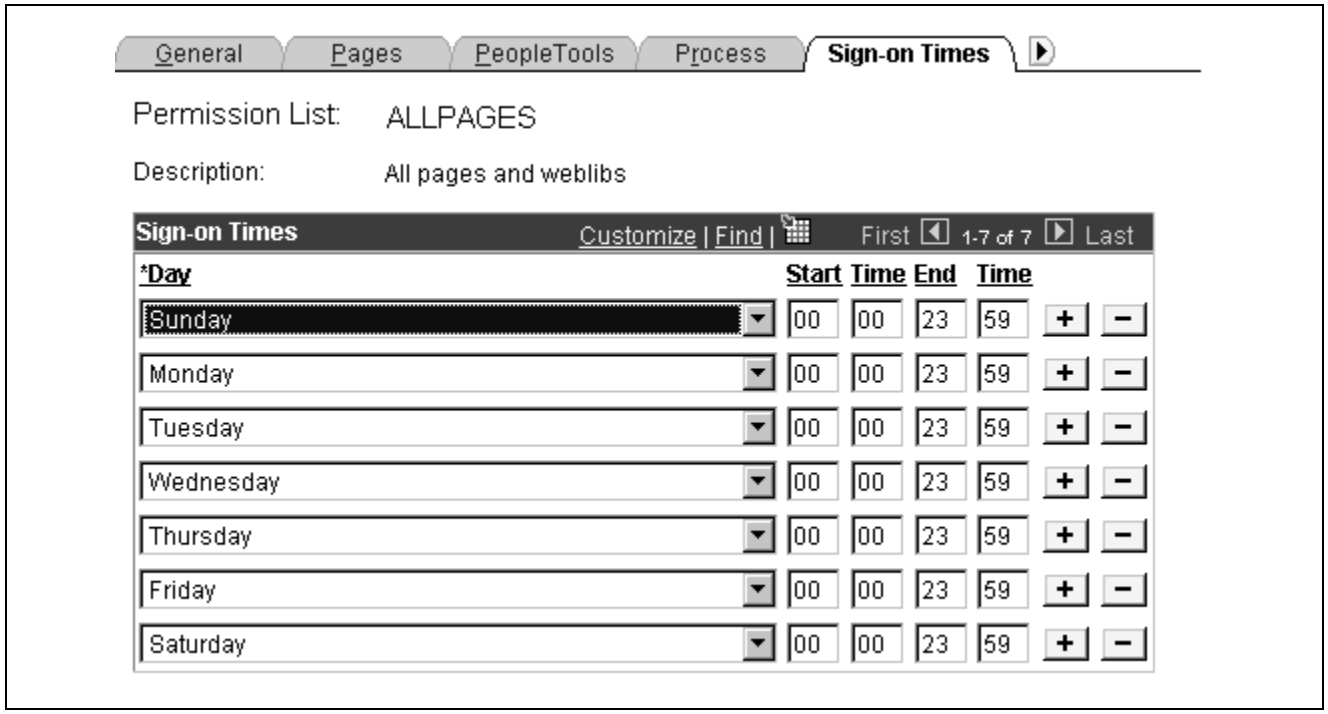
Note. Be careful as you grant update authority to submitted processes. An inexperienced user can easily disrupt batch processing by deleting or holding processes. This is especially true with restarting processes. If a program is not coded for a restart, then users should not be able to restart it. Restarting a program that is not properly coded to acknowledge the previous program run can threaten data integrity. Remember, the process profile permissions are based on the profile of the user who is submitting the process, not the user viewing the process monitor.

The Allow Requestor To options apply to using PeopleSoft Process Monitor and PeopleSoft Process Scheduler Request pages. These options enable you to restrict the authority that a user has while monitoring scheduled processes.

Override Output Destination	Select to allow a user to change the value in the Output Destination column on the Process Scheduler Request page.
Override Server Parameters	Select to enable users to select the server name and modify the run date/time group on the Process Scheduler Request page.
View Server Status	Select to enable users to access the Server List page in PeopleSoft Process Monitor.
Update Server Status	Select to allow a user to suspend, restart, or bring down a server using the Server Detail page from the server list in PeopleSoft Process Monitor.
Enable Recurrence Selection	Select to enable a run recurrence value for processes and jobs scheduled to run on the server.

Setting Sign-in Time Permissions

Access the Permission Lists - Sign-on Times page.



Permission Lists - Signon Times page

Pick a day and set a sign-in duration.

Sign-in 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 p.m.

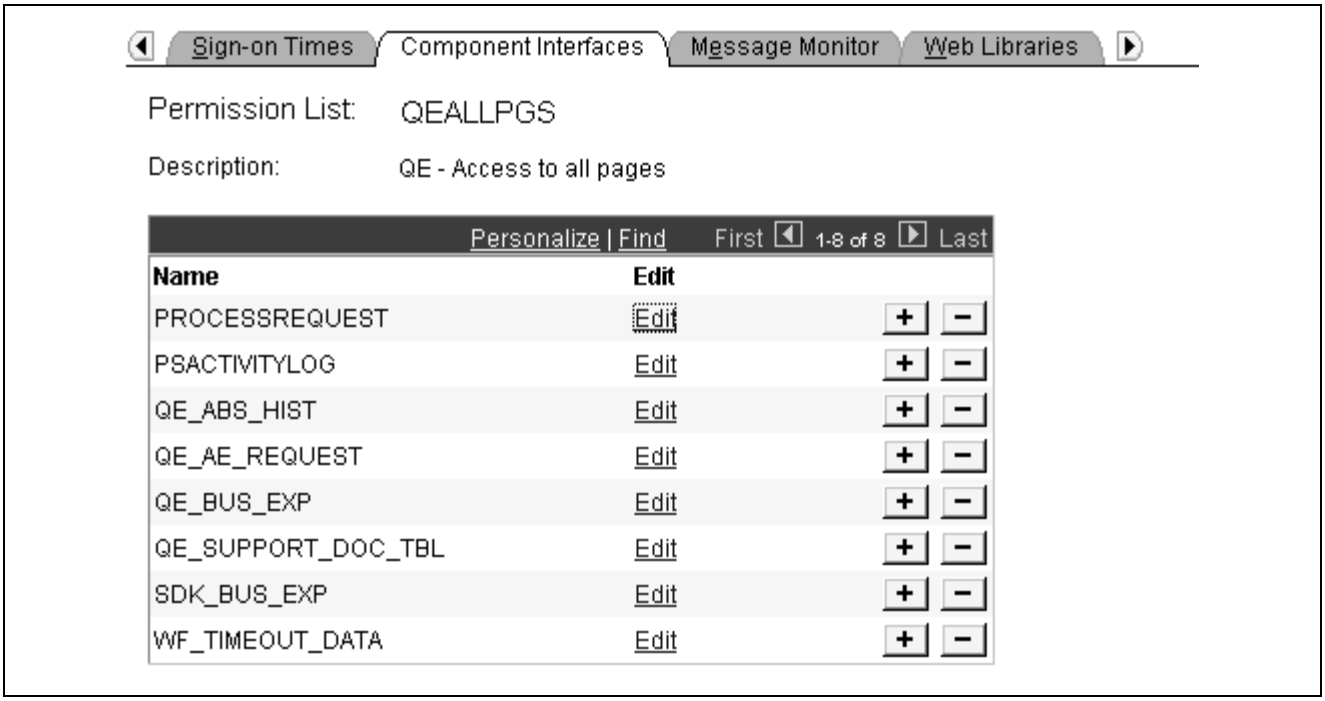
To create a sign-in time that spans multiple days, use adjoining sign-in times. For example, to create a sign-in time running from 8 p.m. Tuesday to 6 a.m. Wednesday, you need a Tuesday start time of 20:00 and end time of 23:59. Then you need to add a Wednesday sign-in time with a start time of 0:00 and an end time of 5:59.

By default, all start times are 0:00 and end times are 23:59, and all days are listed. Delete days and change the times to restrict access.

A single day can have more than one sign-in period as long as the periods don't overlap. If there are multiple non-overlapping sign-in periods for one day, that day appears once for each period.

Setting Component Interface Permissions

Access the Permission Lists - Component Interfaces page.



Permission Lists - Component Interfaces page

Name Shows the name of the component interface.

Edit Click to access the Component Interface Permissions page and grant access to a particular component interface method.

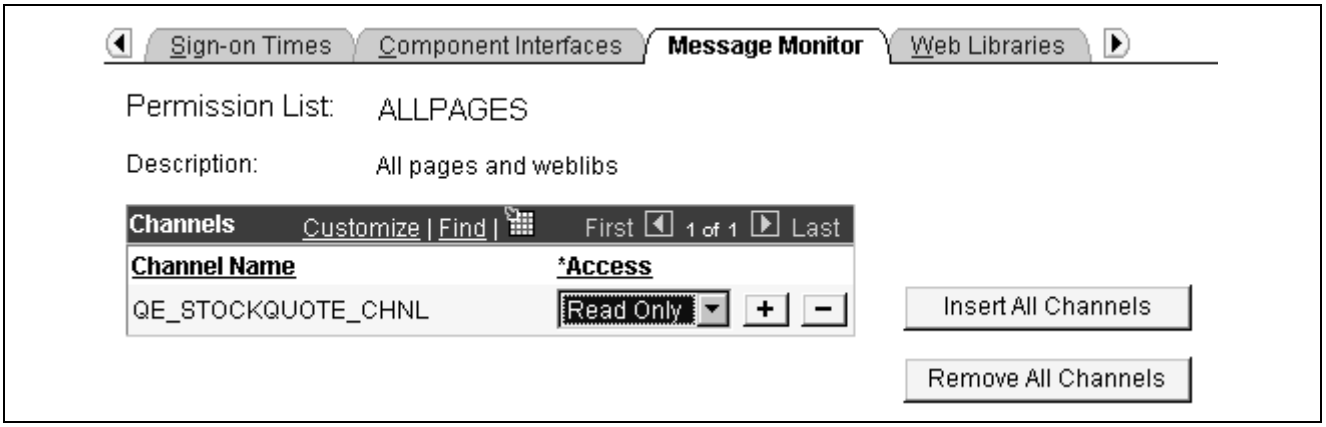
You grant access to component interfaces similarly to adding page access. Add a new row to insert a component interface into the definition list. You must also grant access to the component interface methods.

After adding a new permission to a component, you must delete the web server cache for users to access the component through the portal. To delete the web server cache, reboot the web server.

Note. If more than one JVM services the web server, rebooting the web server only purges the in-memory cache. No procedure exists to specify which JVM receives the request. For this reason, you must reboot all JVMs that service the web server.

Setting Message Monitor Permissions

Access the Permissions Lists - Message Monitor page.



Permission Lists - Message Monitor page

Administrators use the PeopleSoft Integration Broker message monitor to monitor messages and components involved in messaging. You add access to the message monitor using the Pages page, but after you add access to the message monitor, you must customize user access to your channels. You use the Message Monitor Permissions page to enable an administrator to view or edit messages within a particular channel.

Channel Name Displays the name of the message channel.

Access Select the degree of access. Select from:

Full: An administrator can view and edit messages within the channel.

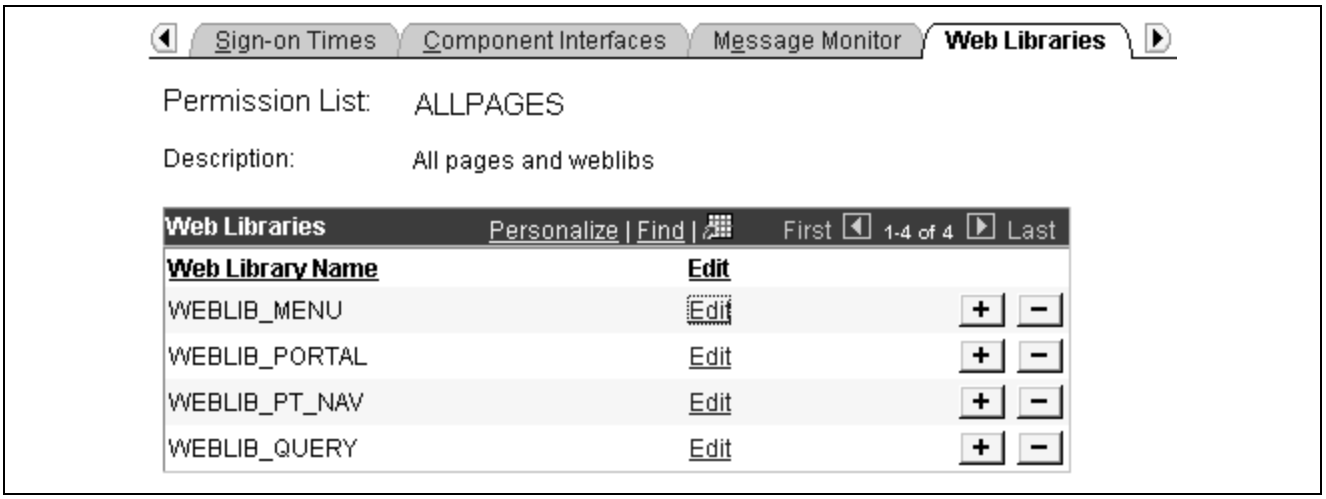
Read Only: The administrator can view, but not edit, messages within the channel.

Insert All Channels Inserts all channels in the database.

Remove All Channels Removes all items from the message channel list.

Setting Web Library Permissions

Access the Permission Lists - Web Libraries page.



Permission Lists - Web Libraries page

A web library is a derived/work record whose name starts with WEBLIB_. All PeopleSoft iScripts are embedded in records of this type. An iScript is a specialized PeopleCode function that generates dynamic web content.

Administrators should make sure that users have the proper access to web libraries. For example, the default navigation system for PeopleSoft Internet Architecture 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 have proper access to the system. If users are not authorized for a particular web library or script, then they can't invoke it.

After you add a web library, you set the access for each script function individually. Invoking an iScript requires the assembly of a URL. Developers assemble the URL using PeopleCode.

Web Library Name Displays the web libraries added to the permission list.

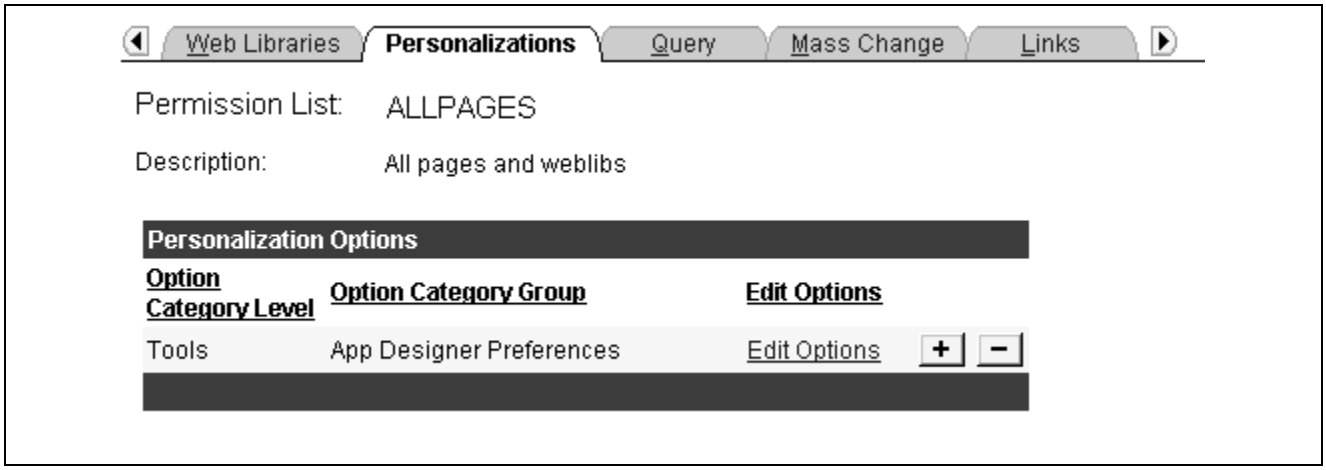
Edit Click to set access to web library functions. Select access rights for each function.

See Also

Enterprise PeopleTools 8.45 PeopleBook: PeopleCode Developer's Guide, "PeopleCode and PeopleSoft Pure Internet Architecture," Using Internet Scripts

Setting Personalization Permissions

Access the Permission Lists - Personalizations page.



Permission Lists - Personalizations page

Note. Only those personalization options that accept customization are available for your users to modify.

Option Category Level Displays the high-level grouping of personalizations.

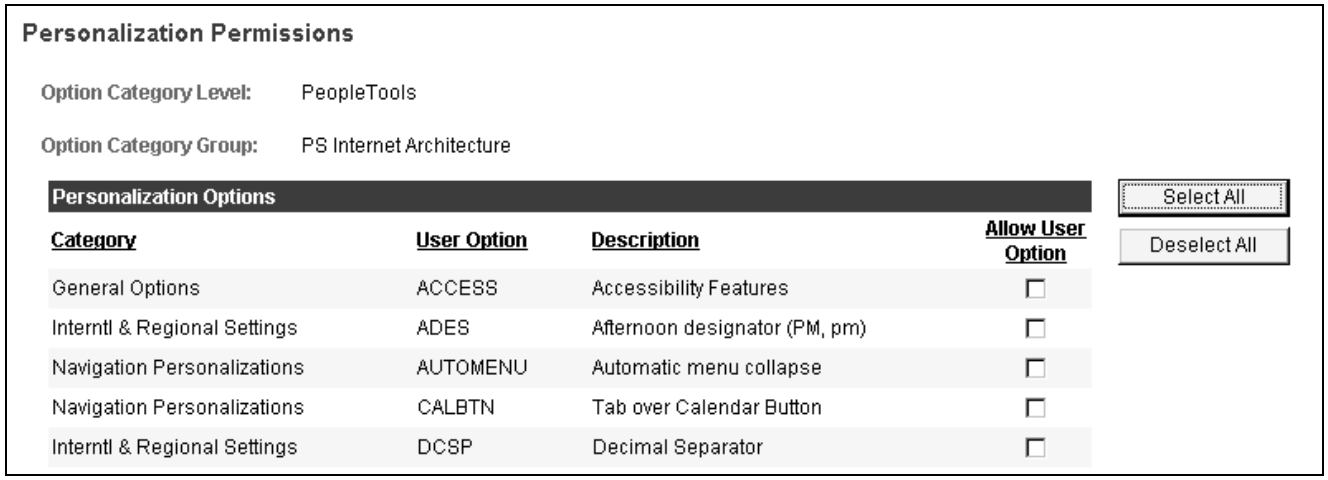
Option Category Group Shows the further categorizations of personalization options within the category level.

Edit Options Click to access the Personalization Permissions page and enable specific personalization options for an option catgory group.

See Chapter 12, "Managing PeopleSoft Personalizations," page 199.

Personalization Permissions

Click Edit Options for an option category group on the Permission Lists - Personalizations page to access the Personalization Permissions page.



Personalization Permissions page

Enable a particular user personalization option for a permission list.

Category Displays the category or type of personalization option.

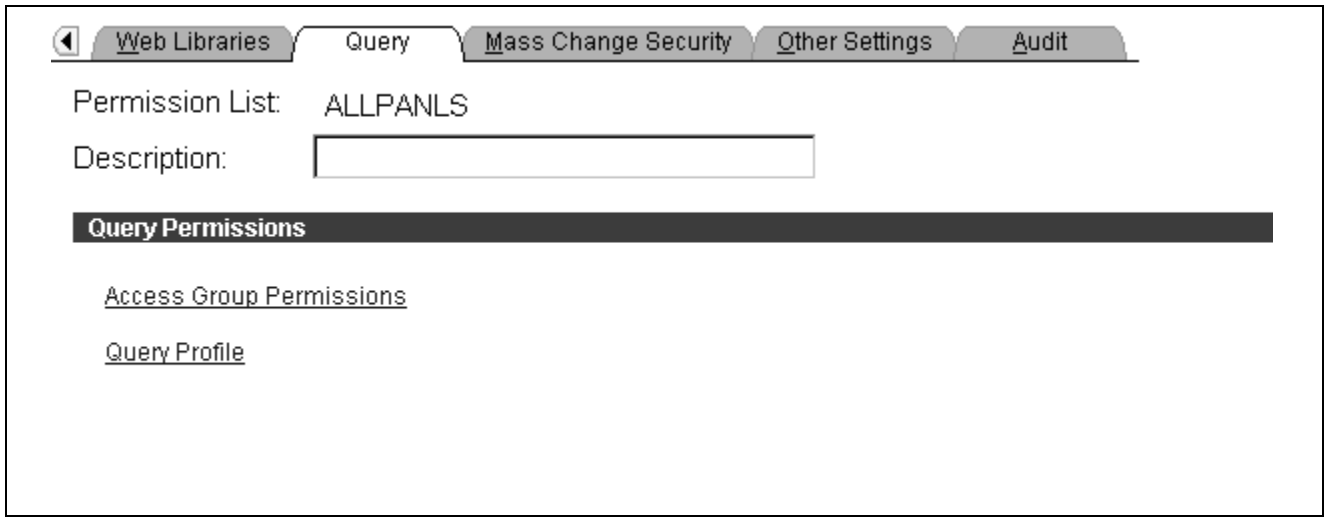
User Option Displays the internal code name associated with the personalization option.

Description Displays the text that the users see on the My Personalizations page.

Allow User Option Select to enable the option for a permission list.

Setting Query Permissions

Access the Permission Lists - Query page.

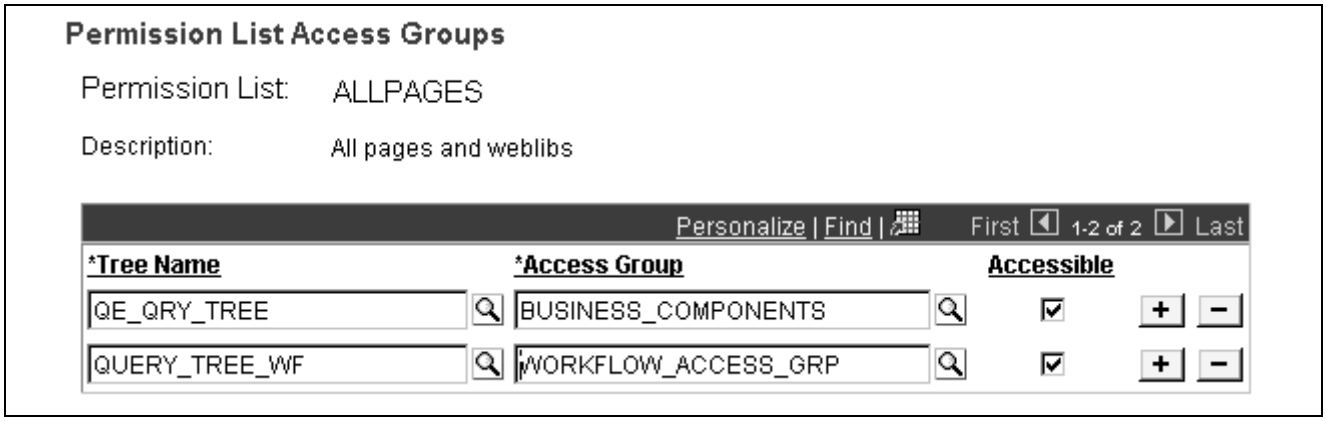


Permission Lists - Query page

The Query page has links to the Access Group Permissions page, where you can define the records to which the user can have access in PeopleSoft Query, and the Query Profile page, where you can define the query operations that the user can perform.

Defining Access Groups

Access the Permission List Access Groups page.



Permission List Access Groups page

Access groups are nodes in a query tree, which you build with PeopleSoft Tree Manager. After 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.

When you open Query Manager, it displays either an access group structure or an alphabetical list of records to which you have access. Access groups enable you to logically organize the record components to control security access within PeopleSoft Query. It is not a physical representation of your database.

You can generate queries on and retrieve information only 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.

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

To add an access group to a permission list:

1. Open the permission list and select Query, Access Groups Permissions.
2. Select a tree name.
3. Select the highest access group that the user can access.

   The system displays access groups in the selected query tree only.

   The access group that you select should be the highest-level tree group to which this permission list needs access. The Accessible check box is selected 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.
4. (Optional) Clear the Accessible check box.

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

Note. Because it hinders system performance, don't clear the Accessible check box for lower-level access groups. To restrict access to record components on a particular branch of a tree, consider creating a new tree for those definitions. Attempting to expand an access group that is not accessible causes all access groups below that access group to be loaded into memory.

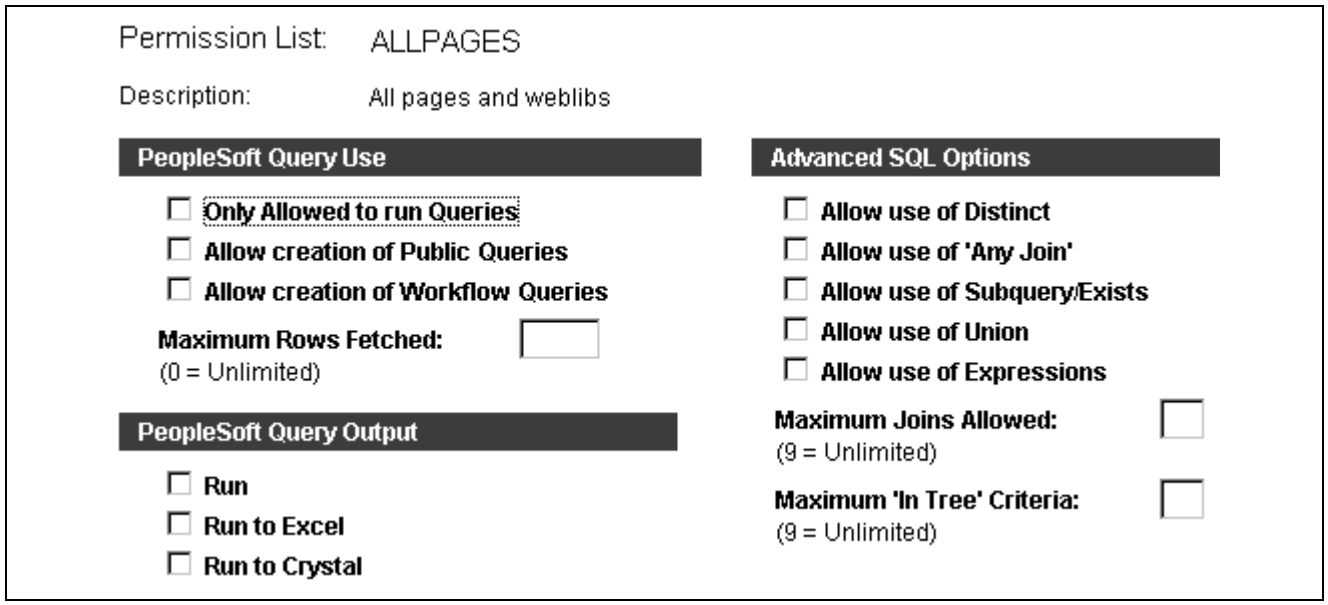
---

5. Save your changes.

Note. When the system loads an access group into memory for the first time, you'll 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, don't group a large number of record components into a single access group.

Defining Query Profiles

Access the Query Profile page.



Query Profile

Query profiles specify available query operations. 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 that users can perform. You control these options through the query profile.

Each permission list has its own query profile, and the combination of all permission lists that are assigned to a role determine the total query access for the role. User profiles inherit query access only through the roles that you assign to them.

The first level of security is access to PeopleSoft Query itself. Not every user needs to create queries. You select at least one of the options in the PeopleSoft Query Use section of this page to give users query access.

PeopleSoft Query Use Select from:

- Only Allowed to run Queries.

  Select to prevent users from being able to create queries and restricts them from running PeopleSoft Query. The values of the remaining options in this group are irrelevant if you have selected this option.

- Allow creation of Public Queries.

  Select to enable users to create public queries.

- Allow creation of Workflow Queries.

Select to enable users to create workflow queries in addition to private queries. A workflow query is used in PeopleSoft Workflow, either as a database agent query or a role query. These queries can circumvent security restrictions; the system doesn't check access group rights while running the query. To make sure that users can't bypass the system's security, clear this check box.

- Maximum Rows Fetched.

  Enter a number to restruct the number of rows retrieved by a query. 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.

PeopleSoft Query Output Select at least one:

- Run.

  PeopleSoft Query displays the query results in a view-only grid control. This option is useful as users are refining their queries.

- Run to Excel.

  PeopleSoft Query passes the query results to Microsoft Excel, where users can analyze the results further.

- Run to Crystal.

  PeopleSoft Query passes the query results to Crystal Reports Pro, a report formatter, where users can select predefined formats or create new ones to print query results.

Note. If using PeopleSoft Query in the Microsoft Windows environment, you grant runtime access through PeopleSoft Navigator by selecting at least one of the PeopleSoft Query output options.

Advanced SQL Options Restrict less experienced users from generating complex queries, as such queries can affect system performance.

Setting Mass Change Permissions

Mass change operator 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 run.

  These definitions must also be based on a template with the same PeopleSoft owner as the user.

Note. Users inherit mass change authorizations through their primary permission lists, not through roles.

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

To modify mass change template permissions:

1. Add or remove templates from the Mass Change Template ID list.
2. Select or clear OK To Execute Online, as needed.

When you have enabled the OK To Execute Online option, users with the given primary permission list can run mass change definitions after saving any modifications to the Mass Change Definitions pages.

3. Save your work.

Viewing When a Permission List Was Last Updated

Access the Audit page.

View when a permission list was last updated and by whom. You can also view who has made changes to security tables by using the Database Level Auditing feature.

See Also

Enterprise PeopleTools 8.45 PeopleBook: Data Management, "Employing Database Level Auditing," Understanding Database Level Auditing

CHAPTER 4

Setting Up Roles

This chapter provides an overview of roles and discusses how to:

- Manage roles.
- Define role options.
- Create a NEWUSER role.

Understanding Roles

Roles are an intermediate object that exist between permission lists and user profiles. Roles aggregate permission lists so that you can arrange permissions into meaningful collections. If you implement dynamic roles, then you can add permissions to users dynamically, which reduces administration tasks.

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

Role users are the user profiles or users that have membership to a particular role. Users inherit most of their permissions from the roles assigned to the user profile. However, you assign the following permission lists directly to a user profile:

- Data permissions.

  These are assigned through a primary permissions list or a row security permissions list.
- PeopleSoft Navigator homepage permissions.
- Process profile permissions.

When you assign roles to profiles manually, through the Security pages, these users are called static role users.

Other users may obtain membership in a role programmatically. You can run a batch process that runs 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.

Use dynamic role assignment to make your security system scale to large user populations. If you have thousands of users and need to make every change to a user profile manually, the security administrator becomes a bottleneck.

Managing Roles

This section discusses how to:

- Copy roles.
- Delete roles.
- Remove users from roles.

Copying Roles

To clone a role:

1. Select PeopleTools, Security, Permissions & Roles, Copy Roles.
2. On the search page, search for the role that you want to copy (clone), and click it.

   The Role Save As page appears.
3. On the Role Save As page, enter a new name in the as: edit box.
4. Click Save.

Deleting Roles

To delete a role:

1. Select PeopleTools, Security, Permissions & Roles, Delete Roles.
2. On the search page, locate the role that to delete and click it.

   The Delete Permission List page appears.
3. Click Delete Permission List.
4. Click OK to confirm the deletion, or click Cancel to cancel the deletion.

Note. If you attempt to delete a role definition that is currently in use by one or more static or dynamic role users, you must confirm deletion of the role definition. When you confirm, you remove all references to the role.

Removing Users From Roles

To delete the users assigned to a static or dynamic role, use the NO_USERS query to locate the users. You invoke this query using the query rule with dynamic roles.

See Also

Chapter 4, “Setting Up Roles,” Displaying Dynamic Role Members, page 55

Defining Role Options

This section discusses how to:

- Assign permissions to roles.
- Display static role members.
- Display dynamic role members.
- Set user routing options.

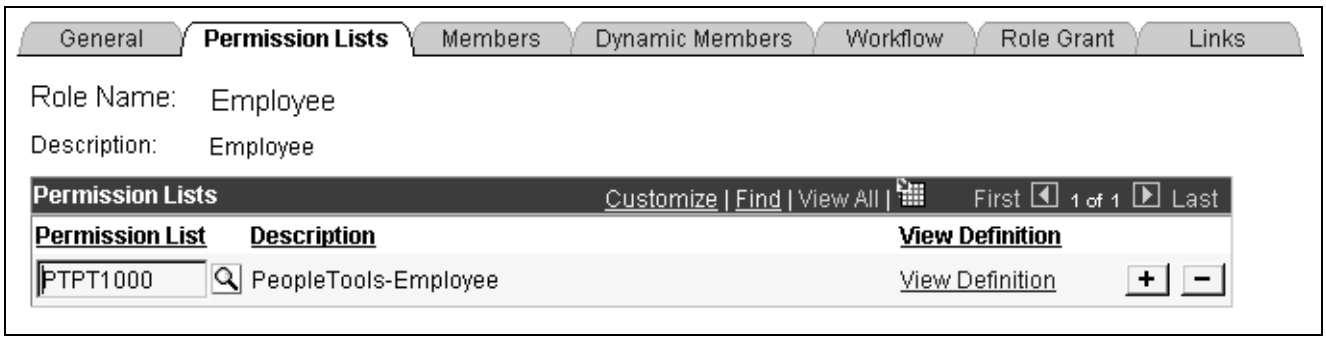
- Decentralize role administration.
- Display additional links for user profiles.
- Run role queries.
- View when a role was last updated.

Pages Used to Define Role Options

Page Name	Object Name	Navigation	Usage
General	ROLEDEFN	PeopleTools, Security, Permissions & Roles, Roles, General	Describe the role.
Permissions Lists	ROLE_CLASS	PeopleTools, Security, Permissions & Roles, Roles, Permission Lists	Grant permissions to roles.
Members	ROLE_MEMBER	PeopleTools, Security, Permissions & Roles, Roles, Members	View the current list of static role members.
Dynamic Members	ROLE_DYNMEMBER	PeopleTools, Security, Permissions & Roles, Roles, Dynamic Members	View the current list of dynamic role members. If you are not using the dynamic roles, then this list is not populated.
Workflow	ROLEWRKFLOW	PeopleTools, Security, Permissions & Roles, Roles, Workflow	Set user routing options.
Role Grant	ROLE_GRANT	PeopleTools, Security, Permissions & Roles, Roles, Role Grant	Decentralize role administration.
Links	ROLE_OTHER	PeopleTools, Security, Permissions & Roles, Roles, Links	View additional links for user profiles.
Role Queries	ROLE_QUERY	PeopleTools, Security, Permissions & Roles, Roles, Role Queries	Run queries about a role.
Audits	ROLE_AUDIT	PeopleTools, Security, Permissions & Roles, Roles, Audits	View when a permission list was last updated.

Assigning Permissions to Roles

Access the Permission Lists page.



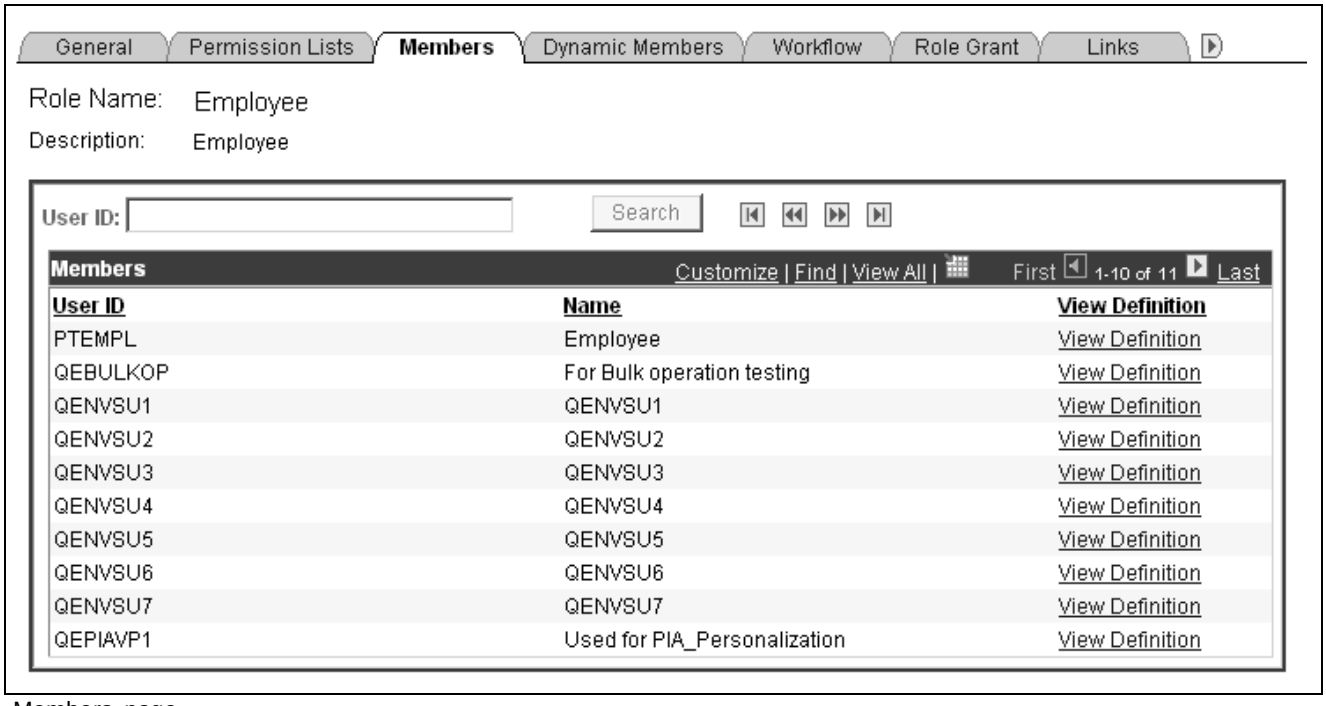
Permission Lists page

To add new permission lists to a role, add more rows. Remember that a user's access is determined by the sum of all the permission lists applied to each role to which the user belongs. For instance, suppose you add permission list X and permission list Y to a role. Permission list X has a sign-in time of 8 a.m. to 5 p.m. and permission list Y has a sign-in time of 1 p.m. to 9 p.m. In this scenario, the users assigned to this role can sign in to the system from 8 a.m. to 9 p.m. Always be aware of the contents of each permission list prior to adding it to a role.

View Definition Click to open the permission list definition and view the options in the permission, to make sure it is suitable for a particular role.

Displaying Static Role Members

Access the Members page.



Members page

If your database contains more than 1000 role members, this page initially retrieves only the first 1000. You can view the other chunks of 1000 members one chunk at a time, either by searching for a user ID or by using the navigation buttons above the Members grid. With the navigation buttons you can display the first chunk, the previous chunk, the next chunk, or the last chunk.

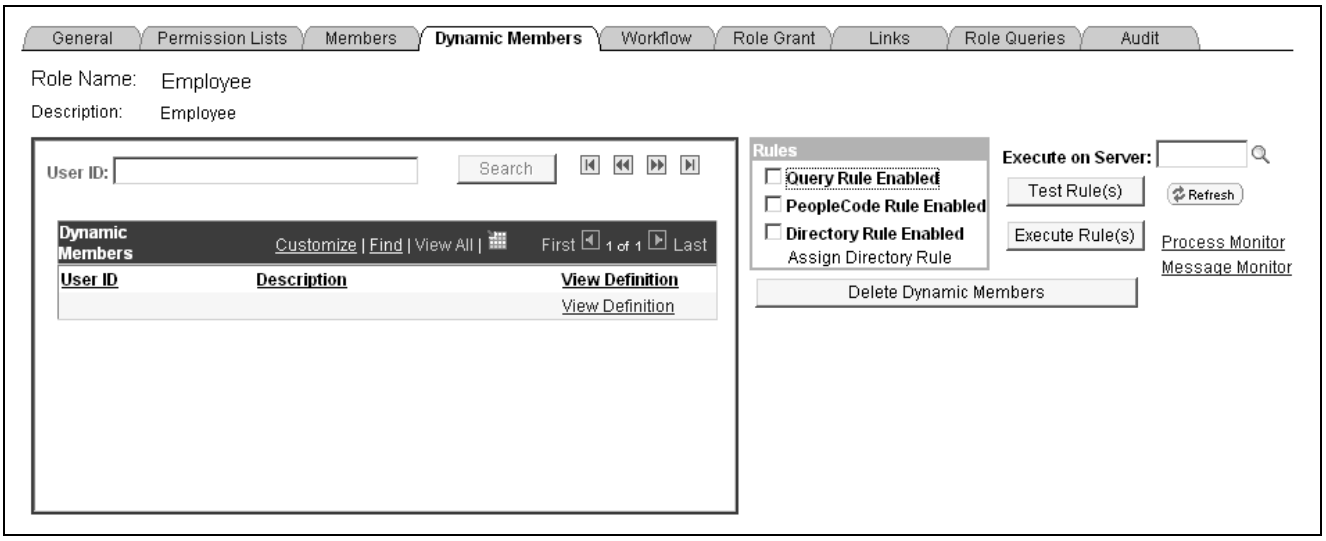
User ID Enter part or all of a role member user ID to search for.

Search Click to search through the role members for the first chunk of rows that contains the user ID you entered.

View Definition Click to view the user ID of the role member and make sure that you have selected the appropriate definition for inclusion in the role.

Displaying Dynamic Role Members

Access the Dynamic Members page.



Dynamic Members page

Use this page to set the rule to invoke to assign roles. A dynamic role rule is defined or coded in PeopleSoftQuery, PeopleCode, or your Lightweight Directory Access Protocol (LDAP) directory. A rule can use a combination of PeopleSoft Query and PeopleCode or PeopleSoft Query and LDAP. For the rule to successfully assign a role to the appropriate users, you must select the rule type you have in place for a particular role, and then specify the object that contains the rule you coded.

Note. You must define your role rules before you apply the options on this page. If you change the name of the rule, add a new rule, and so on, save all changes before you run the rule.

If your database contains more than 1000 dynamic role members, this page initially retrieves only the first 1000. You can view the other chunks of 1000 dynamic members one chunk at a time, either by searching for a user ID or by using the navigation buttons above the Dynamic Members grid. With the navigation buttons you can display the first chunk, the previous chunk, the next chunk, or the last chunk.

User ID Enter part or all of a role member user ID to search for.

Search Click to search through the role members for the first chunk of rows that contains the user ID you entered.

View Definition Click to view the user ID of the role member to ensure that you have selected the appropriate definition for inclusion in the role.

Query Rule Enabled Select if you defined your rule with PeopleSoft Query. The Query Rule group box appears below the Rules grou box. Use the Query drop-down list box to select the query that contains your role rule.

PeopleCode Rule Enabled Select if your rule is a PeopleCode program. The PeopleCode Rule group box appears. Specify the record, field, event, and function associated with your PeopleCode role rule.

Directory Rule Enabled Select if your role rule is based on information in your directory server. With a directory-based rule, you must assign directory groups. The PeopleCode Rule group box appears, because directory rules are implemented using a PeopleCode program, DynRoleMembers. The DynRoleMembers PeopleCode program uses the Directory business interlink to retrieve user and group information from the directory. To view the program, open the FUNCLIB_LDAP record in PeopleSoft Application Designer. Click Assign Directory Groups to select a particular directory group that exists in your LDAP server hierarchy. For example, suppose you have your LDAP server grouped by geographic region. If so, your rule could assign a new self-service role to all users in the North America group. Use the Directory Group drop-down list box to select the appropriate directory group value. The values are derived from the LDAP data that you import using the Directory Group Import process.

Execute on Server Select the appropriate PeopleSoft Process Scheduler server to run the rule.

Refresh After you run a rule, click to repopulate the grid with updated information.

Process Monitor Because the role rules are executed by an application engine program that runs through PeopleSoft Process Scheduler, click to view the status of the program run.

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

Note. To clear all dynamic users from the role, run the delivered NO_USERS query.

Query Rule Example

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

Note. The following text assumes a working knowledge of PeopleSoft Query.

In this example, we need to find all users that currently have job code KC012 (Human Resource Analyst), and add them to the appropriate role.

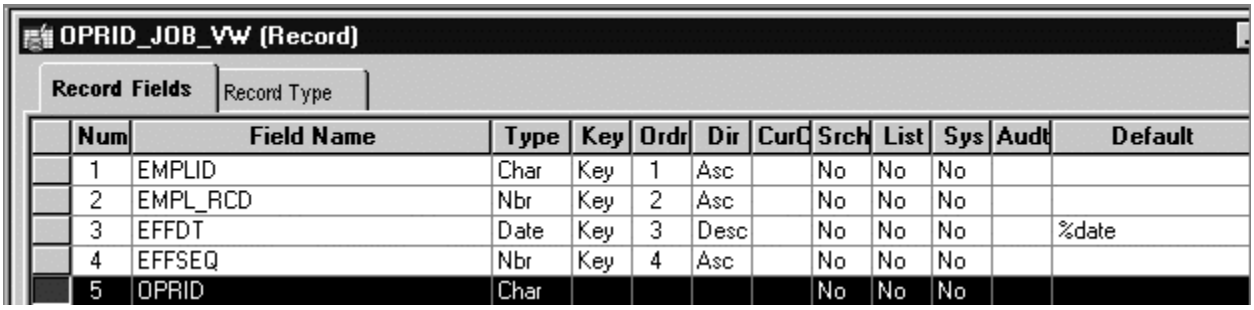
To create this rule:

1. Create a view.
2. Create the query.
3. Run the dynamic rule.

Note. The Dynamic Role functionality is not designed to resolve bind variables. When you select a query with a bind variable as a dynamic role rule, the system issues an error. Do not use queries with bind variables as a query rule for dynamic roles. Many of the delivered queries are intended to be used with PeopleSoft Workflow, and many of them contain bind variables. These queries are not designed to work as role rules, but you can modify them to do so.

Note. To create a role query based on PSOPRALIAS and avoid issues with row-level security, use PSOPRALIAS_VW instead. This view must be manually synchronized with PSOPRALIAS.

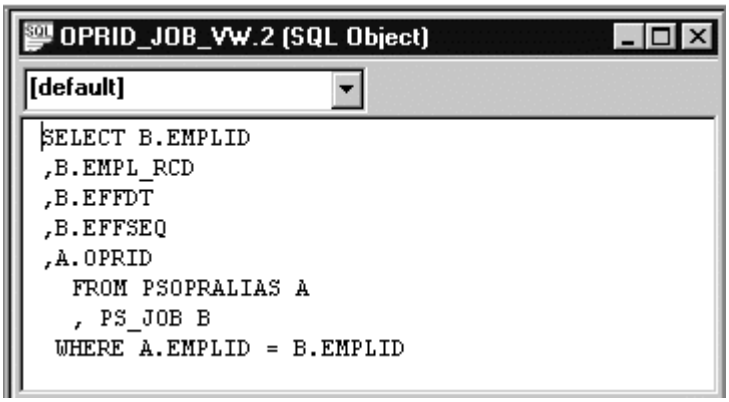
The view definition for the example role rule might be:



Num	Field Name	Type	Key	Ordr	Dir	CurC	Srch	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

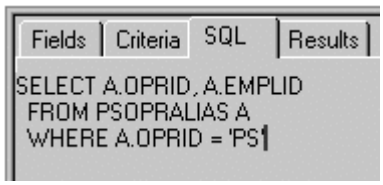
The associated SQL object is:



Dynamic role rule, SQL object

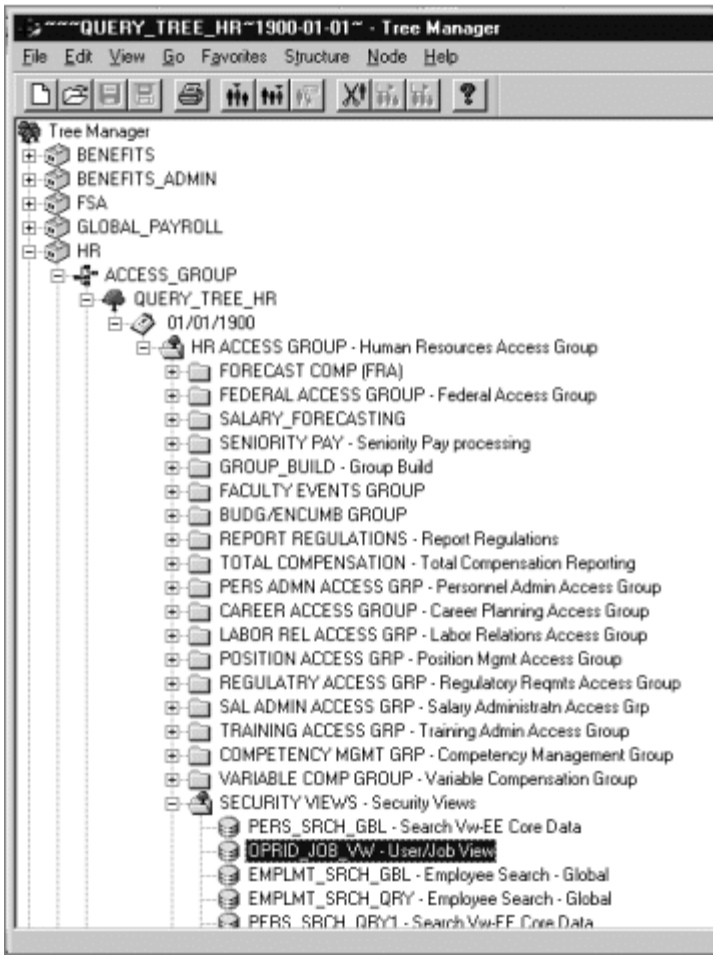
Note. The OPRID must not be a key in this view because PeopleTools appends AND OPRID = “current users oprid” in PeopleSoft Query. This occurs if we use the record OPRALIAS directly in the query.

The SQL is:



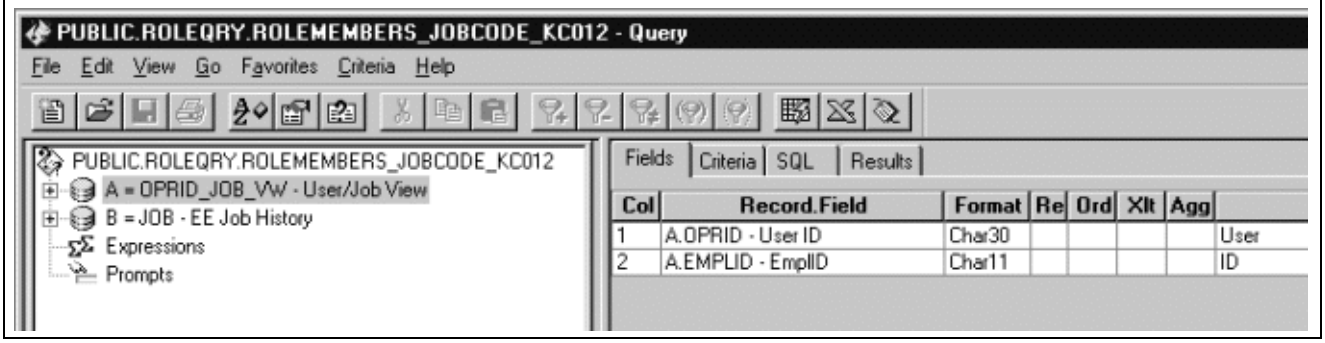
Query view SQL

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.



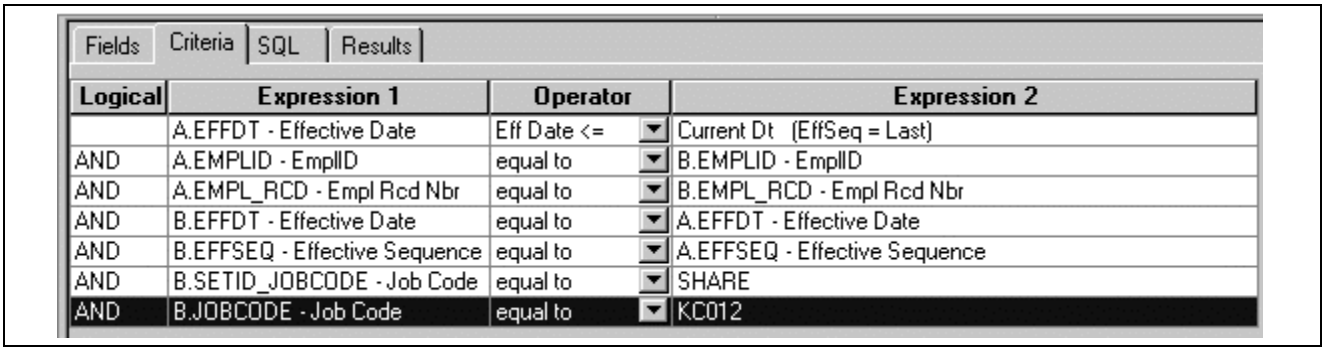
Adding the view to a query tree

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. The following screen shot shows query properties:



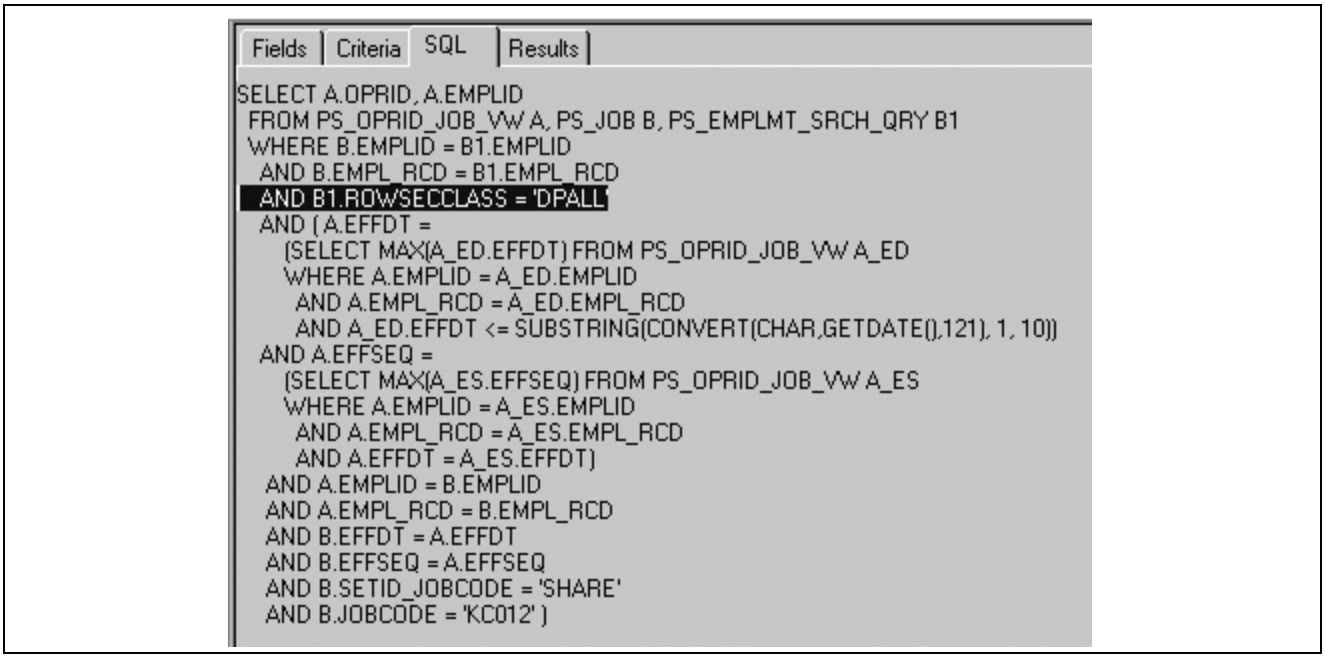
Query definition

The query contains the following criteria:



Query criteria

The SQL for the query is:



Query SQL

Because the view doesn't have OPRID as a key, the resulting SQL does not contain the extra line `AND B.OPRID = PS.`

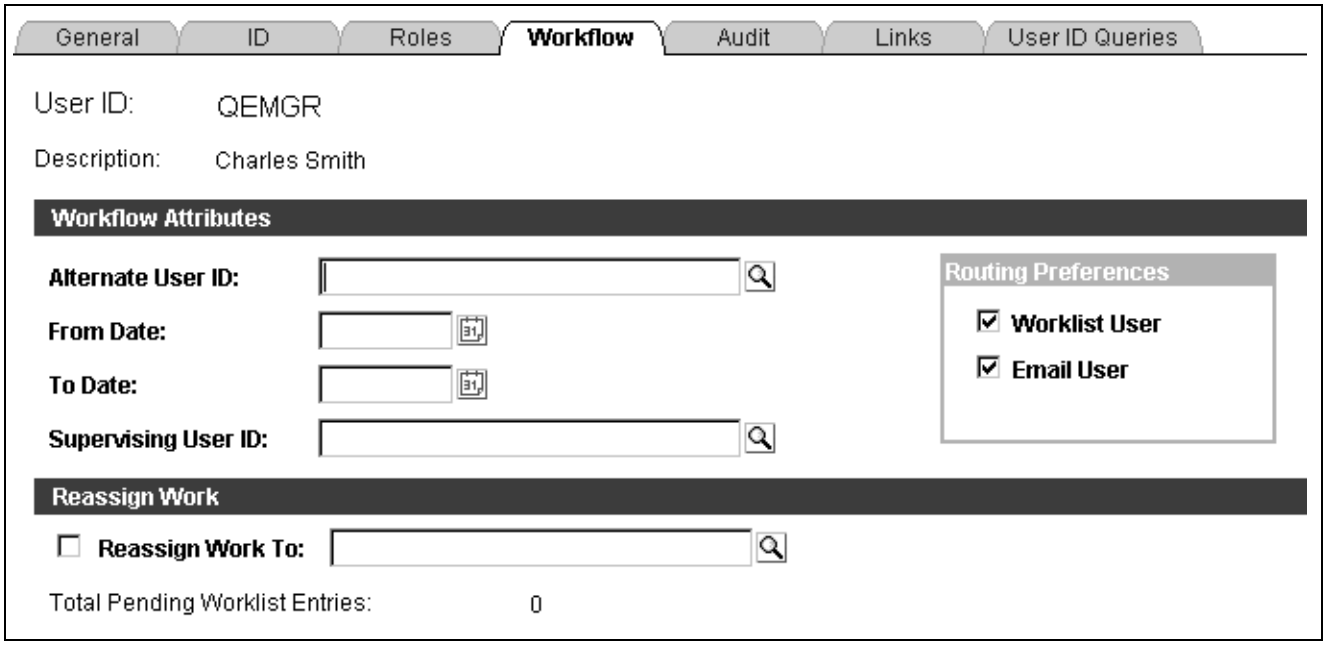
Note. When you save a query used for a dynamic role query, you need to specify that it's a role query when you save it.

With the view and the query created, you then set up the query rule on the Roles - Dynamic Members page. Select Query Rule Enabled and select the query in the Query field.

After enabling the query rule, test the rule to make sure the system assigns the appropriate roles to the appropriate users. To populate the role membership table, click Execute Rule.

Setting User Routing Options

Access the Workflow page.



Workflow page

Allow notification Select to enable PeopleSoft Workflow notification. Users can notify others of data on a PeopleSoft page through email or worklists.

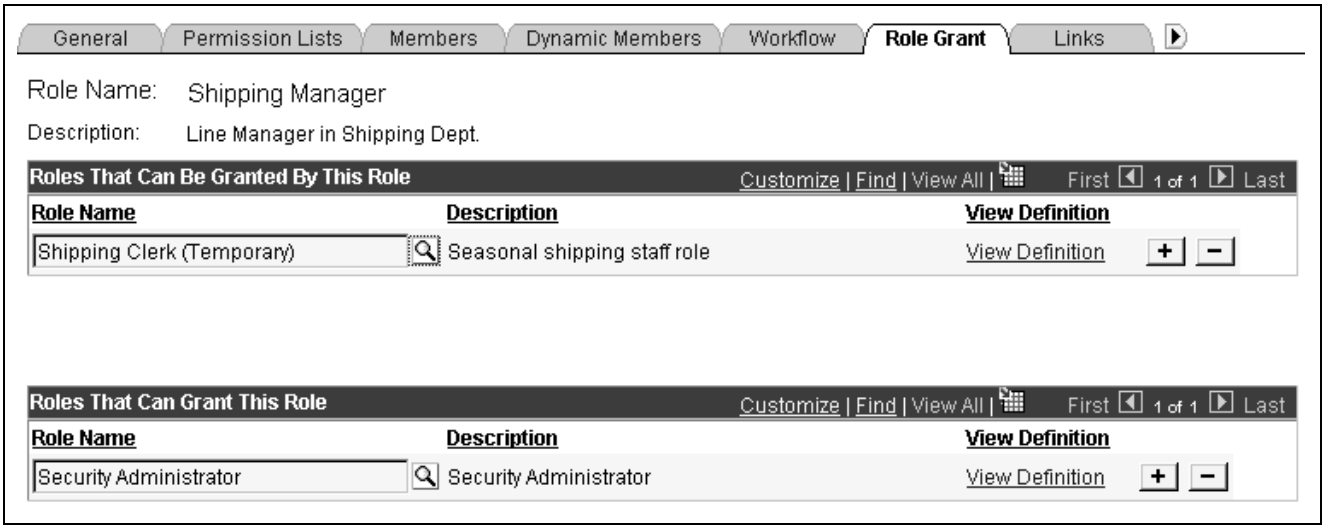
When components are designed, developers can enable the Notify toolbar on the Component Properties dialog box in PeopleSoft Application Designer. If this option is set for a particular component, then this check box enables security administrators to enable the Notify feature per role.

Allow Recipient Lookup Select to enable role users to browse the database for the email addresses of other users in the PeopleSoft system, which includes vendors, customers, employees, sales leads, and so on. Available only if Allow notification is selected.

Use Query to Route Workflow Select to determine workflow routings by a workflow query. This depends on your workflow scheme.

Decentralizing Role Administration

Access the Role Grant page.



Role Grant page

With this feature, you don't need to rely on dynamic roles, and yet you don't need to bother a security administrator to assign roles either. For example, you can enable a line manager to assign roles to direct reports.

The Role Grant page works in conjunction with the Distributed User Profiles and Distributed User Setup pages in the User Profiles component.

Roles That Can Be Granted By This Role This grid contains the roles that the current role is allowed to grant to other user IDs. For example, the line manager in the shipping department may need to grant a role to a temporary worker. Typically, the roles can be granted should report to the granting role. To add multiple roles, add more rows.

Roles That Can Grant This Role This grid contains the roles that can grant the current role to other user IDs. For example, on this page for the Shipping Temp role, Line Manager might appear in this grid. To add multiple roles, add more rows.

View Definition Click to view the associated definition and make sure that you have selected the appropriate definition for inclusion in the role.

See Also

Chapter 5, "Administering User Profiles," Working With Distributed User Profiles, page 79

Displaying Additional Links for User Profiles

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

See Also

Chapter 1, "Getting Started with Security Administration," Administering Security from Applications, page 8

Running Role Queries

Use role queries to provide detailed information regarding a role, such as the user IDs and permission lists associated with the role. The available queries are documented on the Role Queries page.

To run a role query:

1. Click the link associated with the query that you want to run.

This invokes a new browser window.

2. View the information the query returns, or select a download option.

   For downloading, you have the following options:

   • Microsoft Excel spreadsheet.

     Downloads the query results as a Microsoft Excel spreadsheet (.XLS) file.

   • CSV text file.

     Downloads the query results as a comma-separated values (CSV) file.

Viewing When a Role Was Last Updated

Access the Audit page.

View when a role was last updated and by whom. You can also view who has made changes to security tables by using the Database Level Auditing feature.

See Also

Enterprise PeopleTools 8.45 PeopleBook: Data Management, “Employing Database Level Auditing,” Understanding Database Level Auditing

Creating a NEWUSER Role

When a new user enters the system, and you have implemented dynamic role 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 employees become a member of the roles that apply to their position.

Note. The NEWUSER role is not a role that PeopleSoft delivers. You can name the role to suit your requirements.

To implement a NEWUSER role:

1. Create your NEWUSER role.
2. Add permission lists to the role so that members of this role have access to the pages that are appropriate for *all* users within the system, like My Profile and any other areas that are not a threat to your system security.
3. Apply the appropriate 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 must 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 one of the permission lists used by the NEWUSER role.

• Reduce the duration between the dynamic rule execution.

Note. 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.

CHAPTER 5

Administering User Profiles

This chapter provides an overview of user profiles and discusses how to:

- Set up access profiles.
- Work with user profiles.
- Specify user profile attributes.
- Work with distributed user profiles.
- Work with full user profile synchronization.
- Work with passwords.
- Work with user profile options.
- Transfer users between databases.
- Track users' signin and signout activity.

Understanding 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 to be a usable profile. The majority of values that make up a user profile are inherited from the linked roles.

Note. It's possible to have a user profile with no roles. This might be a user who isn't allowed access to the PeopleSoft application; however, you still want workflow-generated email sent to the user.

You define user profiles by entering the appropriate values on the user profile pages. 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.

The user ID and description appear at the top of each page to help you recall which user profile you are viewing or modifying as you move through the pages.

Setting up Access Profiles

This section provides an overview of access profiles and discusses how to:

- Use the Access Profiles dialog box.
- Set access profile properties.
- Work with access profiles.

Understanding 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 in to the PeopleSoft database directly (two-tier).
- When batch programs connect to the database.

Users signing in to the system through PIA take advantage of the Access ID that the application server used for connecting to the database.

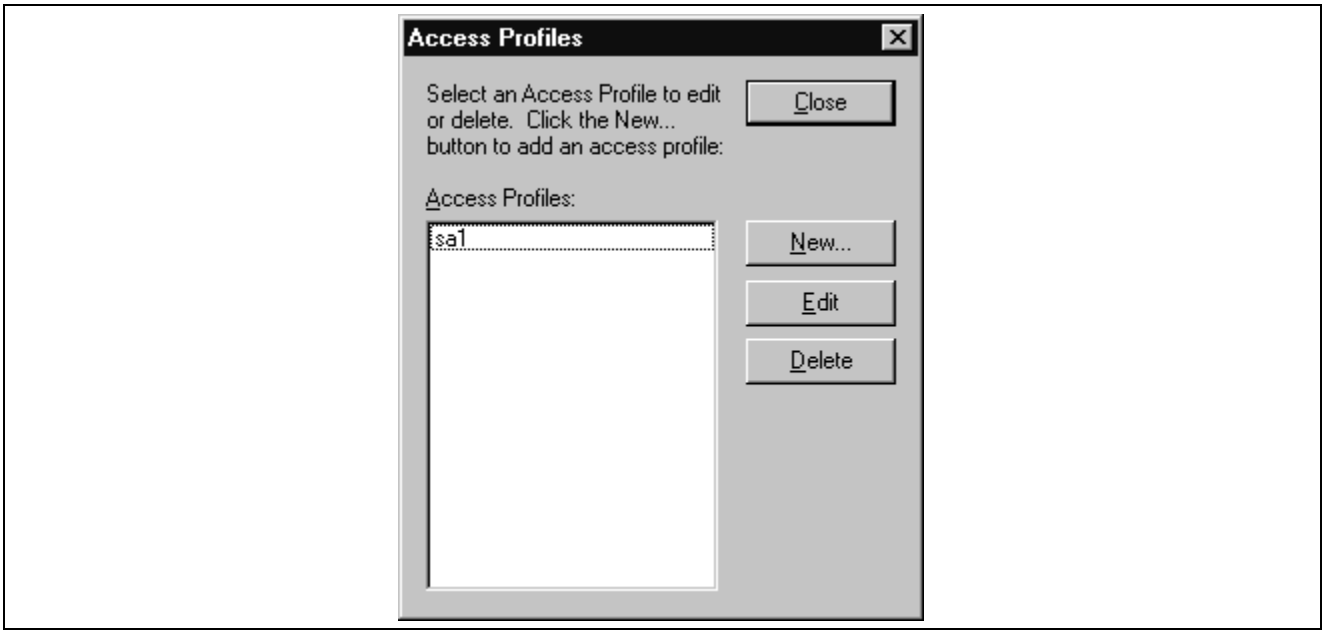
Access profiles allow you to minimize the number of Maintain Security users who need to know system administrator passwords. In fact, only one person needs to know these passwords. That person can create the required Access Profiles—by providing the necessary passwords, when prompted—and all other Maintain Security users can simply assign users to the pre-defined Access Profiles. The Access ID and password are encrypted in the database in the PSACCESSPRFL table.

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. This association is by way of the symbolic ID, which is a proxy ID for the Access ID and Access password.

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. This is created when you first install your database.

Using the Access Profiles Dialog Box

You manage Access Profiles using the Access Profiles dialog, which you open from Application Designer by selecting Tools, Miscellaneous Definitions, Access Profiles.



Access Profiles Dialog Box

Close Exit this dialog.

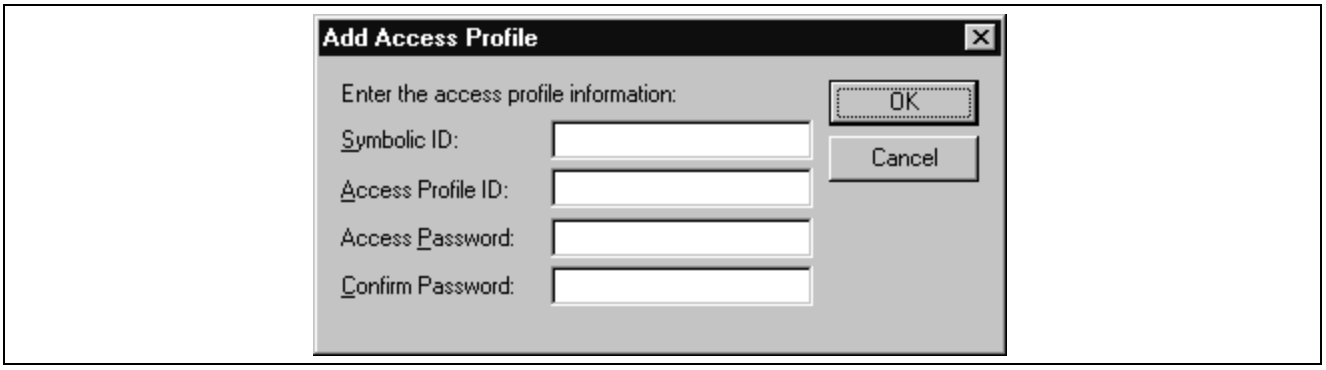
New Create a new access profile definition.

Edit Edit an existing access profile definition.

Delete Delete an existing access profile definition.

Setting 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

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.

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 Note. 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 PeopleSoft Application Designer, select Tools, Miscellaneous Definitions, Access Profiles.

   The Access Profiles dialog appears.

2. Click New.

   The Add Access Profile dialog appears.

   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.

Note. PeopleSoft suggests that you only use one Access ID for your system. Some RDBMS do not permit more than one DB table owner. If you create more than one Access ID it may require further steps to ensure that this ID has the correct rights to ALL PeopleSoft system tables.

To change an Access Profile password

1. In Application Designer, select Tools, Miscellaneous Definitions, 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.

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 Definitions, 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.

Important! Make sure you do not delete the *only* available Access ID or you will not be able to logon to PeopleSoft in any capacity.

Working With User Profiles

This section discusses how to:

- Create a new user profile.
- Copy a user profile.
- Delete a user profile.

Creating a New User Profile

To create a new user profile:

1. Select PeopleTools, Security, User Profiles, User Profiles to access the Find Existing Values page.
2. 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. The name that you use can't contain a comma (,) or a space. Also, you can't create a user ID named PPLSOFT; this ID is a reserved user ID used within PeopleTools.

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

Copying a User Profile

To copy a user profile:

1. Select PeopleTools, Security, User Profiles, Copy User Profiles to access the Find an Existing Value search page.
2. Select the user ID that you want to clone.

3. On the User Profile Save As page, enter the new user ID, description, and the password that the new user ID should use to sign on to the system.

Deleting a User Profile

To delete a user profile:

1. Select PeopleTools, Security, User Profiles, Delete User Profiles to access the Delete User Profile page.
2. Make sure that you have selected the *correct* user profile.
3. Click Delete User Profile to remove information related to this particular user profile that appears in every security table in the system, PeopleTools, and application tables.

   To prevent any of the information from being deleted, you can specify tables that the delete user process bypasses.

Specifying User Profile Attributes

This section discusses how to:

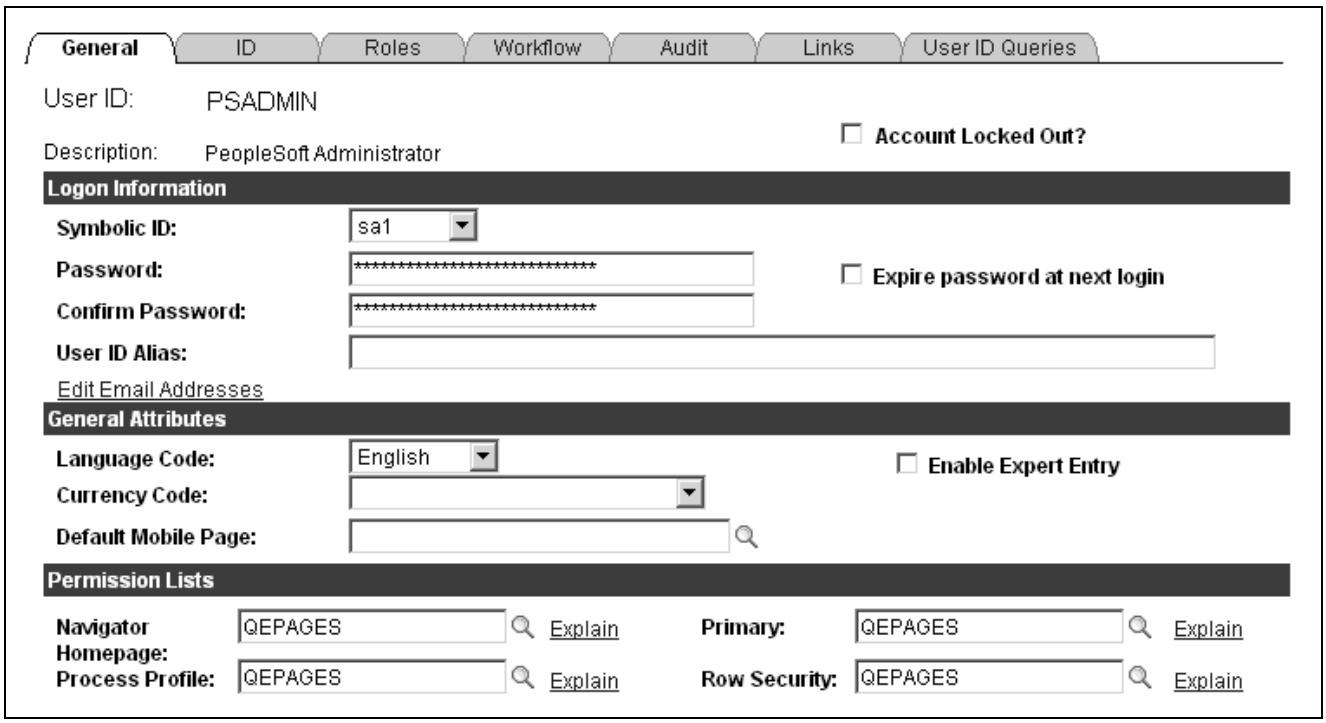
- Set general user profile attributes.
- Set ID type and attribute value.
- Set roles.
- Specify workflow settings.
- Inquire about user profile audit information.
- Display additional links added.
- Run user ID queries.

Pages Used to Specify User Profile Attributes

Page Name	Object Name	Navigation	Usage
General	USER_GENERAL	PeopleTools, Security, User Profiles, User Profiles, General	Set general user profile attributes.
ID	PSOPRALIAS	PeopleTools, Security, User Profiles, User Profiles, ID	Set ID type and attribute value.
Roles	USER_ROLES	PeopleTools, Security, User Profiles, User Profiles, Roles	Add roles to a user profile. This defines what the user can access in the PeopleSoft system. Through roles, the user inherits permission lists.
Workflow	USER_WORKFLOW	PeopleTools, Security, User Profiles, User Profiles, Workflow	Specify workflow settings for a user.
Audit	USER_AUDIT	PeopleTools, Security, User Profiles, User Profiles, Audit	Inquire about when and who last updated a profile.
Links	USER_OTHER	PeopleTools, Security, User Profiles, User Profiles, Links	Displays any additional links added.
User ID Queries	USER_QUERY	PeopleTools, Security, User Profiles, User Profiles, User ID Queries	Run queries about a user profile.

Setting General User Profile Attributes

Access the General page.



User Profiles - General page

Logon Information

Account Locked Out? Select this check box to deactivate a user profile for any reason. The user can't sign on until you have cleared this option.

Note. This check box is also automatically selected by the system if the user exceeds the maximum number of failed logon attempts (if using password controls). The administrator would then need to manually open the user profile and clear the check box to reinstate the user.

Symbolic ID Associated with a user's encrypted access ID and access password. The correct symbolic ID must be entered to retrieve the appropriate access ID and password. This value determines which access ID and password are used to log the user onto the database after the system validates the user's user ID.

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

With PeopleSoft Internet Architecture (PIA), the application server maintains the connection to the database, so the application server must submit an access ID.

Password and **Confirm Password** Enter the user password, which is the password string that the user must supply when signing on. The value in the Confirm Password field must match that in the User Password field.

Note. These values are required to sign on to the system, but you can save the profile without populating these fields.

Expire password at next login

If you are using PeopleSoft password controls, this option enables you to force users to change their passwords in the following situations:

- First time that a user signs on to PeopleSoft.
- Next time that a user signs on.
- First time that a user signs on after the system has emailed the user a randomly generated password.

Note. To use this option, you must first enable the Password Expires in 'x' Days PeopleSoft password control.

User ID Aliases

Enables you to use a fully qualified email ID (email address) as a user ID alias. For example, Tom_Sawyer@peoplesoft.com could be the user ID used to sign on to the system. The character limit is 70.

Edit Email Addresses

If a user is part of the workflow system or you have other systems that generate emails for users, enter an email address for a user with this link. You can enter multiple email addresses for a user, but one must be selected as the primary email address. The system allows only one email address per type. For example, you can't enter two home email addresses.

The Email Addresses interface has the following controls:

- Primary Email Account: If you enter multiple email accounts, one must be selected as the primary account.
- Email Type: Select from Blackberry, Business, Home, Other, or Work.

  The Blackberry email type is used with the Workflow/RIM technology.
- Email Address: Enter the email address in this edit box.

General Attributes

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 in which language to generate the reports for the user who submitted the job.

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

For Windows workstations, the user's language preference is derived from the Display tab in PeopleSoft 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 PeopleSoft Configuration Manager.

Currency Code

If the user deals with international prices, set the currency code to reflect the native or base currency. This enables values to appear in the currency with which the user is familiar.

Default Mobile Page

Select the mobile homepage that should appear after users sign on to their mobile device.

Enable Expert Entry

You can specify that some users—for example, your expert or power users—have the option of deferring all processing of the data that they enter for PeopleSoft. This enables users to reduce the amount of trips

to the server for data processing, regardless of how the developer set field deferred or interactive processing. You enable this option in a component in Application Designer, and you specify which users have this option using the Enable Expert Entry check box.

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

Permission Lists

Navigator Homepage Associated with PeopleSoft Workflow.

Process Profile Contains the permissions that a user requires for running batch processes through PeopleSoft Process Scheduler. For example, the process profile is where users are authorized to view output, update run locations, restart processes, and so on.

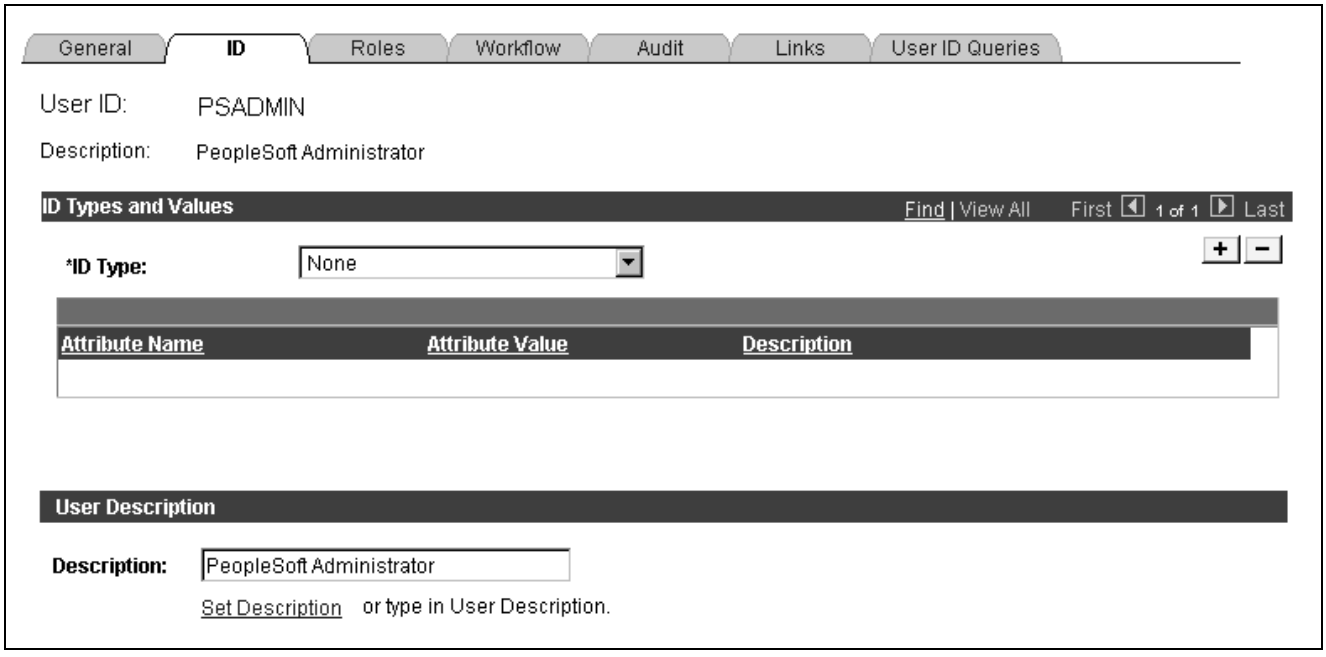
Note. Only the process profile comes from this permission list, not the list process groups.

Primary and **Row Security** PeopleSoft determines which data permissions to grant a user by examining 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 (if needed), and definition security permissions from the primary permission list.

Setting ID Type and Attribute Value

Access the ID page.



ID page

ID Types and Values

ID Types and Values

Select the ID type and attribute value. Separating user profiles by ID type enables 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 payroll deductions application, they see only information that applies to them.

A user profile is a set of data about an entity—a user—that interacts with the system. The human resources (HR) system, which keeps track of your employee data, is designed to focus more on your employee user types. On the other hand, your financials system is designed to keep track of customer and supplier user types. ID types enable you to link user types with the records that are most relevant when a user interacts with the system.

The Attribute Value field 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.

User Description

The User Description section enables you to help identify the user.

Description You can add a description, such as a name of an individual or an organization, for the user profile.

Set Description Click this link to populate the edit box with an existing description in the database.

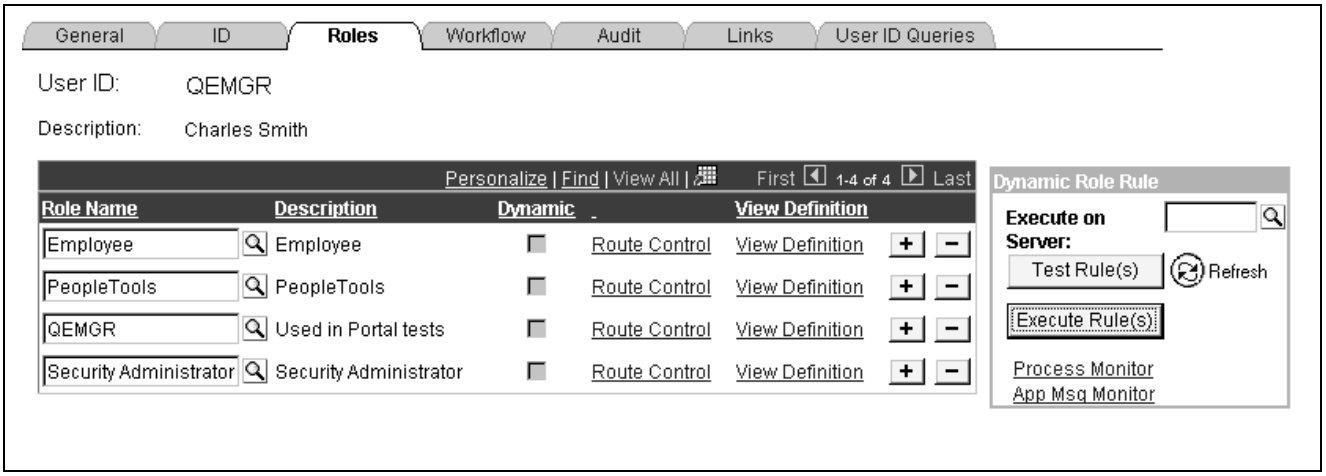
Note. Before you assign a user type to a user, you must create user types.

See Also

Chapter 5, “Administering User Profiles,” Working With User Profile Options, page 86

Setting Roles

Access the Roles page.



Roles page

Role Name	Displays the name of the role added to the user profile.
Description	Displays a description of the role added to the user profile.
Dynamic	Selected if the system has assigned a particular role dynamically.
Route Control	For each role assigned to a user, you can specify a route control profile. For example, suppose that you have a role named EXPENSE_REP. If you wanted a particular expense representative to handle all of the expense reports submitted by people who had last names beginning with *A*, you could assign the user a specific route control profile—one sending the user reports submitted by individuals with a last name beginning with *A*.
View Definition	Enables you to view the role definition associated with this user profile.

See *Enterprise PeopleTools 8.45 PeopleBook: Workflow Technology*, "Using Additional Routing Options," Understanding Route Control Development.

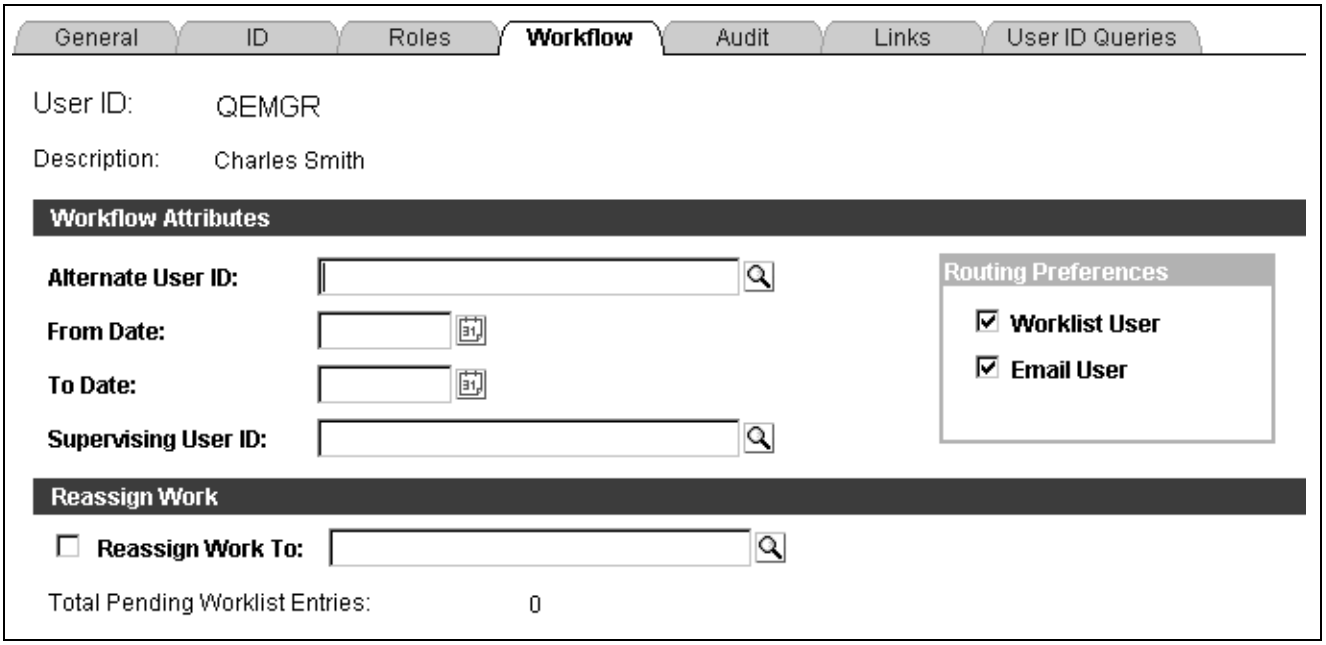
Dynamic Role Rule

Use the Dynamic Role Rule options to test and manually carry out your rules for assigning roles dynamically. You design your role rules using Query Manager, PeopleCode, or your LDAP scheme.

Execute on Server	Select the Process Scheduler server that should run your role rule.
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 this button to run your rules and assign the appropriate roles to a particular user. This is the manual approach. Typically, you carry out role rules through PeopleSoft Process Scheduler on a regularly scheduled basis.
Process Monitor and **App Msg Monitor** (application message monitor)	Enables you to view the status of the process carrying out your role rule and the application messages that the process invoked.

Specifying Workflow Settings

Access the Workflow page.



Workflow page

Workflow Attributes

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 edit box, the system automatically forwards new work items for whoever is assigned as the current role user to the alternate role user.

Note. 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, access the Role User Archiving component.

From Date and **To Date** This edit box applies to the alternate user ID. Here you enter the date on which the current role user is going to begin and return from a temporary vacancy.

Supervising User ID Select the user ID of the user's supervisor in this drop-down 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.

Note. If you're using PeopleSoft Human Capital Management (PeopleSoft HCM) applications, this field shouldn't appear. If it does, you must set your workflow system defaults.

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

Reassign Work

Re-assign Work To 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 (as shown by the Total Pending Worklist Entries in your Workflow interface), select this check box and select the user to whom work items should be forwarded from the drop-down list box. When you save the page, the system reassigns existing worklist entries to the specified user.

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

Total Pending Worklist Entries Displays worklist items that require a user's attention.

See Also

Enterprise PeopleTools 8.45 PeopleBook: Workflow Technology, "Defining Roles and Users"

Inquiring About User Profile Audit Information

The Audit page is a display-only page that enables you to determine:

- When a profile was last updated.
- Who updated the profile.

Displaying Additional Links Added

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

See Also

Chapter 1, "Getting Started with Security Administration," Administering Security from Applications, page 8

Running User ID Queries

User ID queries enable you to run queries that provide detailed information regarding a user profile, such as the permission lists and roles associated with a user profile. The available queries are documented on the page.

To run a user ID query:

1. Click the link associated with the query that you want to run.

   This invokes a new browser window.
2. View the information that the query returns to the new browser window, or select a download option.

   For downloading, you have the following options:

   - Excel Spreadsheet: Downloads the query results as an Excel spreadsheet (.XLS) file.
   - CSV Text File (comma-separated values text file): This downloads the query results as a CSV file format.

Working With Distributed User Profiles

The distributed user security administration feature is enabled using the Role Grant page in the Roles component.

This section provides an overview of distributed user profiles and discusses how to set up distributed user administration.

See Also

Chapter 4, “Setting Up Roles,” Decentralizing Role Administration, page 60

Understanding Distributed User Profiles

PeopleSoft offers self-service security pages, such as Change My Password and My System Profile. This distributes the security administration throughout the organization freeing system administrators to focus on higher priority tasks. The distributed user profile feature is also how you can distribute security administration. With distributed user profiles, you grant a particular role the ability to modify another role, such as a manager modifying a small number of users under his or her control. For example, with distributed user profiles the HR Manager could modify the permissions of the HR Clerk role.

The pages in the Distributed User Profiles component are exactly the same as the corresponding pages in the "regular" User Profiles component. The regular User Profiles component is intended for system administrators. The Distributed User Profiles component contains a reduced number of pages, the ones that managers most likely would need to modify for their direct reports.

To set up distributed user profile maintenance, you must have the following items in place:

- Specify the appropriate settings in the role definition (which is not discussed here) to allow the role access to the Distributed User Profiles component.
- Specify the appropriate search record on the Distributed User Set Up page.

Setting Up Distributed User Administration

Select PeopleTools, Security, User Profiles, Distributed User Setup to access the Set Distributed User Profile Search Record page.

On this page, the system administrator selects the search record to control which user IDs can be opened in the Distributed User Profile.

When a manager accesses the Distributed User Profile, only those roles that can be granted through the Role Grant page are available in the prompt. Changing the delivered functionality requires changes to the appropriate search records.

See Also

Enterprise PeopleTools 8.45 PeopleBook: PeopleSoft Application Designer, “Creating Component Definitions,” Understanding Search Records

Working with Full User Profile Synchronization

PeopleSoft provides the ability to synchronize users between an 8.1x database and an 8.4x database or between two 8.4x databases using the USER_PROFILE application message.

This section discusses how to:

- Configure full user profile synchronization.
- Set up USER_PROFILE transactions.
- Set up the User_Sync Application Engine program.

Configuring Full User Profile Synchronization

To set up full user profile synchronization, you use PeopleSoft Integration Broker to configure one database to *send* user profile data and another database to *receive* user profile data. The Application Engine program User_Sync accesses profiles on the sending database through the USER_PROFILE_SYNC component interface. After the User_Sync program opens up the profiles through the USER_PROFILE_SYNC component interface, it publishes the USER_PROFILE application message. After publication, the User_Sync program enables the component interface to send the application message to the receiving database.

To set up full user profile synchronization:

1. Set up PeopleSoft Application Messaging for 8.1 databases and PeopleSoft Integration Broker for 8.4 databases.

   Important! For Full User Profile synchronization to function properly, you must set up PeopleSoft Application Messaging for 8.1x databases and PeopleSoft Integration Broker for 8.4x databases.

   See *Enterprise PeopleTools 8.45 PeopleBook: PeopleSoft Integration Broker*.

   See *PeopleTools 8.14: Application Messaging.*
2. Give permission to the methods on the USER_PROFILE_SYNC component interface.
3. In PeopleSoft Integration Broker, set up the 8.4 node Transactions for the USER_PROFILE message.

   See Chapter 5, “Administering User Profiles,” Setting Up USER_PROFILE Transactions, page 80.
4. Set up and run the User_Sync Application Engine program.

   See Chapter 5, “Administering User Profiles,” Setting Up the User_Sync Application Engine Program, page 81.

Setting Up USER_PROFILE Transactions

Select PeopleTools, Integration Broker, Node Definitions. Open the appropriate node and select the Transactions tab.

Configure transactions to send and receive user profiles using the following:

- Transaction Type: Select InAsync when configuring your 8.4x database to *receive* user profiles.

  Select OutASync when configuring your 8.4x database to *send* user profiles.
- Request Message: USER_PROFILE

- Request Message Version: Select VERSION_81X to send messages to or receive messages from an 8.1x database.

  Select VERSION_84 to send messages to or receive messages from an 8.4 database.

Setting Up the User_Sync Application Engine Program

The User_Sync Application Engine program synchronizes user profiles between databases using the USER_PROFILE application message. You set up this program on the database that you configured to send user profile information. Once you have set up the program, click Run.

To set up this program, select PeopleTools, Application Engine, Process.

Create a new request using the following configuration:

- Program Name: USER_SYNC
- State Record: AE_USRSYNC_AET
- Bind Variable Name: RECNAME
- Value: Enter the record or view that contains the user IDs that you would like to send to the receiving database.

  You can either insert a value of PSOPRDEFN if you would like all user IDs to be sent, or you can create a custom view for a subset of user IDs to be sent.

Note. If you leave the Parameters section blank, the record value PSOPRDEFN appears by default.

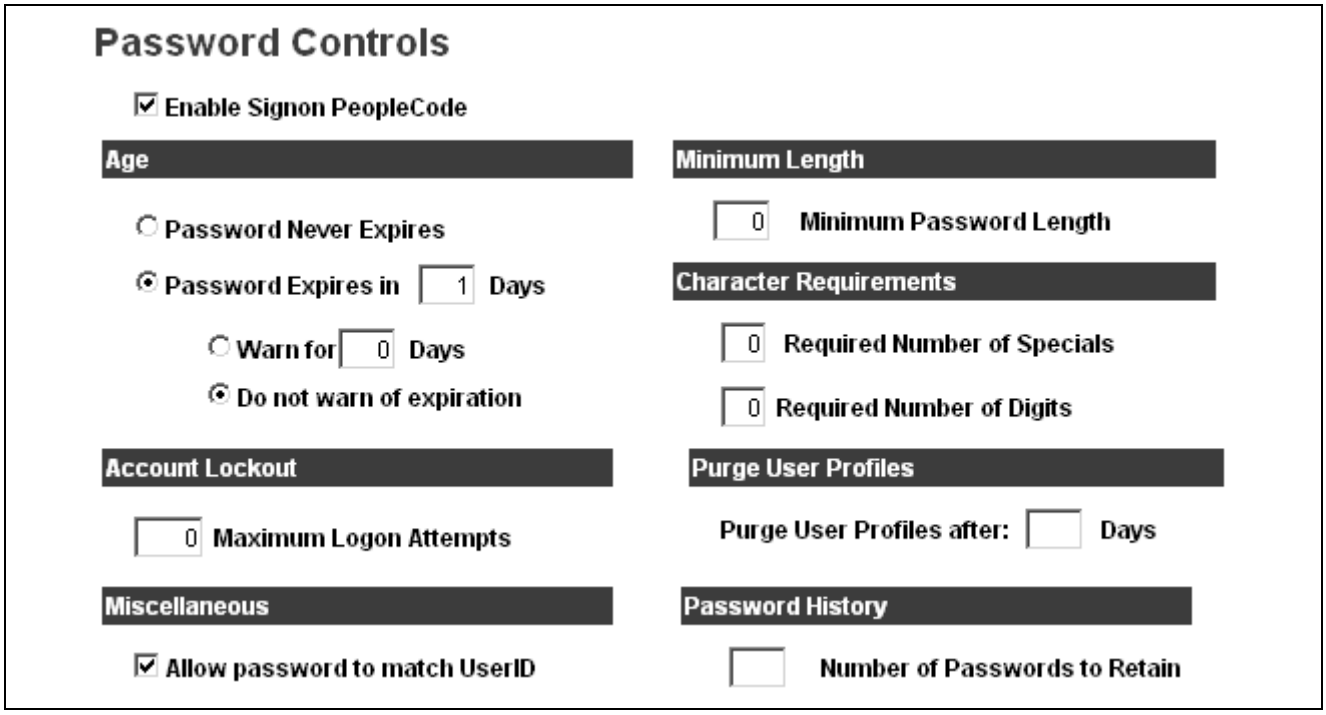
Working With Passwords

This section discusses how to:

- Set password controls.
- Change passwords.
- Create email text for forgotten passwords.
- Create hints for forgotten passwords.
- Delete hints for forgotten passwords.
- Set up the site for forgotten passwords.
- Request new passwords.

Setting Password Controls

Select PeopleTools, Security, Password Configuration, Password Controls to access the Password Controls page.



Password Controls page

You use the Password Controls page to set any password restrictions such as duration or minimum length of a password that you might want to impose on your end users. These options apply when you are maintaining your user profiles *within* PeopleSoft, not within a directory server.

Enable Signon PeopleCode Select this check box to enable the following PeopleSoft password controls: Age and Account Lockout. The other password controls are not enabled by this box.

If you do not want these password controls, as in you already have a third party utility that performs equivalent features, then leave this check box clear.

Note. You can extend or customize the controls by modifying the PeopleCode.

Age You define a number of days (between 1 and 365) that a password is valid. To do this, select the Password Expires in ‘N’ Days option. 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 and will be prompted to change it.

If you want to specify a duration in which the system warns users that their password is about to expire, you have the following options:

- If you want to specify a warning period, select Warn for ’N’ days, and enter the number of days in the edit box.
- If you don’t want any warning period, select Do not warn of expiration.

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 access only items in the PSWDEXPR permission list, which typically grants access to the Change Password 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.

Note. 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 is 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 provides a reminder to your end users to remember the password they choose.

After the account is locked out, a system administrator needs to open the user profile and clear the Account Locked check box manually.

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 the 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 not 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:

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

Purge User Profiles

This setting enables you to purge the system of user profiles that have not been used in a specified amount of time. This aids in general housekeeping. In particular, if you maintain user profiles in a directory server, a row is still added to the PSOPRDEFN table for the system to access while the user interacts with the system. However, if that user is deleted from the directory server you still need to delete the row in PSOPRDEFN associated with the deleted user profile.

Note. The Application Engine program that performs this operation is named PURGEOLDUSERS.

Changing Passwords

The PeopleSoft system enables users to change their passwords as needed.

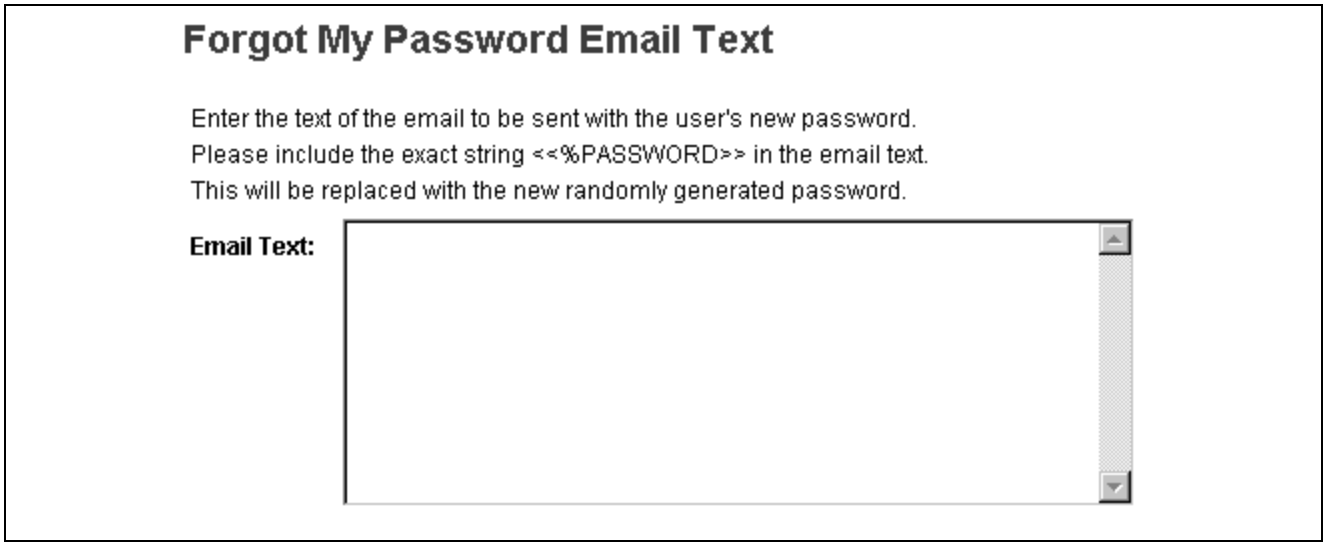
To change a PeopleSoft password:

1. From the portal navigation pane, select Change My Password.
2. On the Change Password page, enter the current password in the Current Password edit box.
3. In the New Password edit box, enter the new password.
4. Confirm the new password by entering it again in the Confirm Password edit box.
5. Click Change Password.

Creating Email Text for 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 feature enables you to pose a standard question to users requesting a new password to verify the user's authenticity. If the user enters the appropriate response, then the system automatically emails a new password.

When a user has forgotten a PeopleSoft password, the system sends the user a new password within an email message. You can have numerous password hints, but typically, you 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 that you use for your template:



Forgot My Password Email Text page

Add the following text string in the Email Text edit box:

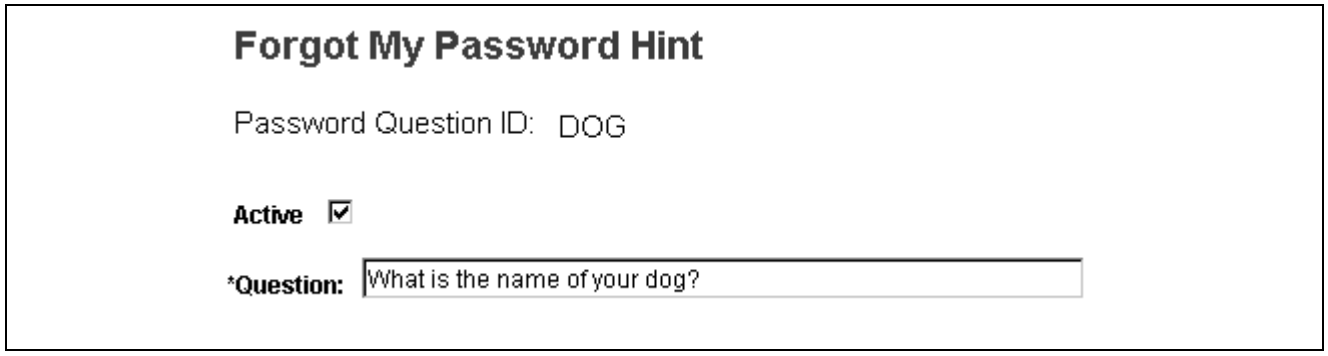
```
<<%PASSWORD>>
```

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

Note. You might instruct the user to change the password to something easier to remember after they sign on 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 using this feature.

Creating Hints for Forgotten Passwords

Select PeopleTools, Security, User Profile, Forgot My Password Hint to access the Forgot My Password Hint page.



Forgot My Password Hint page

With these hints set up, users, upon forgetting their password, access the Forgot My Password page. 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 System Profile component.

To create a forgotten password hint:

1. Click Add a New Value.
2. On the Add a New Value page, enter a three-character ID in the Password Hint ID edit box.
3. Click Add.
4. Select the Active check box.
5. Enter your question to verify that the user is who he or she claims to be.
6. Click Save.

Deleting Hints for Forgotten Passwords

To delete a password hint:

1. Select PeopleTools, Security, User Profiles, Delete Forgotten Password Hint.
2. Enter the specific code for the hint or perform a search for it.
3. On the Delete Forgot My Password Hint page, select the appropriate hint.
4. Click Delete.

Setting Up the Site for Forgotten Passwords

PeopleSoft recommends setting up a site specifically designed for users who have forgotten their passwords. This site would require no password to enter, but provides access only to the forgotten password pages.

To set up a forgotten password site:

1. Set up a separate PIA site on your web server.
2. Set up a direct connection to the site, as in a link that leads right to it.
3. In the web profile, enable public access and specify a public user ID and password for automatic authentication.

   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.

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

Requesting New Passwords

Access the Forgot My Password page, which is a “hidden” component.

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 the user is not allowed to receive a new password through email.

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

Before the system can email you a new password, you must have the following in place:

- A forgotten password hint.
- An email address specified in the user profile.
- The security administrator must permit users to have a new password emailed.

To request a new password:

1. If you can’t remember your password, click the Forgotten Password link on the PeopleSoft signon page.
2. On the Forgot My Password page, enter your user ID.
3. Click Continue.
4. On the Email New Password page, make sure that 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 must 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.

Working With User Profile Options

This section provides an overview of user profile types and discusses how to:

- Define user profile types.
- Preserve historical profile data.

Understanding 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.

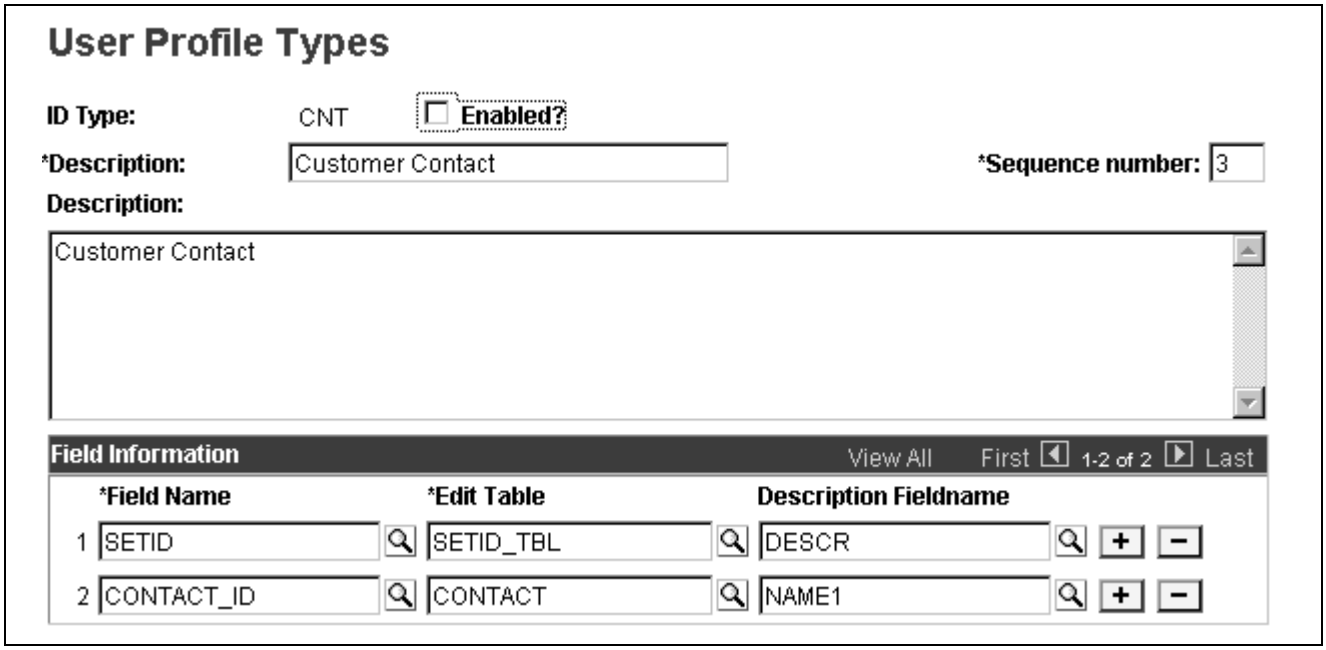
User profile types also provide a means to link user profiles with data stored in application specific records. PeopleSoft applications need this link mostly for self-service transactions. For example, you want employees to see just their own benefits, or you want customers to view and pay their *own* 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.

PeopleSoft delivers the following profile types:

ID Type	Description
BID	Bidder
CNT	Customer Contact
CST	Customer
EJA	External Job Applicant
EMP	Employee
NON	None
ORG	Organization ID
PER	Person (CRM)
VND	Vendor
PTN	Partner

Defining User Profile Types

Select PeopleTools, Security, Security Objects, User Profile Types to access the User Profile Types page.



User Profile Types page

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 selecting this check box. Once enabled, you can assign it to user profiles. If it is disabled then it does not appear in the drop-down list box on the ID page for user profiles.

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

Sequence Number This option is used by the Set Description function. On the User Profiles, ID page you can click a Set Description link to generate the user description based on the values in the Description field name 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 field name of the user type with the lowest sequence number and nonblank 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.

Note. For user types with multiple fields, the system uses the Description field name 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 field name 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 that 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 that the user selects 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.

Preserving Historical Profile Data

There are many occasions when you need to delete a user profile from your system. For instance, perhaps an employee retires or an employee leaves the organization. Regardless of the situation, you don't want to keep the unnecessary user data in your system. 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 as you might discover some interesting financial allocations, and if so, you'll want to know who's responsible.

Note. 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.

Select PeopleTools, Security, Security Objects, Tables to Skip to access the Bypass Tables page.

If there's a table that stores data associated with user profiles which you want to preserve, add a row to the Bypass Tables page. Then select either a PeopleTools security table or a PeopleSoft application security table from the Record (Table) Name drop-down list box.

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.

Note. 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.

   This includes DDDAUDIT and SYSAUDIT to check the consistency of your database.

Tracking Users' Signin and Signout Activity

PeopleSoft Security provides two audit logs which tracks users' signin and signout activity in PeopleSoft. Signin activity includes timeouts, browser closings and browser freezes.

Access these logs by navigating to Security, Review Security Information. Select one of the following logs:

- Access Activity by User

View a single user's signin and signout activity. This log includes a user's Client IP address, signin times and signout times.

- Access Activity by Day

  View one or more days of all user signins and signouts. This log includes User IDs, Client IP addresses, signin times and signout times.

These logs are generated using data from the PSACCESSLOG table. If you are not interested in employing this functionality, delete the PSACCESSLOG table. Deleting this table does not result in any negative impact.

Note. If you deleted the PSACCESSLOG table and would like to track Users' signin and signout activity again, you must recreate the table using the same exact column names and order as were in the previous PSACCESSLOG table: OPRID, LOGIPADDRESS, LOGINDTTM, LOGOUTDTTM.

CHAPTER 6

Employing LDAP Directory Services

This chapter provides an overview of the PeopleSoft Lightweight Directory Access Protocol (LDAP) solution and discusses how to:

- Configure the LDAP directory.
- Cache the directory schema.
- Create the authentication map.
- Create user profile maps.
- Create role membership rules.
- Delete directory configurations.
- Enable signon PeopleCode for LDAP authentication.
- Use LDAP over SSL (LDAPS).
- Set up SSL on the directory (examples).

Note. This chapter assumes you have a working knowledge of LDAP-enabled directory servers.

Understanding the PeopleSoft LDAP Solution

PeopleSoft delivers three technologies that enable you to:

- Authenticate against an LDAP V3 compliant directory server.
- Reuse your existing user profiles stored within LDAP.

The three technologies are:

- Directory Business Interlink: Exposes the LDAP to PeopleCode.

  The system uses it for all communication with the LDAP server process running on a directory server.
- 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: This is PeopleCode that is carried out 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 can configure and extend the Signon PeopleCode to work with any schema implemented in your directory server.

The following topics involve 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.

Note. 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.

Configuring the LDAP Directory

This section provides an overview of LDAP directory configuration and discusses how to:

- Specify network information for LDAP.
- Specify additional connect DNs.
- Install selected PeopleSoft-specific schema extensions.
- Test the connectivity.

Understanding LDAP Directory Configuration

The Configure Directory component contains four pages that you use for specifying connection information and testing directory server connections.

To enable your PeopleSoft system to successfully connect to your directory server, you must enter the appropriate connection information. This includes the server name (DNS or IP address) and the listening port number. You also must enter the user distinguished name (User DN) and associated password.

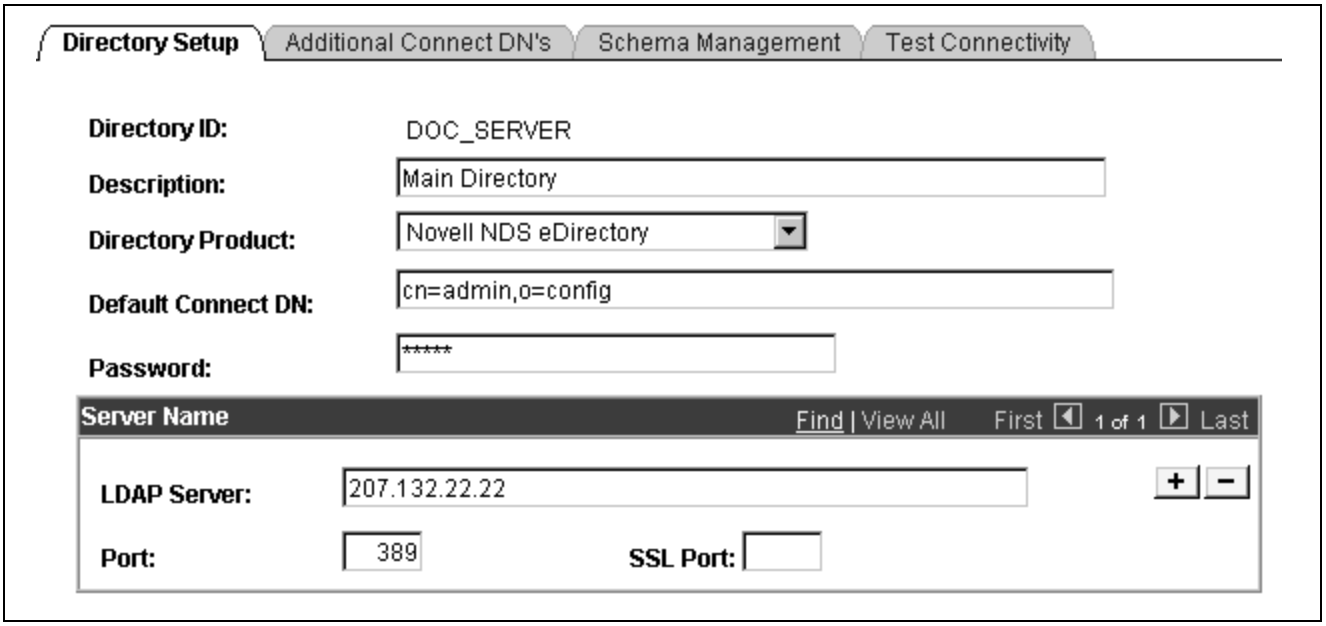
The PeopleSoft application server uses the User DN and password to connect to the LDAP server to retrieve user profile information about the specific user signing in to the system. The User DN must reflect a user with the appropriate LDAP browse rights.

Pages Used to Configure the Directory

Page Name	Object Name	Navigation	Usage
Directory Setup	DSDIRSETUP	PeopleTools, Security, Directory, Configure Directory, Directory Setup	Specify the network information of your LDAP directory servers, such as sign-in IDs and passwords.
Additional Connect DN's	DSSERVERID	PeopleTools, Directory, Configure Directory, Additional Connect DN's	Specify connect DNs in addition to the default connect DN specified on the Directory Setup page.
Schema Management	DSEXTINSTALL	PeopleTools, Security, Directory, Configure Directory, Schema Management	Install selected PeopleSoft-specific schema extensions into your directory.
Test Connectivity	DSSRCHRSLT	PeopleTools, Security, Directory, Configure Directory, Test Connectivity	Test the distinguished names and search criteria that you entered on the previous pages of the Configure Directory component and view the results. The system tests the connectivity when you access this page.

Specifying Network Information for LDAP

Access the Directory Setup page.



Directory Setup page

Directory ID Identifies the directory connection that you are creating. The directory ID that you enter can identify a specific LDAP server or a collection of LDAP servers depending on how many servers you add in the Server Name section.

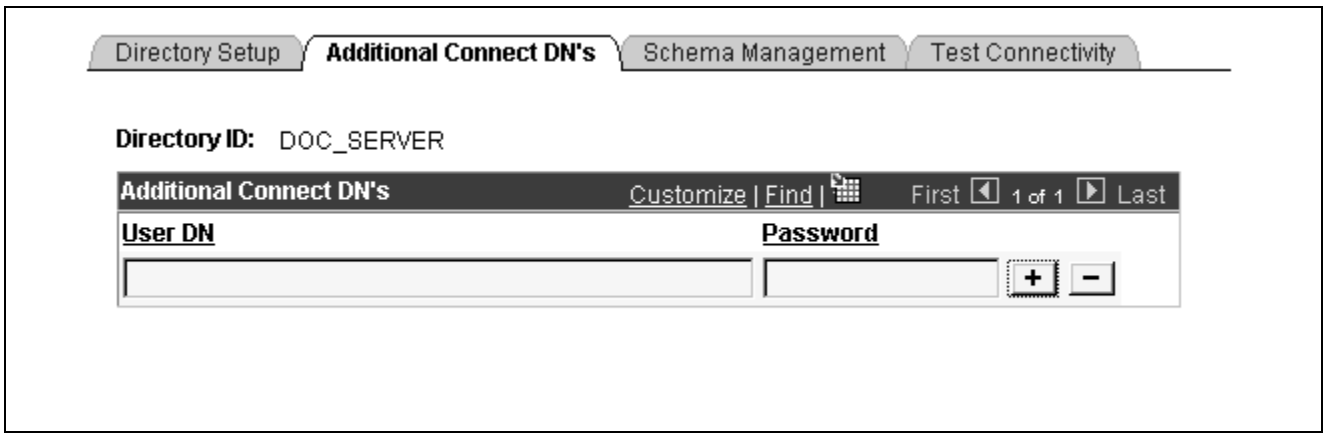
Description	Enter a description of the directory connection.
Directory Product	Select your directory product from the list of options.
Default Connect DN (default connect distinguished name)	Displays the default connect DN associated with the directory ID that you entered or selected on the initial search page. The connect DN is the ID that you can use to connect to the directory server. You can enter an alternative connect DN.
Password	Enter the password associated with the directory-based account that appears in the Default Connect DN field.

Note. The password is stored in encrypted form in the database; not even individuals with administration access to the database can view the password.

Server Name	Add LDAP directory servers to a connection list. You can add multiple servers for failover purposes using the plus button. All servers you add must participate in the same directory service.
LDAP Server	Identify a specific LDAP server. You can use the DNS name or you can use IP address dotted notation. For example, either of the following formats is acceptable: ldap12.yourcompany.com or 192.201.185.90.
Port	Enter the port number on which the LDAP server is configured to receive search requests. The standard LDAP port is 389. If you do not specify the correct port, PeopleSoft Directory Interface can't exchange data with your LDAP server.
SSL Port	If you are implementing SSL, enter the SSL port on the LDAP server.

Specifying Additional Connect DNs

Access the Additional Connect DN's page.



Additional Connect DN's page

The PeopleSoft application server uses the User DN and password specified on this page to connect to the LDAP server to retrieve user profile information about the specific user signing in to the system. The User DN must reflect a user with the appropriate LDAP browse rights.

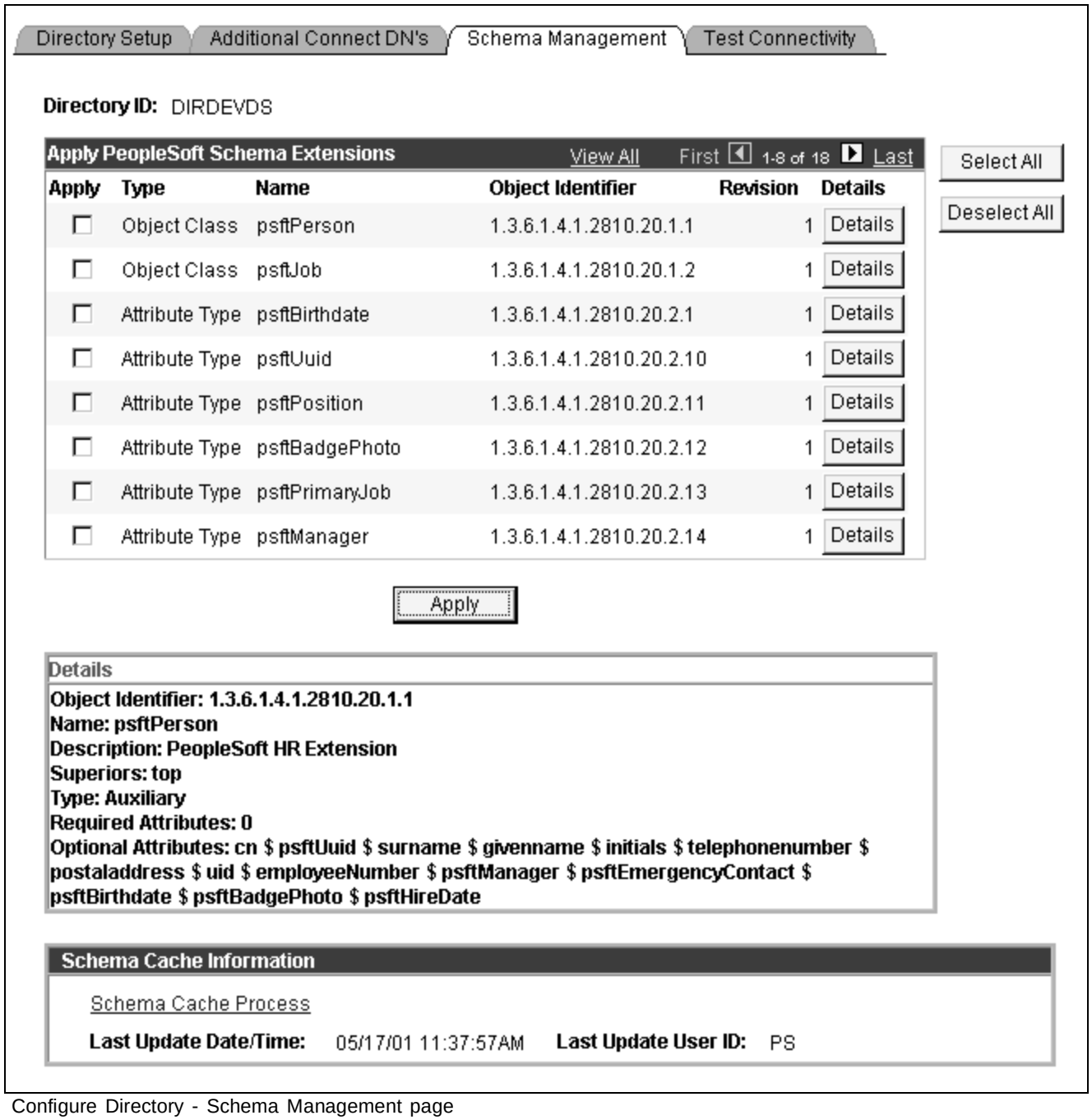
Note. Unless you have installed the PeopleSoft Directory Interface you will not see any available schema extensions.

User DN Add any DNs that you need in addition to the default connect DN that you entered on the Directory Setup page. The default user ID is most likely an administrative ID. This enables you to set up a more secure user ID for the scope of the mapping.

Password For each additional DN that you enter, add the corresponding password.

Installing Selected PeopleSoft-Specific Schema Extensions

Access the Schema Management page.



Configure Directory - Schema Management page

Note. Unless you have installed the PeopleSoft Directory Interface product, you might not have any PeopleSoft schema extensions available to you.

Apply	Select this check box to apply the selected schema extension type to your directory.
Type	Displays the type of schema extension: either *Object Class* or *Attribute Type.*
Name	Displays the schema extension name.
Object Identifier	Displays the schema extension object identifier. The sequence 1.3.6.1.4.1.2810.20 identifies the object as a PeopleSoft object. The second to last number is either a 1 or a 2. A *1* indicates an object class type and a *2* indicates an attribute type. The last number indicates the sequence in which the extension was created.
Revision	Displays the number of times that the schema extension was revised.
Details	Click to display details about the selected schema extension in the Details region at the bottom of the page.
Select All	Click to select all the schema extensions to apply to your directory.
Deselect All	Click to deselect every schema extension.
Apply	Click to apply the selected schema extensions to your directory.

Details

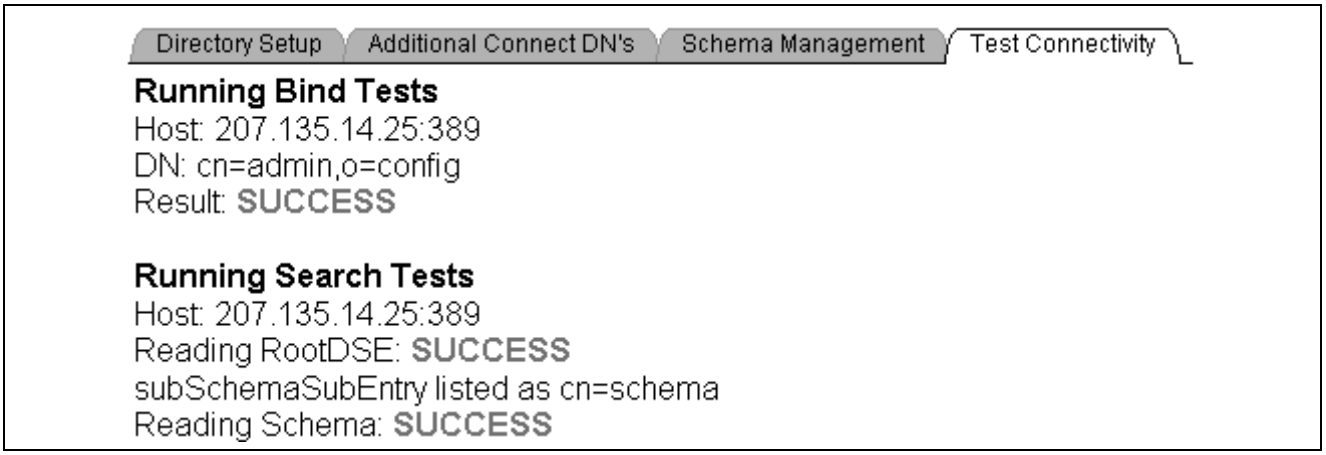
When you click a schema extension's Details button, the system displays the details of that extension. In addition to the object identifier and name, you may also be interested in the Superiors detail, which indicates which extensions are above this one on the hierarchy, if any. Also of interest is the Type detail, which indicates whether the schema extension is a mandatory, optional, or auxiliary extension.

Schema Cache Information

For convenience, you can use the Schema Cache Process link to transfer you to the Schema Cache page so that you can invoke the Schema Cache process. Last Update Date/Time and Last Update User ID enable you to monitor the frequency of updates as well as the last administrator to run the process.

Testing the Connectivity

Access the Test Connectivity page.



Test Connectivity page

The page displays the results (PASS or FAIL) of the connectivity test. If connectivity fails, modify the connect information on the Directory Setup and Additional Connect DN's pages.

Caching the Directory Schema

You use the Cache Schema page to specify a directory server and invoke an Application Engine program designed to create a cache in the PeopleSoft database of the directory schema. This enables you to select names of object classes and attribute types when creating security maps.

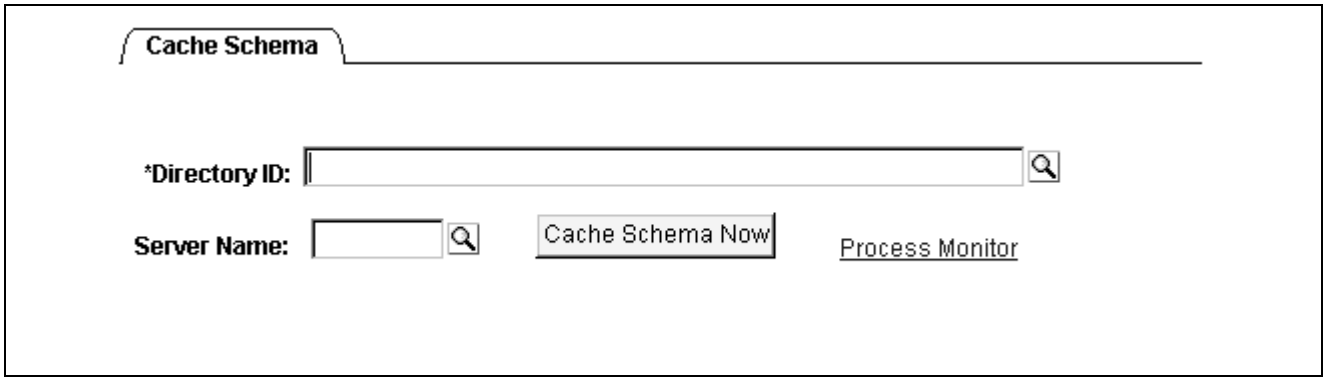
This section discusses how to create a cache of the directory schema.

Page Used to Cache the Directory Schema

Page Name	Object Name	Navigation	Usage
Cache Schema	DSSCHEMACACHE	PeopleTools, Security, Directory, Cache Directory Schema	Specify a directory server and invoke an Application Engine program designed to create a cache in the PeopleSoft database of the directory schema. The cache of the LDAP schema is used to simplify creating maps for authentication and user profile maintenance.

Creating a Cache of the Directory Schema

Access the Cache Schema page.



Cache Schema page

Directory ID Select the directory ID to identify the directory that the system should connect to and retrieve schema information from.

Server Name Search for the Process Scheduler server on which the Cache Schema process should run.

Cache Schema Now Click this button to cache the LDAP schema data to tables within the PeopleSoft database. Typically, you use this option during initial setup and any time that the schema has changed.

Process Monitor After invoking the process, you can monitor the progress by clicking this link.

Creating the Authentication Map

Use the Authentication page only if you're implementing directory authentication as opposed to storing authentication information in the PeopleSoft database. You create authentication maps to define mappings to one or more directories that the PeopleSoft system relies on for authenticating users. You can activate multiple authentication maps. Your PeopleSoft LDAP system authenticates users against all active authentication maps.

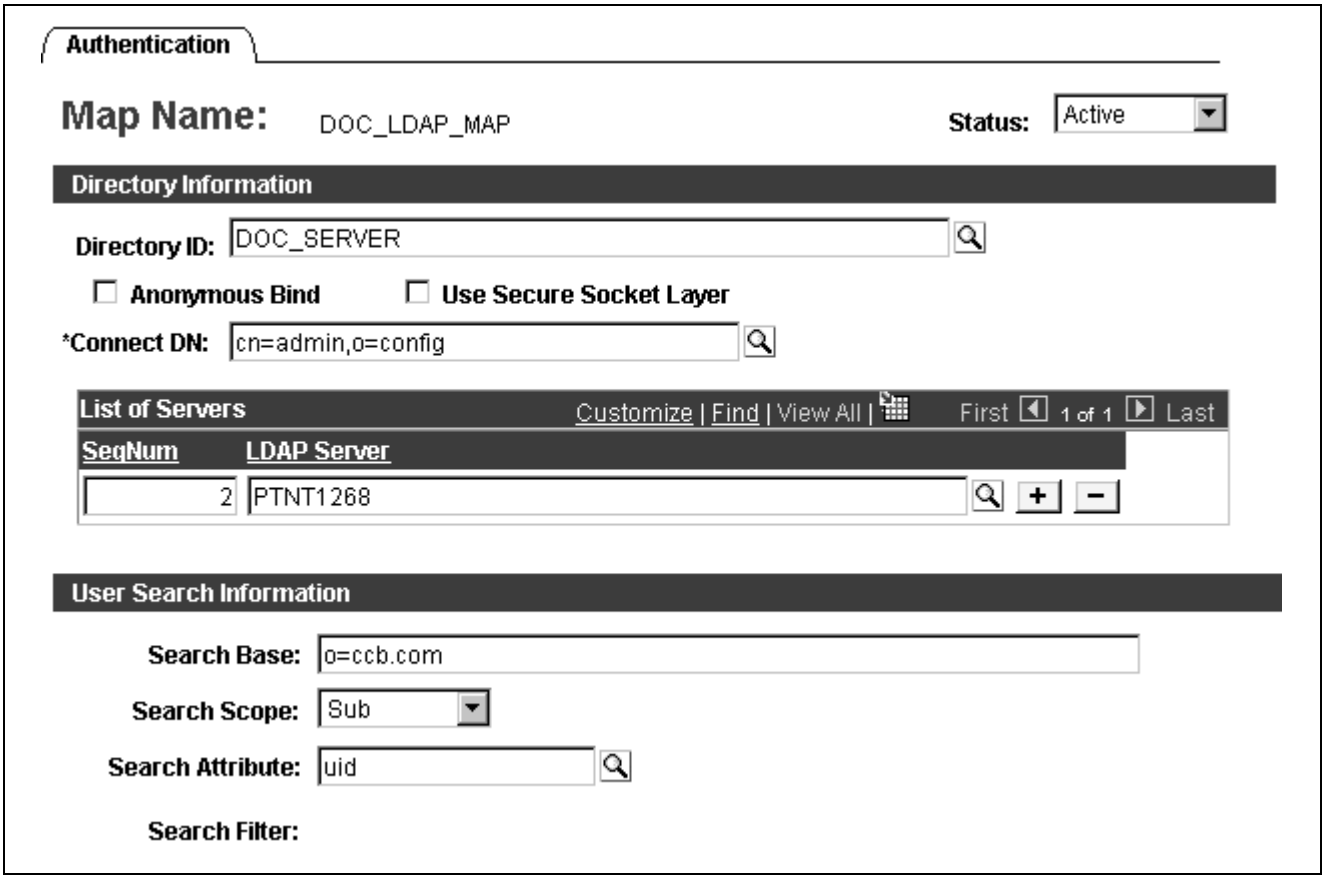
This section discusses how to create the authentication map.

Page Used to Create the Authentication Map

Page Name	Object Name	Navigation	Usage
Authentication	DSSECMAPMAIN	PeopleTools, Security, Directory, Authentication Map	Create a mapping to the directory that the PeopleSoft system relies on for authenticating users.

Creating the Authentication Map

Access the Authentication page.



Authentication page

Status Activate an authentication mapping by selecting *Active.* To disable an authentication mapping, select *Inactive.*

Directory Information

Directory ID Select the directory ID of the directory that you intend to use for authentication.

Anonymous Bind If all directory data required for authentication and user profile maintenance is visible to an anonymous connection, then select this check box.

Use Secure Socket Layer Select this option if you are implementing an SSL connection between PeopleSoft and the directory server.

If you do not specify a port number, the system uses the default LDAPS port.

Connect DN This value is the default connect DN that you specified on the Directory Setup page. To select one of the DNs specified on the Additional Connect DN's page, click the search button.

Note. If Anonymous Bind is selected, the Connect DN will be ignored.

List of Servers

SeqNum (sequence number) Set the order in which the system should access the list of servers for authentication.

LDAP Server Select the name of the LDAP server. Use the plus button to enter additional servers.

User Search Information

Search Base Enter the root of the directory information tree under which the system should search for user information.

Search Scope Select the search scope for this search. Values are:

Base: Not applicable. You should use *Base* on the authentication map.

One: The query searches only the entries one level down from the entry in the Search Base field.

Sub: The query searches the entire sub tree beneath the search base entry.

Search Attribute When a user signs on using LDAP Authentication, the system searches the directory to find the user's user entry. The search attribute is used to construct the LDAP search filter used in finding the person's user entry. The value in the Search Attribute field will be entered by the user when the user signs on.

Enter the attribute to be returned by the search, such as user ID (uid) or customer ID (cid).

Search Filter Displays the LDAP search filter that the system uses to search the directory for equal entries.

Creating User Profile Maps

This section provides an overview of user profile options and discusses how to:

- Specify mandatory user properties.
- Specify optional user properties.

Understanding User Profile Options

If you are going to authenticate users with the directory server, a PeopleSoft User Profile is still required. That is, a row is still required in the table in which PeopleSoft user information is stored (PSOPRDEFN). In this context, you "cache" LDAP user information inside your PeopleSoft system. The properties that you specify on the Mandatory and Optional User Properties pages are the columns in PSOPRDEFN that the system populates with values from your directory server. These values comprise your user profile options.

PeopleSoft applications use this cache of user information, not your directory server. Whenever a transaction requires user information, the application refers to the local PSOPRDEFN table as opposed to querying the directory server. This improves performance.

After a user signs onto the system and the Signon PeopleCode is carried out, PeopleSoft creates a row for that user in the user definition table by retrieving the LDAP information and creating a local cache. Signon PeopleCode maintains this row automatically; there is no need for any manual updates. Any changes made in the directory server are reproduced in the local cache.

Some properties are required when creating a PeopleSoft User Profile; these properties appear on the Mandatory User Properties page. Other properties are optional, and these appear on the Optional User Properties page.

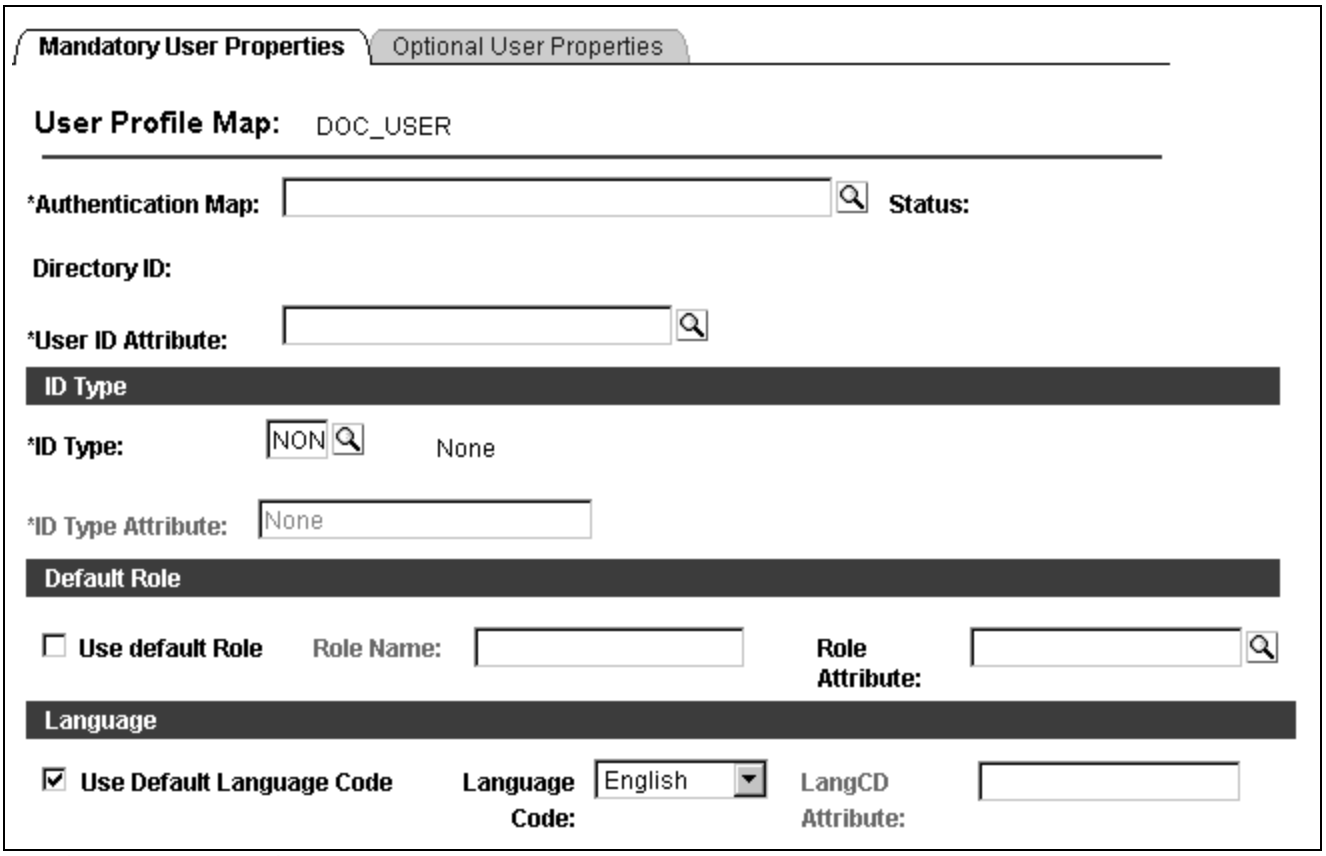
Note. You must supply user properties to Signon PeopleCode only if you intend to authenticate users with your LDAP directory.

Pages Used to Create User Profile Maps

Page Name	Object Name	Navigation	Usage
Mandatory User Properties	DSUSRPRFLMANMAP	PeopleTools, Security, Directory, User Profile Map, Mandatory User Properties	Specify the attributes required for signon. You can select to have the system retrieve these mandatory values from the directory server, or you can enter default values.
Optional User Properties	DSUSRPRFLOPTMAP	PeopleTools, Security, Directory, User Profile Map, Optional User Properties	Specify optional user properties to retrieve from the directory.

Specifying Mandatory User Properties

Access the Mandatory User Properties page.



Mandatory User Properties page

Authentication Map Select the authentication map to associate with this user profile mapping. The server and connection information are taken from the authentication map.

Status Displays the status of the selected user profile map.

Note. Only one user profile map should be active at any time.

Directory ID Displays the directory ID associated with the authentication mapping.

User ID Attribute Displays the value used to populate the OPRID (user ID) field on PSOPRDEFN.

ID Type

ID Type Similar to Symbolic ID, enter this value on this page. This is the default ID type for new users, such as Employee ID, Customer ID, and so on.

ID Type Attribute Specifies the LDAP attribute in the directory that holds the selected ID value. For instance, the ID value might be Employee ID. Some ID types require additional data when creating a profile of that type. LDAP User Profile Management can retrieve that data from the LDAP directory if it is available.

Default Role

Use Default Role Select this option if you want to use the default role. If you enable this option, the Default Role edit box becomes available for entry while the Role Attribute edit box becomes unavailable for entry. You either specify a default role or specify an LDAP attribute on the user entry that holds the valid name of a PeopleSoft Role.

Role Name Enter the name of a default role to be assigned to new users. This value applies to users the first time that they sign on and have not had any roles dynamically assigned to them. Typically, this role has only basic access authorizations, such as for only the self-service pages. Users should get most of their permissions through dynamically assigned roles.

Role Attribute Instead of specifying only a single default role for each and every user, you can enter a value for the LDAP attribute that holds the name of a PeopleSoft role to be assigned to the user.

You can enable your application to automatically apply a role for the user. When signing in to the application, the user provides a value for the search attribute you specified in the authentication map. The system uses that attribute value to search for the user's entry in the LDAP directory, then imports the group containing the entry to the PSOPRDEFN table as the user's role.

To enable this automatic role import feature:

1. Define LDAP groups with names that exactly match the roles defined for your application.
2. Clear the Use Default Role check box on this page.
3. Leave the Role Name and Role Attribute fields on this page blank.

Language

Use Default Language Code Select if you do not maintain language codes in the directory.

Language Code If the default language code is not stored in the directory, then select a default value from the drop-down list box.

LangCD Attribute (language code default) — The name of the LDAP attribute containing a valid language code. The value retrieved from the attribute must be a valid PeopleSoft language code.

Specifying Optional User Properties

Access the Optional User Properties page.

User Profile Property — Select the user profile property that you want to add to the local cache. These properties are described in the following table.

Use Constant Value — To supply a constant value for each user, select this option.

Attribute Name — Add the name of the attribute as it is represented in your LDAP schema.

Constant Value — Appears only if you have selected Use Constant Value.

Always Update — Select this option if you always want the system to update the local user cache to reflect the data stored in the directory server every time the user signs on. If Always Update is not selected, the data will be taken from the directory only when the profile is first created.

The following are optional user properties that you can select from the User Profile Property search button.

Currency Code — If the user deals with international prices, set the currency code to reflect the native or base currency so that values appear in the currency with which the user is familiar.

Email Address — Select if a user is part of your workflow system or you have other systems that generate emails for users.

Multi-Language Enabled — Select if the user is set up to use PeopleSoft with multiple languages.

Navigator Home Page — The homepage is associated with PeopleSoft Workflow (Navigator Homepage).

Primary Permission List — PeopleSoft determines which data permissions to grant a user by examining 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 PeopleSoft application documentation for more detail. PeopleSoft also determines mass change and definition security permissions from the primary permission list.

Process Profile Permission List — The process profile contains the permissions that a user requires for running batch processes through PeopleSoft Process Scheduler. For example, the process profile authorizes users to view output, update run locations, restart processes, and so on. Only the process profile comes from this permission list, not the list of process groups.

Row Security Permission List — See explanation for the Primary Permission List field.

Symbolic ID — If the symbolic ID is required for the user, select this option.

User Description — Displays, typically, the name of the user, such as an employee name or a vendor name.

User ID Alias — In some cases, the user ID is an alias in the form of an email address. If so, select this option.

Creating Role Membership Rules

Use the Role Policy page to define the rules that are read by Dynamic Role Rule PeopleCode and populate PeopleSoft roles with members. The rules return the DNs of "people" directory entries, which supply the system with the user IDs specified on the user profile mapping.

This section provides an overview of role membership rules and discusses how to define role membership rules.

Understanding Role Membership Rules

PeopleSoft security roles are comparable to LDAP directory groups. Roles enable you to group user IDs in logical sets that share the same security privileges. PeopleSoft enables you to keep your external directory groups synchronized with the data stored within the PeopleSoft database.

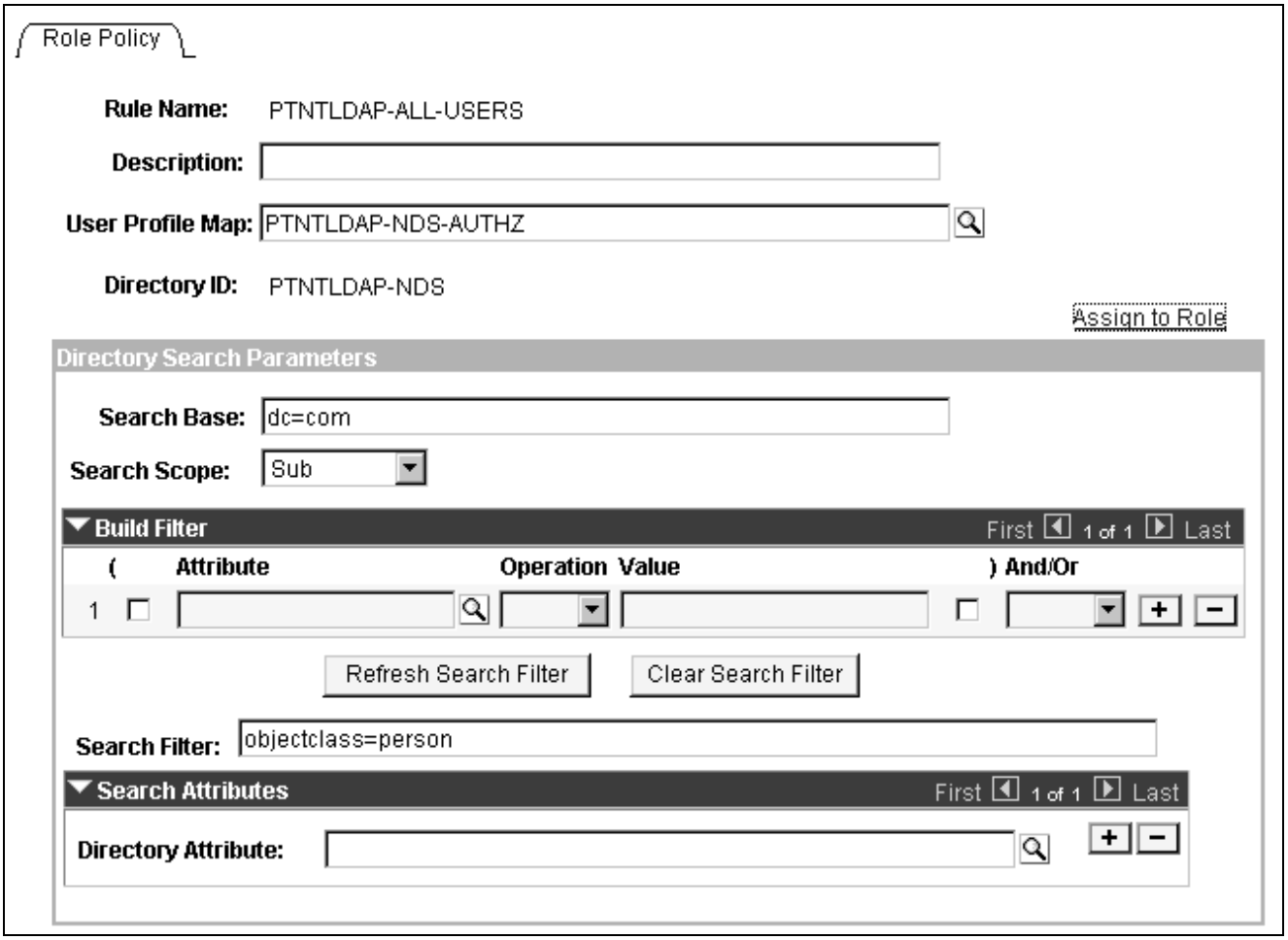
It is important to keep the data within PeopleSoft consistent with any changes made to the structure or content of the external directory server. This is especially crucial when dealing with security data. The Role Membership Rules page enables you to modify a PeopleSoft role based on directory criteria.

Page Used to Create Role Membership Rules

Page Name	Object Name	Navigation	Usage
Role Policy	DSSECROLERULE	PeopleTools, Security, Directory, Role Membership Rules	Define the rules that are read by Dynamic Role Rule PeopleCode and populate PeopleSoft roles with members.

Defining Role Membership Rules

Access the Role Policy page.



Role Policy page

Rule Name Displays the directory search name that you entered on the search page.

Description Enter a short description of the rule.

User Profile Map Select the user profile map to associate with the rule.

Directory ID Displays the directory associated with the user profile map that you select.

Assign to Role Click this link to automatically start the Dynamic Members page in the Roles component of the Security menu. On that page, select Directory Rule Enabled and specify the server on which to carry out the rule.

Directory Search Parameters

Search Base Enter the entry (or "container") at which to begin the search.

Search Scope Select the search scope for this search from the following options:

Base: The query searches only the value in the Search Base field.

One: The query searches only the entries one level down from the value in the Search Base field.

Sub: The query searches the value in the Search Base field and all entries beneath it.

Build Filter

( ) Parentheses; on either side of the filter expression select the check boxes below the parentheses to group expressions.

Attribute Select the attribute that the system will filter.

Operation Assign an operator to your rule, such as <, <=, <>, =, >, or >=.

Value Enter the value to assign to the attribute that you specified.

And/Or To add another line to your rule, select *AND* or *OR*, depending on your rule logic. Select *END* to signify the end of the search. Select *NONE* if you aren't using this kind of filter.

Refresh Search Filter After you make changes using the Build Filter options, click this button to update the Search Filter edit box to reflect the changes.

Clear Search Filter Click this button to delete all values from the Search Filter edit box and the Build Filter selections.

Search Filter The purpose of this field depends on whether you also specify values in the Directory Attribute field, as follows:

- No directory attributes specified.

  Enter a name=value pair that identifies a key field and value on the user record. The system applies this criterion to search for an individual user, regardless of group membership.

- One or more directory attributes specified.

  Enter a name=value pair that the system applies to the search for the DN of the defined container or group. This value typically displays the directory object class of the container in the form "objectclass = GroupOfUniqueNames", for example. This indicates what type of container to search. To retrieve the correct container DNs, the system adds the name of the container to the search filter at runtime.

Search Attributes

Directory Attribute Select attributes that identify the user to add to this membership. This searches for members only within the group that's specified by the Search Filter field.

Note. You can also write PeopleCode to determine group membership using any arbitrary LDAP search criteria.

Deleting Directory Configurations

You can delete the entire directory configuration or just parts of it.

This section discusses how to:

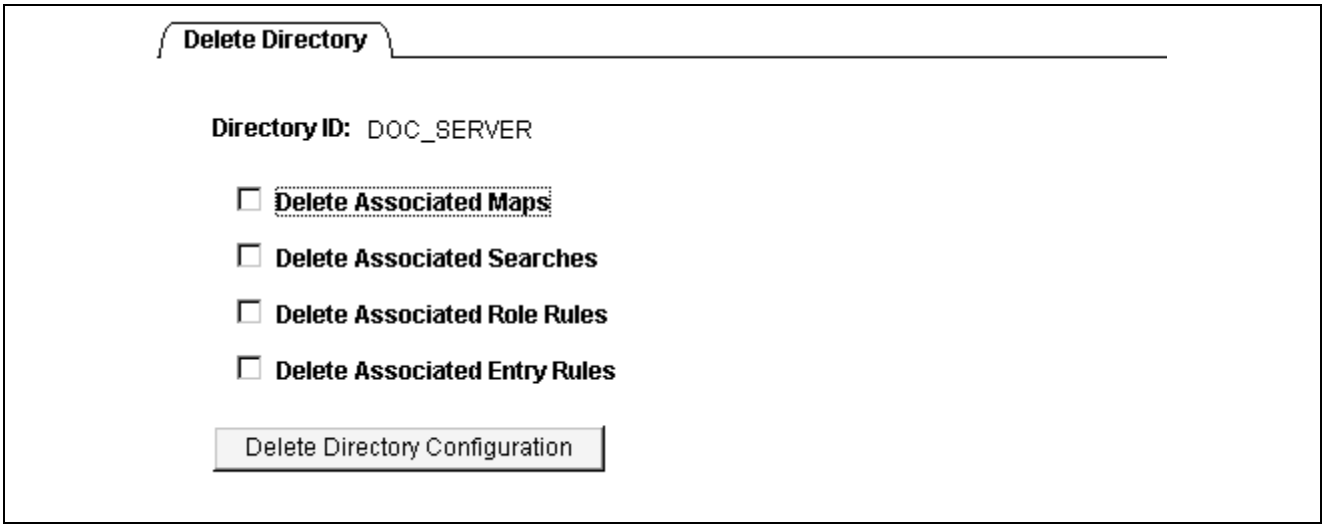
- Delete the directory configuration.
- Work with the workflow address book.

Page Used to Delete Directory Configurations

Page Name	Object Name	Navigation	Usage
Delete Directory	DSPURGEDIRID	PeopleTools, Security, Directory, Delete Directory Configuration	Delete the entire directory configuration or just parts of it.

Deleting the Directory Configuration

Access the Delete Directory page.



Delete Directory page

Delete Associated Maps Deletes the authentication and user profile maps from the configuration.

Delete Associated Searches Deletes any searches related to the directory configuration.

Delete Associated Role Rules Deletes any role rules that you have specified for a configuration.

Delete Associated Entry Rules This applies to the PeopleSoft Directory Interface product only.

Delete Directory Configuration After you have made the appropriate choices, click this button to perform the delete process. If you click this button with nothing selected, the system deletes only the directory ID and leaves all of the other configuration information intact.

Working with the Workflow Address Book

Select PeopleTools, Security, Directory, Workflow Address Book to access the Address Book page.

Use the Address Book page for configuring LDAP address lookups for use with user-initiated notifications in PeopleSoft Workflow. This page contains the controls needed to retrieve the necessary addresses from the directory. This page applies only if you store user information in a directory.

Note. Each of these controls is discussed elsewhere in this chapter.

See Also

Enterprise PeopleTools 8.45 PeopleBook: Workflow Technology, "Adding Events and Routings"

Enabling Signon PeopleCode for LDAP Authentication

LDAP Authentication runs as Signon PeopleCode that must be enabled and configured to be carried out with proper permissions.

To enable Signon PeopleCode:

1. Select PeopleTools, Security, Security Objects, Signon PeopleCode to access the Signon PeopleCode page.
2. Click the Invoke As option 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 the user ID of the user who happens to be signing on to the system? Either way, the value for the user ID and 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.

   Note. 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. Select the Enabled check box (if it is not already selected automatically by the system).
5. Ensure that the Exec Auth Fail check box is selected; if PeopleSoft authorization fails, then Signon PeopleCode is carried out.

   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.

Note. If you intend to use the User Profile Map, you also need to enable LDAP_PROFILESYNCH. The same options apply.

Using LDAP Over SSL (LDAPS)

You can use the LDAP Business Interlink to establish a secure LDAP connection between the application server and the LDAP server. The LDAP Business Interlink uses Netscape's certificate database, cert7.db. You can obtain a cert7.db using the PKCS Utilities distributed by Netscape. Refer to Netscape's documentation for more information on obtaining and using the PKCS Utilities.

To establish the secure connection between the PeopleSoft Application Server and the LDAP server you will need the following:

- Cert7.db certificate database from Netscape.
- A Server Certificate for the LDAP server.
- The Trusted Root Certificate from the Certificate Authority (CA) that issues the Server Certificate.

To enable LDAP authentication over SSL:

1. Follow the documentation for your directory server to add the Server Certificate to your directory server.
2. Using Netscape's PKCS Utilities, add the Certificate Authorities Trusted Root Certificate to the cert7.db certificate database.
3. Place the cert7.db file in the %PeopleTools%\bin\server directory of the application server.
4. Select PeopleTools, Security, Directory, Configure Directory, Directory Setup to access the Directory Setup page, and make sure that the SSL Port field reflects the correct LDAPS port for your directory server.
5. Select PeopleTools, Security, Directory, Authentication Map to access the Authentication Map page, and select the Use Secure Sockets Layer check box.
6. In Application Designer, open the following Business Interlinks, select the Settings tab, and change the SSL setting to YES:
   - LDAP_SEARCH
   - LDAP_BIND

Setting Up SSL on the Directory (Examples)

If you require SSL between your LDAP directory server and your PeopleSoft system, the following topics provide sample procedures for doing so.

This section provides an overview of SSL and the directory and discusses how to:

- Set up SSL for Novell NDS.
- Set up SSL for Netscape (iPlanet).

Note. The procedures outlined in this section are provided as samples. They may not necessarily apply to all situations.

Understanding SSL and the Directory

SSL is a protocol developed by Netscape that defines an interface for data encryption between network nodes. To establish an SSL-encrypted connection, the nodes must complete the SSL handshake. The simplified steps of the SSL handshake are as follows:

1. Client sends a request to connect.
2. Server responds to the connect request and sends a signed certificate.
3. Client verifies that the certificate signer is in its acceptable certificate authority (CA) list.
4. Client generates a session key to be used for encryption and sends it to the server encrypted with the server's public key (from the certificate received in step 2).
5. Server uses its private key to decrypt the client generated session key.

Establishing an SSL connection requires two certificates: one containing the public key of the server (server certificate or public key certificate) and another to verify the CA that issued the server certificate (Trusted Root certificate). The server needs to be configured to issue the server certificate when a client requests an SSL connection and the client needs to be configured with the Trusted Root certificate of the CA that issued the server certificate.

The nature of those configurations depends on both the protocol being used and the client and server platforms. In most cases you replace HTTP with Lightweight Directory Access Protocol (LDAP). SSL is a lower level protocol than the application protocol, such as HTTP or LDAP. SSL works the same regardless of the application protocol.

Note. Establishing SSL connections with LDAP (LDAPS) is not related to web server certificates or certificates used with PeopleSoft integration.

Setting Up SSL for Novell NDS

This section discusses how to configure the LDAP business interlink to establish SSL encrypted LDAP connections. The LDAP business interlink uses a certificate database that resides on the file system of the PeopleSoft Application Server. The certificate database is a file called cert7.db and needs to reside in the file system of the application server. The cert7.db certificate database needs to contain the Trusted Root certificate of the CA that issued the Server Certificate of the LDAP server.

Setting Up the Certificate

To obtain a cert7.db, you must download Netscape Navigator 4.7. Once this is downloaded and installed, launch Netscape Navigator, which prompts you to create a user profile. Create a user profile with the name of PeopleSoft. This will create the following directory structure: Netscape\Users\PeopleSoft.

To import the certificate:

1. In the PeopleSoft directory, find cert7.db.
2. With Netscape Navigator open, click the Security button at the top.

   The Security Information page appears.
3. Select Certificates and Signers.

   This displays the valid certificates in the database.
4. You can delete all of them. Once they are deleted, click OK, then close Netscape Navigator.
5. Import the CA's certificate into the cert7.db certificate database.

You are ready to configure the LDAP business interlink for SSL. There are two relevant settings on all transactions of the business interlink:

- SSL setting.
- SSL_DB location setting.

As with all business interlink inputs, these can be set using either Application Designer or PeopleCode.

To make the settings using Application Designer:

1. Open an existing instance of the LDAP business interlink, or create a new instance.
2. Select the Settings tab.
3. Set the SSL parameter to *YES*.
4. Set the SSL_DB parameter to the name of your certificate database (cert7.db by default).
5. Save the business interlink.

To make the settings using PeopleCode, drag the business interlink definition into the PeopleCode editor. The following code is created:

```
/* ===>
   This is a dynamically generated PeopleCode template to be used only as a helper
to the application developer.
You need to replace all references to '<*>' OR default values with  references to
PeopleCode variables and/or a Rec.Fields.*/

/* ===> Declare and instantiate: */
Local Interlink &LDAP_SEARCH_1;
Local BIDocs &inDoc;
Local BIDocs &outDoc;
Local boolean &RSLT;
Local number  &EXECRSLT;
&LDAP_SEARCH_1 =  GetInterlink(INTERLINK.LDAP_SEARCH);

/* ===> You can use the following assignments to set the configuration parameters.
*/

&LDAP_SEARCH_1.SSL = "NO";
&LDAP_SEARCH_1.SSL_DB = "cert7.db";
&LDAP_SEARCH_1.URL = "file://psio_dir.dll";
&LDAP_SEARCH_1.BIDocValidating = "Off";
…..
```

Note. This example uses the Search transaction, but the same principle applies to any transaction.

You must change the .SSL and .SSL_DB settings to indicate that SSL should be used, and specify the name of your certificate database file. For example:

```
&LDAP_SEARCH_1.SSL = "YES";
&LDAP_SEARCH_1.SSL_DB = "cert7.db";
```

Configuring Your LDAP Server for SSL

This section describes how to configure NDS eDirectory V8.5 for LDAPS using the Organizational CA built into NDS's PKI services.

To configure NDS eDirectory V8.5 for LDAPS:

1. Export the Self Signed Trusted Root Certificate from the CA.
    a. Start Console1 and navigate to the Organizational CA object in the Security container:
    b. Open the Properties dialog, go to the Certificates tab, and choose Self Signed Certificate from the menu.
    c. Click the Export button.
    d. In the Export a Certificate dialog box, choose binary DER format, designate a file name and location, and click Export.
    e. Rename this file using an .X509 file format.
2. Create a Server Certificate to be used by LDAP.
    a. In Console1, navigate to the container that holds the Server Object for the LDAP Server:
    b. Right-click the container entry (such as Config), and select NewObject. Scroll down and find NDSPKI:Key Material in the list, and click OK.

c. In the Create Server Certificate dialog box, make sure that the server name is the name of the directory server running the LDAP service. Also, give the new certificate a meaningful name, select the Standard creation method, and click Next:

d. Review the information in the next dialog box, and click Finish. You should now have a certificate that contains the public key for the server running the LDAP service stored in your directory as an object:

3. Indicate to the LDAP service which port to use for SSL connections and to issue the certificate when a client requests a connection on that port.

   a. Find the object representing your LDAP Server; it will be in the same container that you just created the certificate in and it will be named "LDAP Server - <hostname>-NDS."

   b. Open the properties dialog box on the LDAP Server object, and select the SSL Configuration tab.

   c. Enter the port number that you want to use for LDAPS, and in the SSL Certificate field, click the browse button to select the certificate that you just created. *Do not* check Enable and Require Mutual Authentication unless you have configured this option (which is outside the scope of this discussion).

   Note. Under your Novell Install Directory there should be a file called X509.REG. The path should be similar to install_directory\CERTSERV\MISC\X509.REG. Take this file and move it to the machine on which you've installed Netscape. From the machine that uses Netscape, run the X509.REG file by double-clicking it. This updates your registry so that Netscape can import the certificate.

4. Import the certificate.

   a. Launch Netscape, select File, Open, and enter the file location of the .X509 certificate that you exported from NDS.

   b. Netscape will take you through the certificate import process. Follow along with the wizard until finished. To confirm proper install, you click the security tab (the lock) and open the security administrator for Netscape. Click the Certificates Signers link, which takes you to all valid certificates in the database. You should now see the certificate that you imported.

5. Move the cert7.db to the appserv folder.

   The system should now be running LDAPS with NDS.

Note. You are responsible for receiving certificates from a CA, such as Entrust.Net or Verisign.

Note. If you try to test this with the business interlink tester, the error code 89 is often reported. This does not mean that LDAPS is not working. To test, you can run a trace on the directory to see the SSL handshake occurring. You can also turn off port 389 and see if authentication still works. If it does, then this indicates that SSL is working.

Setting Up SSL for Netscape (iPlanet)

To set up SSL on Netscape:

1. Make sure that your directory is defined in the PeopleTools, Security, Directory component.
2. Modify the Signon PeopleCode page:

   a. Select PeopleTools, Security, Security Objects, Signon PeopleCode to access the Signon PeopleCode page.

b. Select the Invoke as radio button.

c. Enter the user ID and password of a user who has permission to run the Signon PeopleCode.

The password will not be visible once the page is saved.

d. Select the Enabled box to enable the Signon PeopleCode.

e. Enter the Signon PeopleCode location as shown in the default values.

f. Select the Exec Auth Fail box, because Signon PeopleCode is triggered when authentication fails against the PeopleSoft authentication.

g. Save the page.

Note. Make sure that the user ID entered above has permission to run the Component Interface USER_PROFILE.

---

3. Modify the LDAP_BIND and LDAP_SEARCH business interlink definitions:

a. Open Application Designer.

b. Open the LDAP_BIND definition.

c. Select the Input tab.

d. Enter the server name and port for the LDAP server.

The other parameters are not required for this procedure.

e. Select the Settings tab.

f. Select YES from the SSL drop-down list box.

g. In the SSL_DB edit box, enter the location of the certificate database; for example, *c:\peoplesoft\certificates*.

Note. This field should contain just the directory location, not the database filename.

---

h. Click Set Default to save the default settings.

i. Save and close the definition.

4. Consider the following items:

a. The application server binds as a client to the LDAP server as part of the authentication, so it is only necessary to have access to the Root Certificates.

The LDAP administrator at your site should have already installed a server (Node) Certificate on the LDAP Server.

b. The cert7.db file can be transferred to the application server in binary mode and installed in the same directory as PSAPPSERV.CFG and PSTUXCFG of the application server domain.

c. Using a copy of the LDAP server's cert7.db is not a security risk, as the Node Certificates are encrypted strings based on the host name and other site-specific parameters.

The application server accesses the Root Certificates, which are generally available at no charge from the CA.

5. Reboot the application server domain.

CHAPTER 7

Employing Signon PeopleCode and User Exits

This chapter provides an overview of the delivered external authentication solutions and discusses how to:

- Use Signon PeopleCode.
- Use the web server security exit.
- Use the Windows security exit.

Understanding the Delivered External Authentication Solutions

PeopleSoft delivers the most common authentication solutions and packages them with our application for you to use. This saves you the trouble of developing your own solutions and saves you time with your security implementation.

Note. The traditional method, where the user submits signon credentials that the system compares to a row in the PSOPRDEFN table, is a valid means of authentication; however, it is not a recommended method for increased scalability and manageability as you deploy applications to the internet.

The authentication solutions are delivered PeopleCode programs that you can include in your Signon PeopleCode. The following table describes each function that appears on the Signon PeopleCode page:

Function	Exec Auth Fail	Description
WWW_Authentication	Not Required	It applies when you want the browser to pass the client certificate to the web server for authentication by mutual authentication SSL at the web server level (also known as client authentication). In this situation, you configure PeopleSoft to "trust" the authentication performed by a third-party system at the web server. The function performs the following: 1. Extracts the user's distinguished name (DN) from the client certificate passed to the application server by the HTTP server. 2. Sets a global variable to the DN for a subsequent call to the LDAP_ProfileSynch function. 3. Converts the DN to a PeopleSoft user ID and sets the current user context.
LDAP_Authentication	Required	It applies when you want the user to submit signon credentials at the signon page, and then the system passes the credentials to the directory to perform authentication. This function performs the following: 1. Searches the directory for all entries that match the entered user name. 2. Attempts to bind to the directory for each found DN using the entered password. 3. Sets a global variable to the bound DN for a subsequent call to LDAP_ProfileSynch. 4. Converts the DN to the appropriate PeopleSoft Username and sets the current user context.

Function	Exec Auth Fail	Description
SSO_Authentication	Not Required	It applies in situations where you have single signon configured. The system authenticates the user's single signon token, which has already been issued by another database (node). This function performs the following: 1. Converts the PeopleSoft User ID to a DN. 2. Sets a global variable for a subsequent call to LDAP_ProfileSynch.
LDAP_ProfileSynch	Not Required	Applies to situations where PeopleSoft user profiles need to be created or updated with data stored in an LDAP directory. The function requires that the global variable &global_DN has been initialized by one of the previous authentication functions. Remember that regardless of how a user is authenticated, each user still populates a row in PSOPRDEFN to which applications can refer to during transactions (if necessary). The LDAP_ProfileSynch updates that row in PSOPRDEFN (or user profile cache) with the most current information. As delivered, this function performs the following: 1. Retrieves the LDAP entry specified by &global_DN. 2. Either creates or updates the corresponding PeopleSoft user profile. **Note.** One of the XXX_Authentication functions needs to be carried out prior to running LDAP_ProfileSynch. PeopleSoft has provided disabled example Signon PeopleCode with this function. If you work with the NDS, Active Planet, or iPlanet directories, you can use this Signon PeopleCode to assign roles dynamically at signon time. See Chapter 7, "Employing Signon PeopleCode and User Exits," LDAP_ProfileSynch Considerations, page 121.

When using any of the delivered external authentication solutions, the following items apply:

- All functions get the LDAP server configuration from specifications in PeopleTools Security, Directory, Configure Directory.
- All functions support a single database—multiple databases are not required.

This section discusses:

- WWW_Authentication considerations.
- LDAP_Authentication considerations.
- SSO_Authentication considerations.
- LDAP_ProfileSynch considerations.

WWW_Authentication Considerations

If you intend to authenticate your users at the web server level using mutual authentication SSL (also known as client authentication), the users that are authenticated at the web server level must signon to the system using a different website than users of the other authentication methods.

When you configure a PeopleSoft site to enable public access, a public user ID and password in the web profile provide automatic authentication. Keep in mind that this enables public access for the entire site. The web server always passes the specified public user ID and password to the application server. So, if you want some users to be authenticated by PeopleSoft rather than at the web server level, they must sign in through a PeopleSoft site that has public access disabled.

Note. The **RevalidatePassword** PeopleCode function does not work during a user session for which you're using WWW_Authentication.

In WWW_Authentication, PeopleSoft performs no validation of users and their passwords. The signon PeopleCode simply accepts the web server's word that the user was properly authenticated. Your PeopleSoft application has no way to revalidate the user's password in this case, so you shouldn't call **RevalidatePassword** after WWW_Authentication has been used.

You can determine whether WWW_Authentication has been used by examining a global variable. The signon PeopleCode for WWW_Authentication sets the PeopleCode global variable called *&authMethod* to the value *WWW* when a successful signon occurs. In PeopleCode where you want to call **RevalidatePassword**, first examine *&authMethod*. If it's not equal to *WWW*, you can call the function.

See Also

Enterprise PeopleTools 8.45 PeopleBook: PeopleCode Language Reference, "PeopleCode Built-in Functions," RevalidatePassword

LDAP_Authentication Considerations

When using LDAP_Authentication, the default searching behavior can be overridden by entering `<attribute>=%UserId%` in the Search Attribute edit box on the In the Directory Setup page. When you insert this syntax, the system constructs the DN of the user by concatenating the search attribute plus the entered user name with the search base.

For example, given the setup depicted in the following example, if the user entered *Sschumacher* in the User Name edit box of the signon page, the DN would be:

```
uid=Sschumacher,ou=Inkoop,o=ccb.com
```

This constructed DN would be used for the bind attempt rather than searching the directory with the search filter of:

```
uid=Sschumacher
```

SSO_Authentication Considerations

If you are using SSO_Authentication and LDAP_ProfileSynch to automatically generate profiles, then the value of the LDAP attribute mapped to User ID *must be* unique throughout the directory.

The PeopleSoft User ID uniquely identifies a person within PeopleSoft, and a DN uniquely identifies a person within the directory. PeopleSoft "maps" the PeopleSoft User Profile to a directory entry by specifying the directory attribute that holds the value of the PeopleSoft User ID.

You specify the appropriate mapping between the PeopleSoft system and your directory using the User Profile Caching component. On the Mandatory User Properties page, you must equate the PeopleSoft User ID attribute with an LDAP attribute. For instance, in many cases the PeopleSoft User ID is mapped to the LDAP attribute of uid.

With a single signon token, the system can provide the Signon PeopleCode with only a user ID value to identify a person. Then the system must search the directory to find the corresponding DN. If multiple entries within the scope of the search have the same value on the User ID attribute, then PeopleSoft is unable to determine which entry corresponds to the user.

Note. It is not required to use these functions to enable single-signon within PeopleSoft. The SSO_ Authentication combined with the LDAP_ProfileSynch applies only to situations where you want cache profile data from a directory if the user presents a single-signon token during signon.

LDAP_ProfileSynch Considerations

If you work with the NDS, Active Directory, or iPlanet directories and would like to assign roles dynamically at signon time, you can use the disabled example Signon PeopleCode that PeopleSoft has provided with this function. Directory-specific information is included in the comments of the code.

Note. This Signon PeopleCode provides a basic framework for dynamically assigning roles at signon time. If you want to dynamically assign roles at signon time, you must modify this code to work specifically with your NDS, Active Directory, or iPlanet directory schema. You should attempt this only if you are familiar with your directory schema and with writing PeopleCode.

Using Signon PeopleCode

This section provides overviews of signon PeopleCode and signon PeopleCode permissions, and discusses how to:

- Modify signon PeopleCode.
- Enable signon PeopleCode.
- Access X.509 certificates.

Understanding Signon PeopleCode

Signon PeopleCode runs 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 Lightweight Directory Access Protocol (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 can 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 the signon page.
- PeopleTools attempts to authenticate a user with the local PeopleSoft password.
- Signon PeopleCode runs.

It verifies the user and password, and then updates the local cache of user profiles stored in the PeopleSoft database.

Signon PeopleCode runs only when a user is logging through PIA, the portal, or a three-tier Windows workstation.

Note. If you are using LDAP authentication, the PeopleSoft authentication process will 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 run when PeopleSoft authentication fails.

Understanding Signon PeopleCode Permissions

Signon PeopleCode scripts run with full permissions of the user they're invoked as. This includes access to the database using Structured Query Language (SQL), access to the file system, business interlinks, component interfaces application messaging, and so on. A 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 trusted administrators only.

  This will prevent people from configuring un-trusted PeopleCode programs to run 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 selected for any Signon PeopleCode scripts.

- After a trusted administrator configures the list of functions that should run at signon time, you should use Object Security to restrict access to the record objects that contain 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.

Note. 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 a password entered by a user, and store it in a file or database table.

Page Used to Develop Signon PeopleCode

Page Name	Object Name	Navigation	Usage
Signon PeopleCode	SIGNONPPC_PAGE	PeopleTools, Security, Security Objects, Signon PeopleCode	Enable Signon PeopleCode programs.

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 can customize it as needed for testing or production use.

Open the record in PeopleSoft Application Designer, and view the PeopleCode with the PeopleCode Editor. The delivered PeopleCode accommodates 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 login 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 enabling 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.

Note. To see what the Signon PeopleCode program performs, use the PeopleCode debugger. This enables you to step through the program step-by-step.

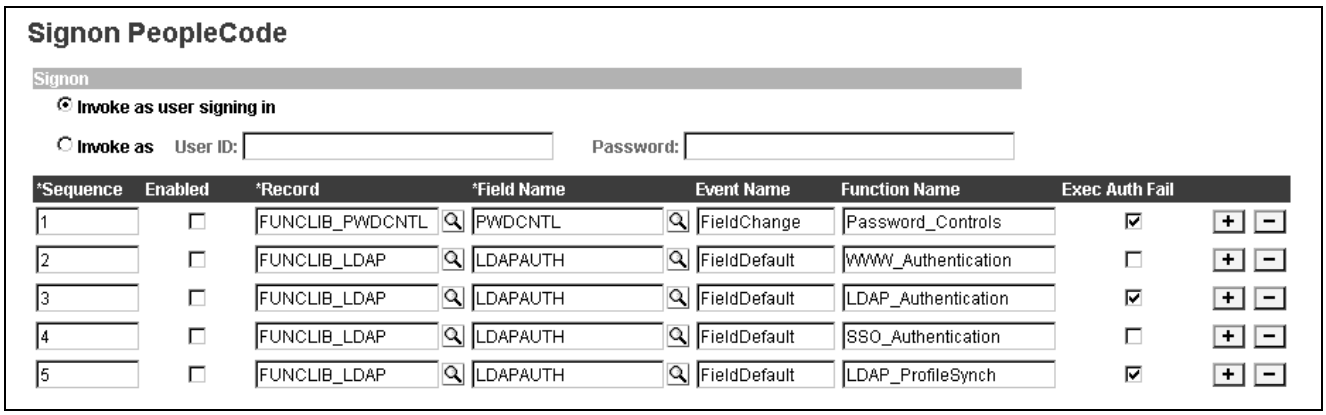
The following table presents the key PeopleCode constructs that you use with Signon PeopleCode. Click the function to view more details in the PeopleCode documentation:

PeopleCode Function	Description
See *Enterprise PeopleTools 8.45 PeopleBook: PeopleCode Language Reference*, "System Variables," %PSAuthResult.	Returns the result (boolean) of PeopleSoft authentication.
See *Enterprise PeopleTools 8.45 PeopleBook: PeopleCode Language Reference*, "PeopleCode Built-in Functions," SetAuthenticationResult.	Used to verify customers who log on to the system even if the PeopleSoft authentication fails.
See *Enterprise PeopleTools 8.45 PeopleBook: PeopleCode Language Reference*, "System Variables," %SignonUserId.	User ID value the user entered at the Signon page. This applies to PIA and Windows signon.
See *Enterprise PeopleTools 8.45 PeopleBook: PeopleCode Language Reference*, "System Variables," %SignOnUserPswd.	User password value the user entered at the Signon page. This value is encrypted. This applies to PIA and Windows signon.
See *Enterprise PeopleTools 8.45 PeopleBook: PeopleCode Language Reference*, "System Variables," %Request.	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 applies only to PIA.

Note. Do not use %SwitchUser in Signon PeopleCode.

Enabling Signon PeopleCode

Access the Signon PeopleCode page.



Signon PeopleCode page

Signon PeopleCode is different from other PeopleCode in that you specify which Signon PeopleCode you want to have on a specific Signon PeopleCode page. Notice that the PeopleSoft Password Controls program, which is written in PeopleCode, is also on this page.

By default, some of the Signon PeopleCode programs are disabled. You enable them on this page. You can also enable them 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.

Note. Using PeopleSoft password controls is valid only if you are *not* using LDAP authentication. When you're using LDAP authentication, the directory server, not PeopleSoft, controls the password.

You can add your own PeopleCode programs, but you must 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.

Invoke as user signing in/ Invoke as… When a PeopleCode program runs, it has to have a context of a user. This is how you indicate to the system which user is executing the program. This is important because the user ID provided must have access to all of the objects that your signon program uses. For example, if you are using LDAP, notice that the Signon PeopleCode 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 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 Displays the sequence in which the signon programs run. You can change the sequence by changing the numerical value in the edit box. The application server runs all programs in the ascending order in which they appear.

Enabled To enable a program to run at signon, select this check box. If it is not selected, then the system ignores the program at signon.

Record	Specify the record on which your record PeopleCode exists.
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 (execute authentication fails)	Select this check box to "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 clear 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.

Accessing X.509 Certificates

X.509 certificates are used to authenticate a user at the web server level—secure sockets layer (SSL) with client-side authentication. You can use PeopleCode to access X.509 certificates.

When you use certificate authentication with PeopleSoft, users do not see the PeopleSoft signon page and enter a user ID. Because of this, the X.509 certificate needs to be available in the Signon PeopleCode so you can write PeopleCode that maps the certificate to a PeopleSoft user ID.

The following sample PeopleCode shows how you access X.509 certificates in Signon PeopleCode:

```
Local string &clientDN;
&clientDN = %Request.GetParameter("com.peoplesoft.tools.ssl_client_dn");
```

The value of &clientDN might be similar to the following:

```
E=tom_sawyer@peoplesoft.com, C=US, S=California, L=Pleasanton,⇒
 O=PeopleSoft, OU=PeopleTools, CN=Tom Sawyer
```

Using the Web Server Security Exit

This section provides an overview of the web server security exit and discusses how to:

- Create a default user.
- Modify the web profile.
- Write a signon PeopleCode program.
- Sign in through the web server.

Understanding the Web Server Security Exit

Part of the integration technology PeopleSoft delivers is to ensure that our security or authentication system is open and flexible. Because the PeopleSoft applications are now designed for internet deployment, many sites must take advantage of the authentication services that exist at the web server level.

Note. The exits described here are offered in addition to the Signon PeopleCode running on the application server, which itself provides integration. There are no PeopleSoft user ("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 when developing new signon integration. The following topics support previous implementations.

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 with which you may want to integrate:

- Web single-signon or authorization or 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.

Note. The previous list is not a list of certified integration points, just examples of authentication technologies that exist in the industry.

For the web server exit configuration to work successfully, PeopleSoft assumes:

- You want to authenticate the user at the web server level only, 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.)
- Your web server environment 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 PeopleCode object.

  For this you can use an HTTP header variable, a cookie, or a form field.

Note. 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.

Creating a Default User

Create a default user ID using PeopleTools Security.

This user ID does not require any roles or permission lists. PeopleSoft recommends creating a long password that is difficult to guess.

For this example, we create the following user profile and password:

- User ID: default_user
- Password: ekdJl3838**&^^%kdjflsdkjfJHJIK

As you can see, the password is long and difficult to guess.

Modifying the Web Profile

With the default user created, you then modify the web profile to include the default user signon information.

To modify the web profile to include the default user signon information, you first must enable public access to the portal. In the Public Users section of the Web Profile Configuration - Security page, select Allow Public Access to indicate that the system should not prompt users to sign on when they click a direct link to a page. When this is selected, the PeopleSoft system does not display the password page to the user. Instead, the system authenticates users with the values specified in the User ID and Password fields in the same section of the page.

Note. In the following discussion, notice that the user is never actually signed on as "default_user." The user ID you specify 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 directory server.

Besides selecting the Allow Public Access check box, you also must set the user ID and password parameters to reflect the user ID created in the previous step. For example, set the User ID field value to *default_user*, and the Password field to *ekdJl3838**&^^%kdjflsdkjfJHJIK*.

Because you hardcode the signon values in the web profile, no end user ever needs to know them—their use is transparent.

PeopleSoft recommends limiting the access to and knowledge of the public access user ID and password 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 web profile.

Even if somebody does discover the public access user ID and password values, he or she won't be able to sign on to PeopleSoft. Recall that the default_user doesn't have any roles or permission lists. Alternatively, a sophisticated hacker could attack the application server directly by sending it a connection request formatted in the BEA 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.

Note. To prevent a user ID from being the default user on the signon page, set the Days to Autofill User ID property on the Web Profile Configuration - Security page to *0*.

See Also

Enterprise PeopleTools 8.45 PeopleBook: Internet Technology, "Configuring the Portal Environment," Configuring Web Profiles

Writing a Signon PeopleCode Program

In addition to creating a default user and enabling publc access, you also must write a Signon PeopleCode program that:

- 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 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 must write PeopleCode to retrieve the value and make a local copy.

Note. 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 SetAuthentication Result */

   &UserID = %Request.GetParameter("UserID");
   SetAuthenticationResult( True, &UserID, "", False);

End-Function;
```

After you have written the program, you must set the Signon PeopleCode program to run only if authentication is successful. On the Signon PeopleCode page, you set the running as follows:

- The Exec Auth Fail check box must *not* be selected.

  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 select the Exec Auth Fail check box when the PeopleCode authenticates the user itself, not when the program relies on the web server to perform authentication.

- You must 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.

Note. Before running the PeopleCode, the application server authenticates the User ID and Password field values in the Public Users section of the Web Profile Configuration - Security page.

Signing In Through the Web Server

This section provides a step-by-step example of what occurs within the system after you have it configured to trust authentication performed at the web server level:

Step	Component	Description
1	Browser	The user clicks a link to the PeopleSoft application, for example http://serverXYZ/servlets/psportal/peoplesoft8/?cmd=start.
2	Web server	The web server receives the request for the uniform resource locator, authenticates the user, and adds the user ID to the HTTP request for the resource. 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 third party web single signon or authorization solution, a PKI/ digital certificate, or SSL with client-side authentication.
3	Servlet	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 public user ID and password from the web profile.

Step	Component	Description
4	Application server	The application server authenticates the connection from the web server by checking the public access user ID and password against the values stored in PSOPRDEFN. The user ID and password must be valid for the connection to succeed and for Signon PeopleCode to run. **Note.** The password check prevents a sophisticated hacker from connecting to the application server directly and carrying out service requests.
5	Signon PeopleCode	Signon PeopleCode runs, 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. The PIA session is set to the user ID of whatever you pass into SetAuthenticationResult. For example: `SetAuthenticationResult(True,"TSAWYER","",False);` In this case, the system sets the session to TSAWYER. The user can access all the pages to which TSAWYER has access.

Using the Windows Security Exit

This section provides an overview of Windows security exits and discusses how to:

- Customize PSUSER.DLL.
- Implement a customized PSUSER.DLL.

Understanding Windows Security Exits

Almost all end users will access PeopleSoft using a browser, so you may not need to implement any client-side Windows exits. However, if you need to provide this functionality, perhaps for developers, PeopleSoft provides the option.

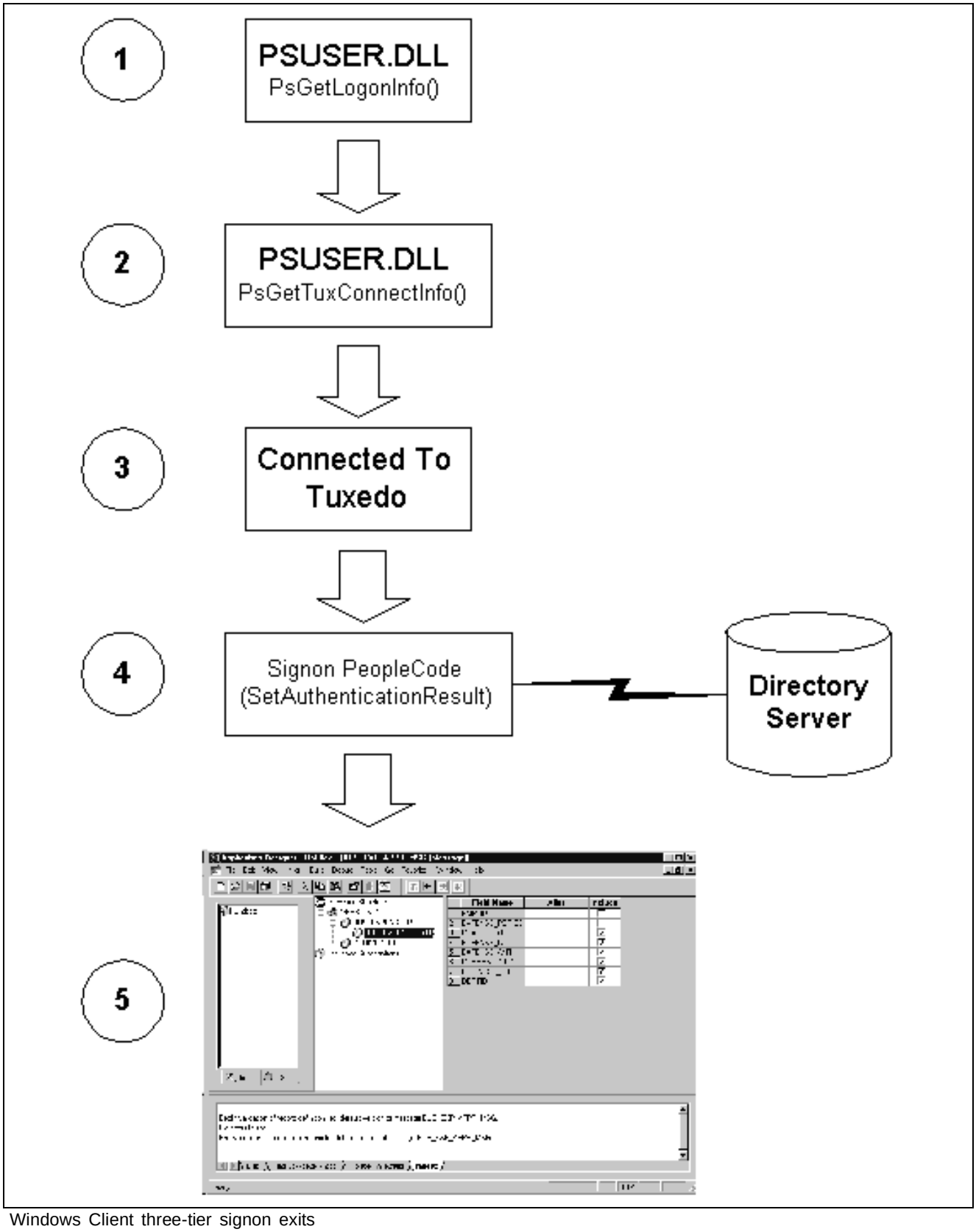
The Windows client-side exits are:

- PsGetTuxConnectInfo(): Used only for three-tier Windows workstations running PeopleSoft Application Designer or Query, for example.
- PsGetLogonInfo(): Used for Windows workstations in both a two-tier and three-tier environment.

Use these functions to create a customized PSUSER.DLL. These exits are used primarily for the PeopleTools Development Environment, PeopleSoft Query users, or PeopleSoft 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 bypass the PeopleSoft Signon window by modifying the PsGetLogonInfo() function as with the two-tier connection. But because you are connecting to the database through Tuxedo, there are some other authorizations that need to occur. This diagram shows those authorizations:



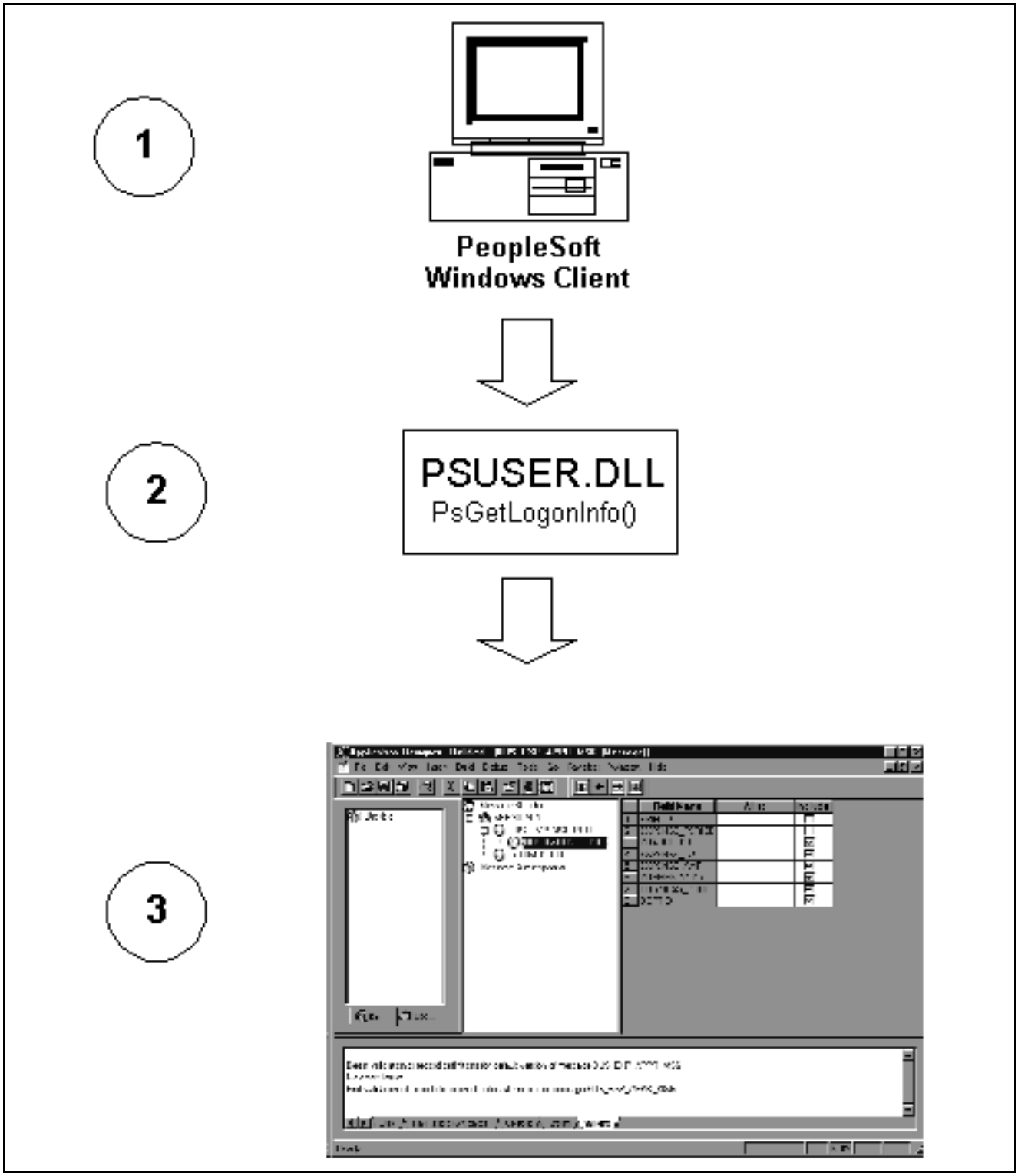
Windows Client three-tier signon exits

The required authorizations are as follows:

1. The PsGetLogonInfo() function must specify APPSERV as the szDBType parameter to bypass the PeopleSoft Signon window.
2. To connect to the Tuxedo application server, the PsGetTuxConnectInfo() function retrieves authentication information from directory server.
3. If the authentication information is valid, Tuxedo allows connection.
4. Tuxedo must connect to the database server.

   The application server verifies the authentication information passed by the PsGetTuxConnectInfo() function.
5. If the authentication is successful, the user is connected to PeopleTools.

The following diagram illustrates the results produced by customizing the PSUSER.DLL PsGetLogonInfo() function to bypass the PeopleSoft Signon dialog box:



Two-tier Windows Client signon using PsGetLogonInfo()

In this case, the sequence of events is as follows:

1. From the workstation the user runs PSTOOLS.EXE. PSTOOLS.EXE calls the PSUSER.DLL.
2. The PsGetLogonInfo() function supplies user signon information.

If information is validated by the RDBMS, the 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.

3. 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, also. This is done through the User Exit (PSUSER.DLL), which also enables you to specify your own encryption for use in encrypting passwords.

To enable these options, you must modify several procedures in the PSUSER.C, and recompile to create a new PSUSER.DLL. Then you must install the new DLL file wherever users run their PeopleSoft executables, such as PS_HOME on the file server.

In this section, we discuss 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 must be familiar with the C programming language.

PsGetLogonInfo()

The PsGetLogonInfo() function is always called when PeopleSoft is started. 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 box is bypassed and the information that you've coded into the function is 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(LPPSLOGINFO 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 must 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 must 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 proceeds directly to your default initial window specified in the PeopleSoft Configuration Manager Startup tab. Your procedure might look something like this:

```
PS_EXPORT(BOOL) PsGetLogonInfo(LPPSLOGINFO 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);
}
```

Note. If any required signon parameters are omitted, the signon screen appears and the missing values are set by 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:

Parameter Name	Description and Values
BSubsequentSignon	An initial or subsequent signon. Values are: FALSE: Initial signon. User just started PeopleSoft. TRUE: Subsequent signon. User probably selected an item from the Go menu in the Development Environment (PSIDE.EXE).

Parameter Name	Description and Values
szDBChange	Change database name or type. Values are: TYPE: Allow to change type and name. YES: Allow to change name only. NO: Do not allow to change either.
szDBType	Database type. Values are: 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	The Change Password feature. Values are: 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. Use this function to pass authentication data (key) to the server. Use this to either supplement or 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

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), and the Windows COBOL interfaces. For Windows NT, you must 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 must ensure that your new PSUSER.DLL is copied to that file server. If any of your workstations run the PeopleSoft executables locally, PSUSER.DLL must be distributed to such workstations.

CHAPTER 8

Setting up Digital Certificates and Single Signon

This chapter discusses how to:

- Work with digital certificates.
- Set up single signon.

Working With Digital Certificates

PeopleSoft takes advantage of HTTPS, Secure Sockets 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 business-to-business processing) over the internet.

PeopleSoft customers can implement PeopleSoft 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.

This section provides overviews of SSL and certificate authorities and discusses how to configure digital certificates.

Understanding SSL

With business-to-business applications, where systems communicate with each other over the internet, data must flow securely. As such, system-to-system authentication is critical. PeopleSoft uses 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 for our Integration Broker 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. With 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 use HTTPS / SSL and how it is implemented in for each technology.

Technology	How HTTPS/SSL is Implemented
PeopleSoft Portal Solutions	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 the client side of SSL connection to gateway. Uses web server platform to provide server side SSL.
PeopleSoft Integration Broker (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.
PeopleSoft 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 — Uses web server SSL client authentication. Certificate data is passed to application server. The application server trusts the web server's authentication. Distinguished name of the certificate is used to logon to PeopleSoft system.

Understanding Certificate Authorities

Anytime you implement SSL with mutual authentication (both client and server authenticate 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 (public and private key) 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 because the web server doesn't require "Client Side Authentication".

Important! When you are importing a digital certificate, you may receive an error message if you attempt to import the digital certificate immediately after downloading it from a certificate authority. This is due to issues related to "valid from" dates and times, and the inconsistencies in time settings between different computers. PeopleSoft recommends saving the certificate to a Windows 2000/NT workstation, right click on it using Windows Explorer, and select Open. This opens the Certificate dialog box. Examine the information regarding the "valid from" and "to" dates. Make sure those dates are valid on the application server the certificate will be installed on. The Details tab on the Certificate dialog presents the most thorough information.

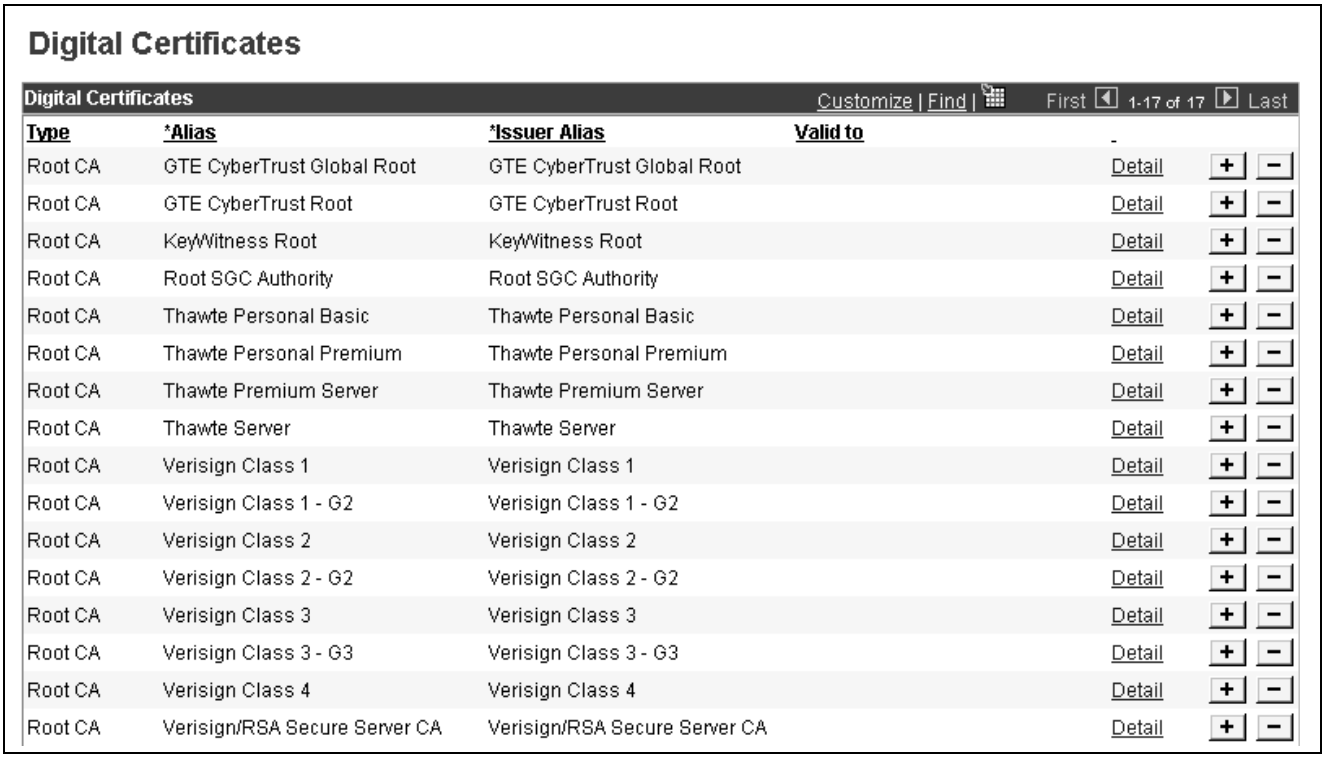
Configuring Digital Certificates

Select PeopleTools, Security, Security Objects, Digital Certificates.

The Digital Certificates page displays your inventory of server-side digital certificates. This page also enables you to import new certificates from a certificate authority.

Note. 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 | Customize | Find | First 1-17 of 17 Last

Type	*Alias	*Issuer Alias	Valid to	
Root CA	GTE CyberTrust Global Root	GTE CyberTrust Global Root		Detail
Root CA	GTE CyberTrust Root	GTE CyberTrust Root		Detail
Root CA	KeyWitness Root	KeyWitness Root		Detail
Root CA	Root SGC Authority	Root SGC Authority		Detail
Root CA	Thawte Personal Basic	Thawte Personal Basic		Detail
Root CA	Thawte Personal Premium	Thawte Personal Premium		Detail
Root CA	Thawte Premium Server	Thawte Premium Server		Detail
Root CA	Thawte Server	Thawte Server		Detail
Root CA	Verisign Class 1	Verisign Class 1		Detail
Root CA	Verisign Class 1 - G2	Verisign Class 1 - G2		Detail
Root CA	Verisign Class 2	Verisign Class 2		Detail
Root CA	Verisign Class 2 - G2	Verisign Class 2 - G2		Detail
Root CA	Verisign Class 3	Verisign Class 3		Detail
Root CA	Verisign Class 3 - G3	Verisign Class 3 - G3		Detail
Root CA	Verisign Class 4	Verisign Class 4		Detail
Root CA	Verisign/RSA Secure Server CA	Verisign/RSA Secure Server CA		Detail

Digital Certificates page

Type Select the type of certificate.

Local Node. Select this option when you are setting up a local node for the PeopleSoft messaging system (PeopleSoft Integration Broker).

Root CA. Select this when you are adding a new Root CA to your key store.

Remote. Select this option when you are setting up a remote node for the PeopleSoft messaging system (PeopleSoft Integration Broker).

Alias Enables you to add a custom alias for identification purposes.

Issuer Alias Contains the alias of the authority that issued the certificate.

Valid To Shows how long the certificate is valid for use.

Detail Launches a sub-page with more certificate information. The Certificate Detail page reveals subject and certificate information so you can determine such characteristics as the serial number, the fingerprint, the encryption algorithm, and so on.

Note. Depending on the type of certificate you're adding, this link might be displayed as Add Root, Import, or Request.

Note. When adding a Local Node certificate and you click the Import link, the Request New Certificate page appears in which you need to add Subject information (Organization, Locality, and so on) and Key Pair information (encryption algorithm, and key size).

Setting Up Single Signon

This section provides an overview of single signon and discusses:

- Working with the Single Signon page.
- Defining nodes for single signon.
- Sample single signon transaction.
- Single signon configuration considerations.
- Single signon configuration examples.
- Making the PeopleSoft single signon token secure.
- Using the single signon API.
- Configuring single signoff.

Understanding Single Signon

PeopleSoft supports single signon within PeopleSoft applications. 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 different applications and databases, the user navigates seamlessly through the system. Recall that each suite of PeopleSoft applications, such as HR or CRM, resides in its own database.

Note. The PeopleSoft single signon solution applies only to PeopleSoft applications.

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 authenticated initially. 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 complete 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 a live portal solution.

Note. 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.

Field	Description
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 the 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 PeopleTools Security, Single Signon page. The value is in Greenwich Mean Time (GMT) so it does not matter which time zone the application server is in.

Field	Description
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. Single signon is not related to Integration Broker messaging, except for the fact that single signon functionality leverages the messaging concept of 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.
Signature	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), `signature = SHA1_Hash ( UserID + Lang + Date Time issued + Issuing System + Local Node Pswd )` There is only one way to derive the 160 bits of data that make up the signature, and this is by hashing exactly the same User ID, Language, Date Time, Issuing System, and node password. **Note.** If you are using digital certificate authentication, the signature of the digital certificate occupies this space. The above description applies to using password authentication only.

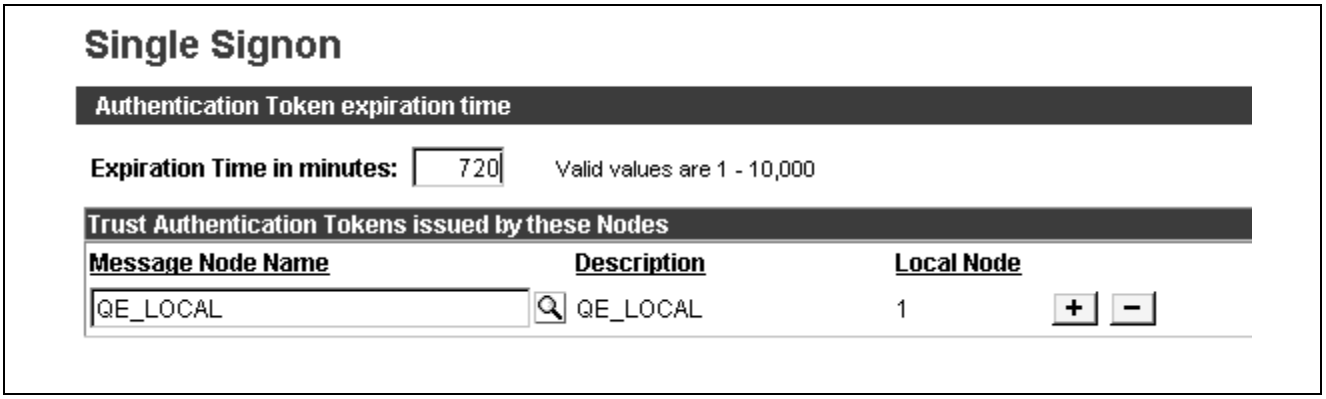
Note. Single signon does not depend on LDAP directory authentication. You can implement single signon and not LDAP, you can implement LDAP and not single signon, or you can implement both LDAP and single signon.

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, which is hardly enough time for a hacker to decrypt the information.

Working with the Single Signon Page

Select PeopleTools, Security, Security Objects, Single Signon to access the Single Signon page



Single Signon Page

Expiration time in minutes

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 HCM_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.

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

Message Node name

Shows the name of the Message Node. 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. When a node is trusted, the local node accepts tokens issued by it.

By default, no nodes appear in the "trusted" nodes list. 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 as 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. Then you add the names of other nodes in the system that should be trusted.

Note. You define nodes in Portal, Node Definitions.

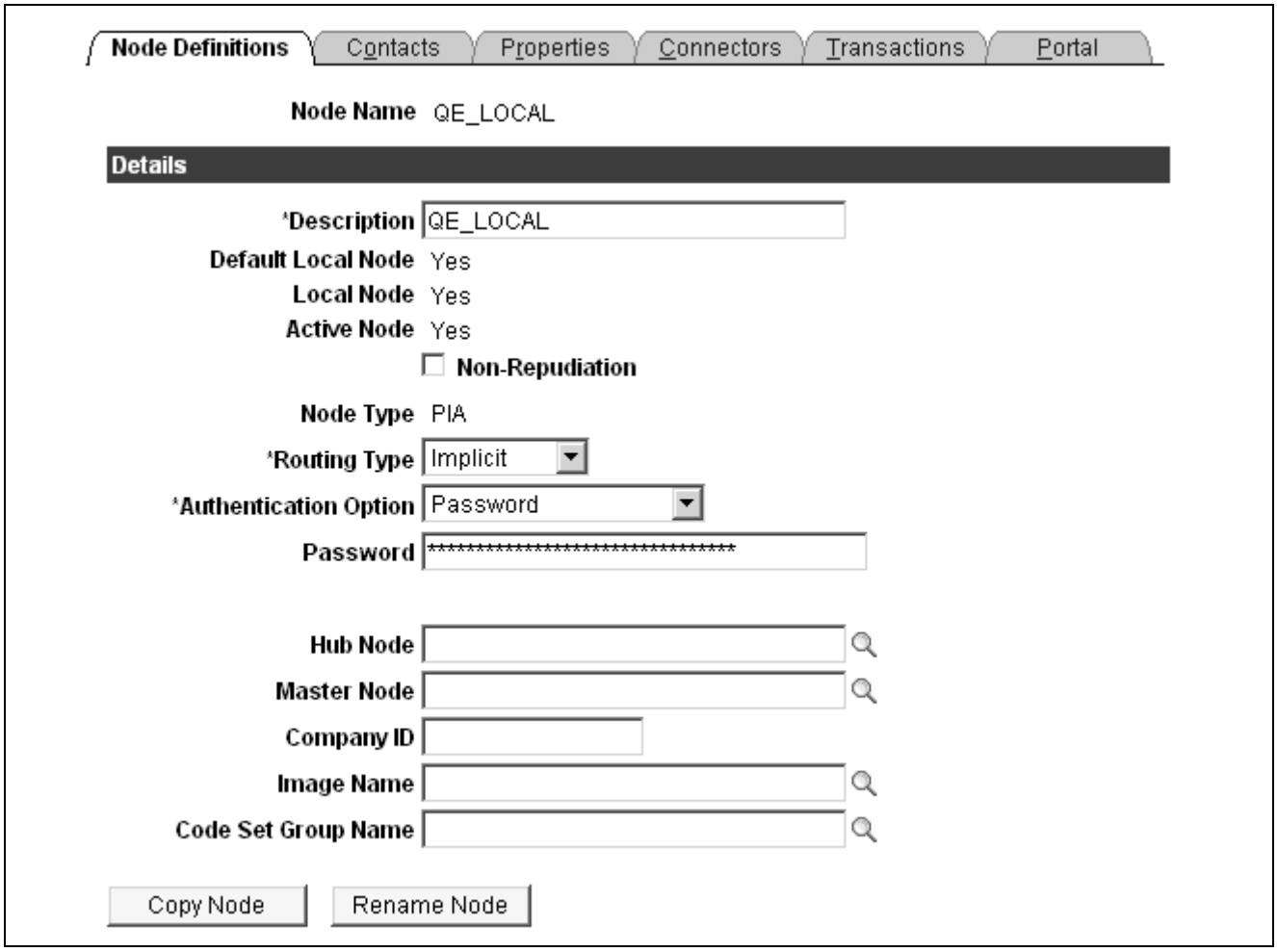
Local Node

Indicates whether the node is local or not.

Note. After you update the list of trusted nodes, the system automatically recognizes the new list. Rebooting the application server is not required.

Defining Nodes for Single Signon

Select PeopleTools, Portal, Node Definitions to access the Node Definitions page.



Defining nodes for single signon

The two options related to single signon are:

Authentication Option Determines how nodes in a single signon configuration authenticate other nodes in the same configuration. You have the following options:

None. Specifies no authentication between nodes.

Note. This option conflicts with PeopleSoft Integration Broker. If you select None, PeopleSoft Integration Broker messaging will fail, as will Single Signon.

Password. Indicates that each node in the single signon configuration authenticates other nodes by way of knowing the password for each node. For example, if there are three nodes (A, B, and C), the password for node A needs to be specified in its node definition on nodes A, B, and C.

Certificate. Indicates that a digital certificate authenticates each node in the single signon configuration. PeopleSoft recommends using certificate authentication for single signon. For certificate authentication, you need to have the following in the key store in the database for each node:

- Certificate for each node.
- Root certificate for the CA that issued the certificate.

Important! For single signon, the alias for the certificate of a node needs to be the *same* as the node name.

And, you *must* set up your digital certificates before you set the Authentication Option to certificate authentication.

Default Local Node The default local node is used specifically for setting up single signon. This indicates that the current node represents the database you're signed on to. The options you set for single signon should be made on the default local node.

See Also

Enterprise PeopleTools 8.45 PeopleBook: PeopleSoft Integration Broker, "Configuring Nodes and Transactions," Renaming or Deleting Node Definitions

Enterprise PeopleTools 8.45 PeopleBook: PeopleSoft Integration Broker, "Setting Up Secure Messaging Environments," Implementing Authentication and Nonrepudiation

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: an HCM 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 HCM database, completes a transaction, and then click a link that targets a page in the Financials database.

Step 1: User Signs on to HCM Application

The following occurs:

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

Step 2: Application Server Authenticates User

The following occurs:

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

Step 3: Application Server Generates Single Signon Token

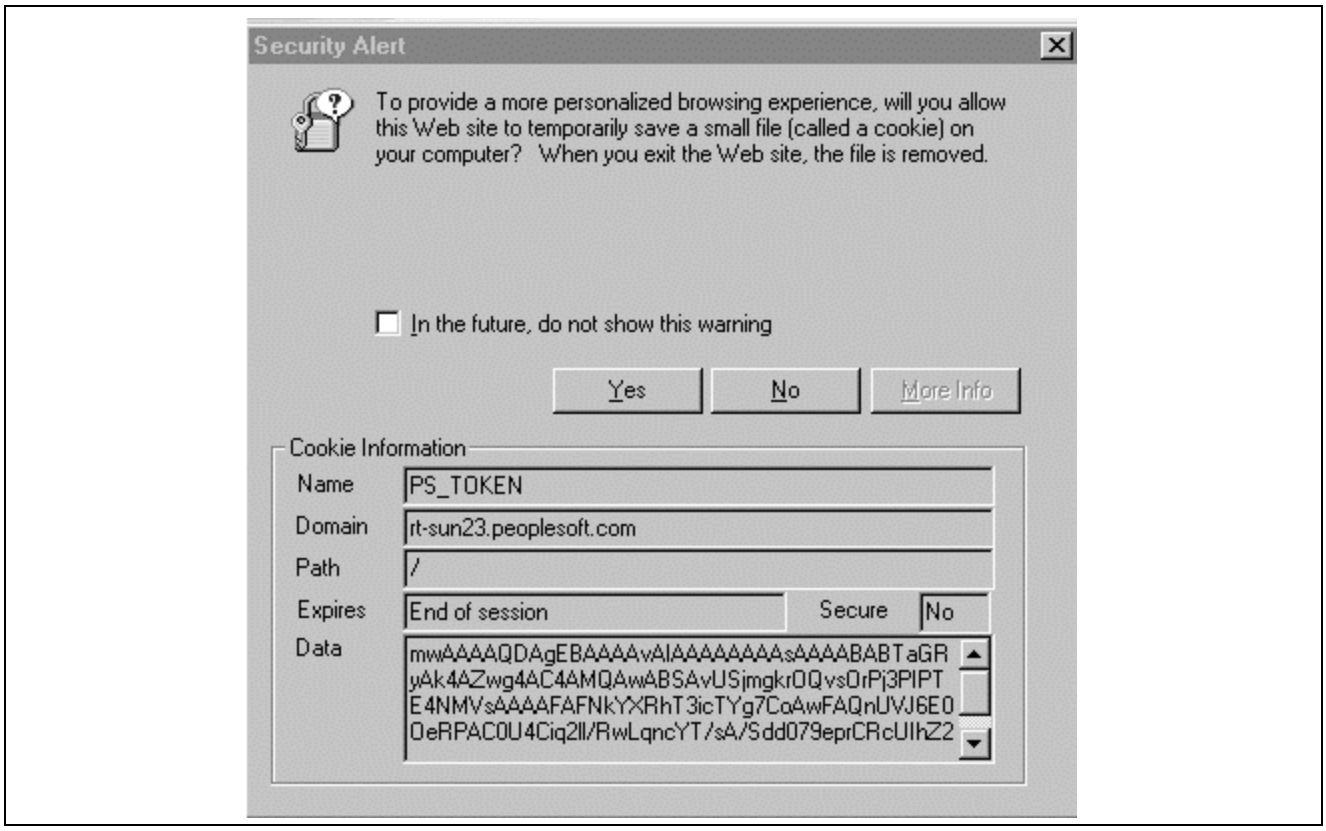
The following occurs:

- If the signon attempt to the HCM 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 encodes the token (base 64).
- 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 the 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 binary data across the HTTP protocol, the token data is encrypted and base 64 encoded.

Step 5: User Needs to Access Financial Application

After the user completes a few transactions in the HCM 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 HCM 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 HCM application), the Financials web server attempts to connect to the Financials application server. It passes only the Data field from the PS_TOKEN cookie; the application server needs only 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 PeopleTools, Security Objects, Single Signon. The Single Signon page enables the administrator of the Financials system to "trust" authentication tokens generated from HCM 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 Single Signon page.

Note. It is important to note that the expiration parameter specified in the Financials system is the relevant value, not the expiration value specified in HCM. 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 HCM 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.

Note. PeopleSoft recommends using digital certificate authentication when implementing single signon.

Single Signon Configuration Considerations

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

Single Authentication Domain Limitation

Web servers must be assigned to the same authentication domain — the server name in the URLs used to access them must contain the same domain name. A browser sends a cookie back only to the same domain from which it received the cookie.

On PeopleSoft systems, an authentication domain is not the same thing as an internet protocol (IP) address. It's a logical URL address that you specify during PIA setup, and its purpose is to associate different web servers (even at different physical locations) so that they appear to be at the same location to the PeopleSoft applications that use those web servers.

Important! Specifying authentication domains incorrectly for multiple PIA installations can produce single signon errors.

If you want to keep two PeopleSoft applications from erroneously attempting to employ single signon, make sure that the authentication domain you specify for one application's web server is not a subset of the authentication domain you specify for the other. For example, if your CRM web server has an authentication domain of *.user.mycompany.com*, your Financials web server authentication domain must not be *.mycompany.com* (the parent of the CRM server domain) or *.fin.user.mycompany.com* (a child of the CRM server domain). It can, however, be *.fin.mycompany.com* (or any child of that domain).

If you *do* want two PeopleSoft applications to employ single signon, you must ensure that each application contains a definition of the other as a trusted node, and you must specify the same authentication domain for both applications' web servers during PIA setup.

Furthermore, the web server that generates the cookie must have the domain that shares the PS_TOKEN cookie specified in the web profile of the local PIA web site. For example, in the context of our HCM to Financials example, the web profile for the HCM web server must contain the value of *.peoplesoft8.com* in the Authentication Domain property.

Note. 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. All PeopleSoft portal solutions products (Enterprise, Employee, Customer, Supplier portals) are built using frame-based templates.

Frame-based templates aren't proxied automatically. Proxying refers to when the system rewrites the URL to point to a location on the portal servlet, rather than the original location of the URL.

Single Signon Between Machines without DNS Entries

If you're setting up single signon between machines that don't have DNS entries, you need to modify the "hosts" file on the machine that's running the web browser. For example, let's say that you are using machine a.peoplesoft.com to signon to the web server a.peoplesoft.com, and then access b.peoplesoft.com using single signon. In this situation, you would need to update the "hosts" file on a.peoplesoft.com as follows.

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
```

```
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
216.131.221.88  a.peoplesoft.com
66.122.220.101  b.peoplesoft.com
```

See *Enterprise PeopleTools 8.45 PeopleBook: Internet 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:

http://hcm.peoplesoft.com/myapplication/signon.html

as opposed to the following:

http://hcm/myapplication/signon.html

When using the portal, the domain name that you specified in the Portal URI Text edit box on the Content Provider administration pages needs to match the fully qualified domain name you entered for the authentication domain. For example, you would need to specify serverX.peoplesoft.com/servlets, not serverX/servlets.

Cross Domain Single Signon

The current PeopleSoft single signon solution deals mainly with systems where there is only one DNS domain. Many sites need to deploy the PeopleSoft Portal in multi-domain environments. For instance, you might want to have the portal in one domain—www.PSFT_ecenter.com, for example—and the HCM database in another domain, such as www.yourcompany.com.

While there is no "out-of-the-box" solution for this implementation currently, you can configure your environment to support cross-domain single signon by completing the following configuration tasks.

- Setup a third-party web security product that supports multi-domain single signon and supports LDAP user profiles. There are several industry-standard products on the market.
- Configure the portal and content provider web servers to "trust" the web server for authentication. For PeopleSoft, this involves enabling the public access feature.
- Set up the PeopleSoft systems to download the user profiles from the same LDAP server that the web security product uses. This means that the DN that comes from the subject field of the certificate has to be a valid DN for the directory that the LDAP_profilesynch() function references. Because of this you need to build a user profile cache map that points to the same directory that generated the subject's DN.

Note. This cross-domain limitation does not apply to the portal if the content from the provider in a different domain is wrapped in an HTML template. However, this limitation does apply for any content in the portal that is wrapped in a frame template. Because the Enterprise, Customer, Supplier, and Employee portals shipped with PeopleTools all include frame templates as defaults, you'll need to perform the extra configuration steps to support cross-domain single signon in multi-domain environments. This limitation also applies to PIA-to-PIA (iClient-to-iClient) single signon.

Single Signon Configuration Examples

The following topics describe examples of single signon configurations and the steps required to implement them.

One Database and Two Web Servers

In this scenario there is one database and two or more web servers. While single signon is configured at the database level (that is, you specify time out minutes and trusted nodes for the entire database), it's actually used any time two different PeopleSoft servlets connect to the same database.

To set up single signon with one database and multiple web servers:

1. Select PeopleTools, Portal, Node Definitions and make sure that at least one node is defined as the Default Local Node.

   In the results on the search page, you can determine this by looking for a Y in the Default Local Node column.

2. Select PeopleTools, Security, Security Objects, Single Signon and set the following:

   - Make sure the Default Local Node appears in the list under Trust Authentication Tokens issued by these Nodes.
   - Set the timeout minutes to an appropriate value (the default is 720).

3. Access the web profile for each web server and modify the Authentication Domain property.

   Because single signon is implemented using browser cookies, it must be configured so that the user's browser sends the single signon cookie to each web server machine involved. By default, the browser only sends cookies back to the machine that set the cookie. So if web server a.peoplesoft.com sets a cookie after the user is authenticated, the browser (by default) only sends the cookie to a.peoplesoft.com. By default, the browser would not send the cookie to b.peoplesoft.com. To make the browser send the single signon cookie to all servers at in a domain (peoplesoft.com), access the Web Profile Configuration - General page and set a value of *.peoplesoft.com* for the Authentication Domain property.

   Note. You need the leading period (.) before the domain. It should appear as ".peoplesoft.com," not "peoplesoft.com."

   If you use only one web server, you *don't* need to modify the Authentication Domain property. A web server is designed to accept the cookies it distributes.

Two Databases and Two Web Servers

To set up single signon with multiple databases and multiple web servers:

1. Select PeopleTools, Portal, Node Definitions for *each* node that you want to involve in the single signon configuration and check the following:

   - Make sure that at least one node definition is defined as the Default Local Node for each database. In the results on the search page, you can determine this by looking for a Y in the Default Local Node column.

- Make sure that each database contains a node definition for the other nodes in the single signon configuration.
- Make sure that the Authentication Option is set correctly. For example, if you are using password authentication make sure that the node password for node 'X' is the same in each node definition for node 'X' in each database.

  PeopleSoft recommends using digital certificate authentication. Make sure the certificates are properly installed in the PeopleSoft Keystore before setting the node's Authentication Option to Certificate.

2. Select PeopleTools, Security, Security Objects, Single Signon and set the following:
   - Make sure the Default Local Node appears in the list under Trust Authentication Tokens issued by these Nodes.
   - Set the timeout minutes to an appropriate value (the default is 720).
3. Access the web profile on your web server and modify the Authentication Domain property.

   Because single signon is implemented using browser cookies, it must be configured so that the user's browser sends the single signon cookie to each web server machine involved. By default, the browser only sends cookies back to the machine that set the cookie. So if web server a.peoplesoft.com sets a cookie after the user is authenticated, the browser (by default) only sends the cookie to a.peoplesoft.com. By default, the browser would not send the cookie to b.peoplesoft.com. To make the browser send the single signon cookie to all servers at in a domain (peoplesoft.com), modify the authentication domain as follows.

See Chapter 8, "Setting up Digital Certificates and Single Signon," Working With Digital Certificates, page 139 and Chapter 6, "Employing LDAP Directory Services," page 93.

Single Signon with Third Party Authentication

This section presents a simple example of how to implement single signon when you have implemented a third party authentication system at the web server level. This applies to both portal and intranet web servers.

Note. This example does not cover authentication. This example assumes that you have set up your third party authentication correctly. Third party authentication is out of the scope for PeopleSoft support and documentation.

Note. Also, this discussion assumes that you have enabled public user access in the web profile for the appropriate site.

For PeopleSoft application single signon, the PeopleSoft system needs to know the user ID to be used for the web session. If implementing this configuration, you are required to address the following:

1. Authenticate the web user.
2. Determine which PeopleSoft User ID to use for this web user.
3. Send the User ID to the PeopleSoft application server.
4. Write signon PeopleCode to retrieve the User ID from wherever step 3 sent it.
5. Reauthenticate the User ID during signon PeopleCode.
6. Indicate to the PeopleSoft application server to use the User ID for all subsequent service requests.

The following examples address items 3, 4, and 6.

The following HTML applies to step 3 above. You can change the JavaScript function to set the cookie name and value that you want. Also, change the location to point to the PeopleSoft page to which you want to redirect users. For example,

```
<html>
<head>
<title>PeopleSoft 8 Single Sign-On Example</title>
</head>

<!--
PeopleSoft 8 Single Sign-On Example

In this example, security is non-existent.  In a production
system, the UserId could come from your site's single signon
tool.  Other information could also be included.  For this
example, only the UserId is saved into cookie.  This cookie then
gets sent to the PIA Web Servlet which passes it on to the
PeopleSoft Application Server.  A piece of signon PeopleCode is
needed to extract the UserId from the cookie and call
SetAuthorizationResult in order to "sign on" the user.

o  Change the domain value of the cookie to your domain.
o  Change the location ref to the target URL within your PeopleSoft site.
//-->

<body>
<script language=JavaScript>
var cookie = "ThirdPartyUserId=PS; Domain=.peoplesoft.com; path=/; MaxAge=1";
document.cookie = cookie;
location="https://hcm.peoplesoft.com/servlets/iclientservlet/hrdb/?ICType=Panel⇒
&Menu=ROLE_EMPLOYEE&Market=GBL&PanelGroupName=IT_TIME_OFF&RL=&target=main1"
</script>
</body>

</html>
```

The following Signon PeopleCode example applies to steps 4 and 6 above. The Signon PeopleCode needs to retrieve &UserID from where the third party portal put it in the HTTP Request. For example,

```
Function SSO_EXAMPLE()

/*This is step 4*/
   &TPUserId = %Request.GetCookieValue("ThirdPartyUserId");
   /*This is step 6*/
   If &TPUserId <> "" Then
      SetAuthenticationResult( True, &TPUserId, "", False);
   End-If
End-Function;
```

After you write the program, you need to enable the program using the Signon PeopleCode page. (PeopleTools, Security, Security Objects, Signon PeopleCode.

Making the PeopleSoft Single Signon Token Secure

PeopleSoft single signon functionality also applies at the web server level. For example, let's say that you have two web servers: server X and server Y. Assume that web server X is a Secured Sockets Layer (SSL) site, and assume that web server Y is not. In these situations, many sites want server Y to "trust" the authentication token, PS_TOKEN, issued by server X. This requires that the PS_TOKEN be set to be "secure."

If the PS_TOKEN is not marked as "secure," then when a user signs on through server Y, the browser sends PS_TOKEN to server Y over the unencrypted, non-SSL link. This is typical behavior for browsers when dealing with "non-secure" cookies. Potentially, in this situation a hacker could "sniff" this token from the clear network and use it to signon to the SSL-secure server X.

Another important use of this feature relates specifically to the PeopleSoft Portal. When the portal proxies content with an HTML template, it should forward PS_TOKEN cookies that are marked "secure" only over SSL connections.

To resolve this potential security issue, select the Secure Cookie with SSL check box on the Web Profile Configuration - Security page. You use this property to control the "secure" attribute of the single signon cookie. If you enable the property, and the scheme of the current request is HTTPS (an SSL server), the system sets the "secure" attribute of the single signon cookie (PS_TOKEN) to "true". This prevents the single signon token from travelling over an insecure network.

Note. If you enable this property, you are effectively disabling single signon to any non-SSL servers.

If, at your site, you want users to signon to an HTTPS server, and then want to do single signon with HTTP servers, set this property to false, which allows single signon between HTTPS and HTTP servers.

Note. If you can tolerate the security risk, and want single signon between secure and non-secure links, you can set this flag to "false". However, before doing this you need to make sure you are aware of all the security implications, such as the security of the HTTPS server may be compromised.

Using the Single Signon API

PeopleSoft delivers a component interface named PRTL_SS_CI that enables external applications to seamlessly integrate a single signon solution with the PeopleSoft portal applications. This makes sure that users who have already signed on to the portal don't have to sign on again for every system you reference in your portal.

To take advantage of the Single Signon API, you need to create a custom API, which includes building the dynamic link libraries, classes, and registry settings necessary to enable an external application to communicate with PeopleSoft. Only external applications, such as COM or C/C++ programs, require a component interface API. PeopleCode programs do not require a component interface API, and in fact, we do not recommend building a component interface API if the component interface is to be accessed from PeopleCode only.

The files of your custom API need to reside on the client machine; that is, the web server for ASP, and the machine running the Java program for Java. The registry file may also need to be executed to update the registry with the new libraries.

Understanding the Signon Process with the API

The PRTL_SS_CI Component Interface contains two user-defined methods:

- Authenticate( ). Your external authentication program distributes an authentication token that can be retrieved from a cookie in the browser. The Authenticate function determines if an authentication token is valid.
- GetUserID( ). If the token is valid, you use the GetUserID function to retrieve the User ID associated with the authentication token.

Before we describe the development requirements of your API, PeopleSoft recommends that you take a moment to examine the steps that occur internally when you use the API in conjunction with the delivered PRTL_SS_CI.

Step	Description
1	The user enters the User ID and password into the PeopleSoft Portal signon page.
2	If the login on portal application server is successful, the server generates a single signon token. The web server receives the single signon token from the application server, and issues a cookie to the browser.
3	The user navigates in the portal and encounters a hyperlink to the external system. The user clicks on the link.
4	The browser passes the PS_TOKEN cookie to your external web server.
5	The external web server checks for the PS_TOKEN cookie before displaying a signon page.
6	Once it is determined that the user is accessing your application through the PeopleSoft portal, you retrieve the authentication token and send it to the PRTL_SS_CI component interface to verify authentication. For instance, Call PRTL_SS_CI.Authenticate(Auth. token string)
7	After the system authenticates the token, the system can then make calls to the PRTL_SS_CI.Get_UserID() function to return the appropriate User ID.

Developing your External Application to Support Single Signon

Developers of the external applications need to alter the signon process to conform to the following requirements.

1. Check for the PS_TOKEN cookie. If the cookie doesn't exist, continue with your normal signon process. Otherwise, bypass the signon screen.
2. Retrieve the authentication token from the PS_TOKEN cookie.
3. Make a connection to PeopleSoft through the PRTL_SS_CI API.
4. Pass the authentication token to the Authenticate() function of the API.
5. If Authenticate() returns True, you then retrieve the User ID associated with the authentication token by using the Get_UserID() function.

For example, the following PeopleCode walks through the process of validating your authentication token and retrieving the user's User ID. The following sample is designed to provide a general idea of the process involved and help you to incorporate the PRTL_SS_CI API into your signon process.

```
Local ApiObject &THISSESSION;
Local ApiObject &THISCI;
Local string &AUTHTKN;
```

```
/* Assigns the Authentication Token to a variable */
&AUTHTKN = %AuthenticationToken;

/* Open a session and make a connection */
&THISSESSION = GetSession();
If &THISSESSION.connect(1, "EXISTING", "", "", 0) <> True Then
   WinMessage(MsgGet(30000, 1, "Session Connect Failed."));
   Exit (1);
End-If;

/* Retrieves the component interface PRTL_SS_CI */
&THISCI = &THISSESSION.GetCompIntfc(CompIntfc.PRTL_SS_CI);

/* Checks to see if the component interface is NULL */
If &THISCI = Null Then
   WinMessage("Component Interface PRTL_SS_CI not found. Please ensure Component⇒
 Interface
Security access is granted to this user.");
   Exit (1);
End-If;

/* Key fields would usually be set before the Get() function is called⇒
 in order to map the component interface to a particular set of data.⇒
 This component interface is not mapped to data. Therefore, the component interface⇒
 is retrieved and then the user defined methods are retrieved */
&THISCI.get();

PRTL_AUTH = &THISCI.Authenticate(&AUTHTKN);
PRTL_USER_ID = &THISCI.Get_UserID();
```

Note. The component interface is not mapped to data because the key field for the data would be the authentication token. This token is dynamically assigned when the user signs on to the portal, and it is not stored anywhere in the system as data. Therefore, there are no key fields and the token is passed directly to the user defined functions.

Configuring Single Signoff

In addition to single signon, PeopleSoft also signs the user off of content providers when the user signs off. However, there are some exceptions to the sign-off functionality.

The portal only signs off content providers that meet the following criteria:

- Content providers are accessed only through HTML templates.
- Content providers are all PeopleSoft 8.x applications.

This means that for content providers accessed through frame templates, single sign-out is not automatically enabled when you configure single signon. This section describes the steps you need to complete to configure single sign-off for content providers being accessed through frame templates, which includes all of the PeopleSoft Portal solutions (Employee, Customer, and so on).

The following procedure covers inserting an HTML image tag ("img") containing a logout command into a set of files on the web server. When the user signs off, the browser attempts to download the images using an "HTTP get," which causes the system to send the logout command to each specified content provider.

This procedure is not appropriate for content that is *never* accessed using a frame, as in it is accessed from the content source using an iScript and a business interlink, such as Lotus Notes integration.

To configure single sign-off for frame content:

1. On your web server, locate and open signin.html.
2. Open signin.html, select Save As, and enter the name *signout.html*.
3. Open signout.html, expire.html, and exception.html.
4. Add the following image tags to these files.

   You need to add one image tag to each of these files for each content provider that requires single signoff.

   Add the tags just before the closing body tag, as shown in the following example.

   ```
   <! add tags here>
   </body>
   ```

   If you have three content providers that require single signoff, such as HCM, FIN and HTML Access, you need to add three image tags to each file.

   For example:

   ```
   <IMG src="http://hcm.peoplesoft.com/servlets/psp/ps/hrdb/?cmd=logout"
   height=0 width=0 border=0>
   <IMG src="http://fin.peoplesoft.com/servlets/psp/ps/hrdb/?cmd=logout"
   height=0 width=0 border=0>
   <IMG src="http://htmlaccess.peoplesoft.com/html_access/system/init_asp/⇒
   logout.asp?cmd=dummy"
   height=0 width=0 border=0>
   ```

   The previous code merely shows a sample. To determine the exact URL you need to add for your implementation, right-click on the "logout" link of each content provider. You can usually view the logout link when accessing the application outside of the portal. Examine the "properties" of this link, and add the specified URL to the image tag.

   Note. The "cmd=dummy" is required in the image tag for HTML Access to make sure that the browser doesn't attempt to cache the image, which would prevent it from issuing the logout command.

5. In PIA, select PeopleTools, Web Profile, Web Profile Configuration, Look and Feel on your web server.

   In the Signon/Logout Pages group box, change the value of the Logout Page field to *signout.html*.

CHAPTER 9

Securing Data with Pluggable Cryptography

This chapter provides overviews of data security, pluggable cryptography, and the supported algorithms, and discusses how to:

- Load encryption libraries.
- Define algorithm chains.
- Define algorithm keysets.
- Define encryption profiles.
- Test encryption profiles.
- Invoke encryption profiles from PeopleCode.

Understanding Data Security

To understand pluggable cryptography, it's first necessary to understand the types of data security that cryptography in general can provide.

Data security comprises the following elements:

- Privacy — keeping data hidden from unauthorized parties.
- Integrity — keeping transmitted data intact.
- Authentication — verifying the identity of an entity that's transferring data.

Privacy is normally implemented with some type of encryption. Integrity can be accomplished with simple checksums or, better, with more complex cryptographic checksums known as one-way hashes. Many times, this is combined with a type of asymmetric cryptography to produce digital signatures. These signatures when verified assure you that the data has not changed. Authentication can also be accomplished via digital signatures, which makes them an obvious choice for data security.

Privacy Through Encryption

Encryption is the scrambling of information such that no one can read it unless they have a piece of data known as a key. Using the key, the sender encrypts *plaintext* to produce *ciphertext.* The recipient also uses a key to decrypt the ciphertext producing the original plaintext. The type of key at either end of this transaction, and the way it's applied, constitute an encryption algorithm. In all cases, the security of an encryption algorithm should NOT rely on its secrecy. Rather, it should rely on how well the operations involved affect the input data.

Data encryption algorithms come in two major forms: Symmetric cryptography and asymmetric cryptography. Symmetric cryptography falls into two categories: Block ciphers and stream ciphers. The bulk of cryptographic research has gone into block ciphers, which are employed by PeopleSoft pluggable cryptography.

Symmetric Encryption

Symmetric encryption involves both encrypting and decrypting a piece of data using the same key. To make it a bit harder to crack symmetric encryption schemes, they can be applied in a number of encryption *modes.* These modes provide ways of applying encryption sequentially to blocks of data, such that each block is encrypted by a combination of the encryption key and the previously encrypted block. Of course, when encrypting the first block, a previously encrypted block isn't available, so the encryption software applies a random *initialization vector* (IV) to get the process.started. This IV does not have to be secret.

The most popular symmetric encryption modes currently in use are:

- Electronic Code Book (ECB).

  ECB does not apply any special recombinations while encrypting. Plaintext blocks are simply encrypted with the key to produce blocks of ciphertext.

- Cipher Block Chaining (CBC).

  CBC takes a the previous block of ciphertext and XORs it with the current plaintext block before encrypting the plaintext.

- Cipher Feed Back (CFB).

  CFB produces ciphertext by XORing the plaintext with the result of a symmetric encryption operation on the previous ciphertext.

- Output Feed Back (OFB).

  OFB produces ciphertext by XORing plaintext blocks with a series of blocks resulting from repeated encryptions of the initialization vector.

There's a drawback with symmetric cryptography: The recipient of symmetrically encrypted ciphertext must posess the same key to decrypt it that you used to encrypt it. Because of this, you'll need a secure method of transmitting the key. This can be done a number of ways. You can send the key electronically over a private line that cannot be tapped; you can personally hand the key to your recipient; or you can use a courier to deliver the key. None of these approaches is foolproof or very efficient. A partial solution to this problem is asymmetric encryption.

Asymmetric Encryption

Asymmetric encryption involves the use of a pair of complementary keys, in which one key is used to encrypt a piece of data and the other key is used to decrypt it. This system uses *public key encryption* technology. The encryption key is called the public key and is widely distributed. The decryption key is the private key, which its owner must never reveal or transmit. Asymmetrically encrypted ciphertext is readable only by the owner of the private key. Anyone who wants to send ciphertext to that party needs only to have a copy of the recipient's freely available public key to perform the encryption.

Although asymmetric encryption is by design an excellent way for strangers to exchange data, it requires more computing power and capacity than symmetric encryption. Because of this, symmetric and asymmetric encryption are typically used in combination, to take advantage of the strengths of each system.

You apply the more efficient symmetric encryption to your data using a randomly generated symmetric key, which leaves only the problem of transmitting your symmetric key (also known as the *content encryption key*) to the recipient, who can use it to decrypt the ciphertext. You use the recipient's public key as a *key encryption key,* to apply asymmetric encryption to your symmetric key, not to your already encrypted ciphertext. The ciphertext and your symmetric key can now both be transmitted to the recipient. The recipient's private key is used to decrypt your symmetric key, which in turn is used to efficiently decrypt the ciphertext.

Integrity Through Hashing

Integrity can be provided with a *cryptographic hash.* There are several well-known hash types, including MD2, MD4, MD5, SHA1, and RIPEMD160. These hash types have the following properties in common:

- They're one-way.

  You cannot reverse the operation and get back the text that produced the hash. Indeed, this is obvious since most hashes have values that are 128-256 bits long. The size of a typical message will far exceed this, so it's extremely unlikely that the hash could contain all of the original information.

- They're collision resistant.

  There's almost no possiblility of finding two meaningful messages that produce the same hash. Each hash algorithm has a different degree of collision resistance.

To use hashing, you generate a hash value from your data and include it when you transmit the data. The recipient uses the same hash algorithm to generate a hash value from the received data. If the result matches the transmitted hash, the data wasn't altered in transit.

Authentication Using Digital Signatures

Authentication can be accomplished in a number of ways. These include:

- Fixed passwords.
- Time-variant passwords.
- Digital signatures.

Digital signatures are by far the most popular and most reliable method of authentication. Digital signatures usually combine a hash with another cryptographic operation (typically asymmetric encryption) to produce a type of check that not only verifies that the data was not altered in transit, but also assures that the named sender is, in fact, the actual sender of the data.

For example, if we provide a digital signature based on SHA1 with RSA encryption, this means that an SHA1 hash of the message was encrypted with the private key of the sender. Because the SHA1 hash is very collision resistant, and assuming the private key of the sender is known only by the sender, then verifying such a signature indicates that the message was not altered and that it was sent by the named sender.

Understanding Pluggable Cryptography

Pluggable cryptography provides a way for you to secure critical PeopleSoft data and communicate securely with other businesses. It enables you to extend and improve cryptographic support for your data in PeopleTools, giving you strong cryptography with the flexibility to change and grow, by incrementally acquiring stronger and more diverse algorithms for encrypting data. In PeopleTools, pluggable cryptography capability is provided by PeopleSoft pluggable encryption technology (PET).

Pluggable Cryptography Features

You can encrypt any data used in your application by invoking PeopleCode to apply your preferred encryption algorithms. You can obtain these algorithms from various vendors' cryptographic libraries, using the capabilities you want from each library.

The features of pluggable cryptography include:

- Access to a robust set of algorithms (symmetric and asymmetric ciphers, password-based encryption, hashes, MACs, signatures, enveloping, encoding, and writing/processing secured messages).
- The ability to encrypt, decrypt, sign, and verify fields in a database.
- The ability to encrypt, decrypt, sign, and verify external files.
- A secure keystore for encryption keys of widely varying types.
- The ability to convert data from one encryption scheme to another.

Pluggable Cryptography Development

The functional elements of pluggable cryptography are:

- A DLL for each supported encryption library, which uses C glue code to convert each cryptographic library's API into a unified plug-in with an API accessible from PeopleCode.
- A universal keystore that handles all forms of encryption keys, protected with row-level security.
- A sequence, or chain, of algorithms that you define for a specific type of encryption task. These algorithms are applied in turn to transform data from its original form into a desired final form.
- An encryption profile, which you define as an instance of an algorithm chain, applicable to a specific encryption task.
- The PeopleCode crypt class for accessing the algorithm chains that you define.

To develop and use an encryption profile:

1. Obtain an encryption library.

   The current release of PeopleTools includes the *OpenSSL* encryption library.

2. Develop API glue code to access the encryption library's algorithms.

   PeopleTools includes glue code already developed to support the delivered OpenSSL encryption library, as well as glue code to support the *PGP* encryption library, which you can license from PGP Corporation to enable its functionality.

   The glue code combines with each library to create a plug-in accessible from PeopleCode. The plug-in can be an independent DLL file, or it can be incorporated into the encryption library file, which is the case with the delivered OpenSSL library.

   You can develop glue code to produce plug-in wrappers for other encryption libraries of your choice. The plug-ins make their APIs accessible to PeopleCode, and the new algorithms become as easily available as the delivered algorithms. You can find development information and examples of glue source code in *PS_HOME*\src\pspetssl and *PS_HOME*\src\pspetpgp.

   Important! Use of the PGP® encryption functionality accessible through the PeopleTools PGP plug-in requires a specific license grant from PGP Corporation. Please contact peopletools@pgp.com to inquire about purchasing the required license.

   ---

3. Load the encryption library's algorithms into the PET database, generate accompanying encryption keys, and insert them into the PET keystore.
4. Define a chain of algorithms by selecting from the algorithms in the database.

   Because all algorithms are accessed from PeopleCode, you can combine algorithms from different libraries regardless of their source.

5. Define an encryption profile, which is an instance of an algorithm chain applicable to a specific encryption task.

   With an encryption profile you can apply parameter values that differ from the default values.

6. Test the encryption profile using the Test Encryption Profile page.

7. Write PeopleCode to invoke the encryption profile.

   With the delivered glue code, you can take advantage of the capabilities of these libraries through a single PeopleCode object. The PeopleCode crypt class provides an interface into all algorithms loaded from the underlying encryption libraries.

Note. This documentation discusses how to use an encryption library for which glue code has already been developed and compiled, such as OpenSSL and PGP.

OpenSSL Library Considerations

The OpenSSL toolkit is delivered with its command line program installed and ready to use. The delivered OpenSSL encryption library supports a subset of the encryption algorithms that are included with the OpenSSL toolkit.

Note. As installed, the OpenSSL toolkit doesn't support the PKCS7 algorithms from the delivered OpenSSL encryption library. To use those algorithms, you must further configure the OpenSSL toolkit. Refer to the PeopleTools OpenSSL Setup Red Paper, located in *PS_HOME*\src\OpenSSL.

See Also

http://www.openssl.org/

PGP Library Considerations

If you license the PGP encryption library, you must ensure that its installed location is included in the paths used by both the application server and PeopleSoft Process Scheduler, as follows:

- Using the PSADMIN utility, add the full installed path of the PGP SDK to the *Add to PATH* parameter.

  See *Enterprise PeopleTools 8.45 PeopleBook: System and Server Administration*, "Setting Application Server Domain Parameters".

- In the BEA Tuxedo Settings section of the Process Scheduler configuration file, add the full installed path of the PGP SDK to the *Add to PATH* parameter.

  See *Enterprise PeopleTools 8.45 PeopleBook: PeopleSoft Process Scheduler*, "Using the PSADMIN Utility".

Note. PGP operations are supported only on platforms where the PGP SDK is supported: Windows, Solaris, and Red Hat Linux.

Understanding the Supported Algorithms

This section discusses the minimum set of encryption algorithms supported by PeopleTools. Support for these algorithms is provided through the OpenSSL and PGP plug-ins, and internally through the PeopleCode crypt class.

Note. You use the crypt class to open an encryption profile, which is comprised of the chain of algorithms that you want to invoke. The crypt class then invokes the algorithms and applies their parameters as specified by the profile.

Some algorithms have accompanying parameters, some with default values, which are stored along with the algorithms in the PET database. You supply appropriate parameter values in the encryption profile, and they're used when the algorithm is invoked.

Each algorithm returns data appropriate to its purpose, using properties provided by the crypt class. The Result property is used to make output data available from algorithms that produce or transform data by encoding, decoding, encryption, decryption, generating hash values, or generating signatures. The Verified property conveys the success or failure of algorithms that verify the input data.

See Also

Chapter 9, "Securing Data with Pluggable Cryptography," Defining Encryption Profiles, page 177

Enterprise PeopleTools 8.45 PeopleBook: PeopleCode API Reference, "Crypt Class"

Internal Algorithms

Support for the following algorithms is provided by the PeopleCode crypt class. They're automatically available for inclusion in your algorithm chains.

Algorithm	Description
PSUnicodeToAscii	Convert Unicode text to ASCII.
PSAsciiToUnicode	Convert ASCII text to Unicode
PSHexEncode	Convert octets (bytes) into ASCII hex nibbles.
PSHexDecode	Convert ASCII hex nibbles (with a leading 0x) into binary octets (bytes).

OpenSSL Algorithms

This section describes the algorithms supported by the OpenSSL plug-in, including encoding algorithms, hashing algorithms, symmetric encryption algorithms, digital signature algorithms, and the individual secure messaging algorithms. They're available when you load the OpenSSL encryption library into the PET database.

Encoding

Following are the supported OpenSSL encoding algorithms.

Algorithm	Description
base64_encode	Encode data in base64 format.
base64_decode	Decode data from base64 format.

Hashing

Following are the supported OpenSSL hashing algorithms.

Algorithm	Description
md2_generate	Generate an MD2 hash value from the input data.
md4_generate	Generate an MD4 hash value.
md5_generate	Generate an MD5 hash value.
sha1_generate	Generate an SHA1 hash value.
ripemd160_generate	Generate a RIPEMD160 hash value.
hmac_sha1_generate	Generate a hash message authentication code SHA1 hash value.

Symmetric Encryption

Following are the supported OpenSSL symmetric encryption algorithms, which implement triple Data Encryption Standard (DES) encryption with various key sizes and modes.

Algorithm Name	Description
3des_ks112_ecb_encrypt	Encrypt data using a key size of 112 bits, in electronic code book mode.
3des_ks112_ecb_decrypt	Decrypt data using a key size of 112 bits, in electronic code book mode.
3des_ks112_cbc_encrypt	Encrypt data using a key size of 112 bits, in cipher block chaining mode.
3des_ks112_cbc_decrypt	Decrypt data using a key size of 112 bits, in cipher block chaining mode.
3des_ks112_cfb_encrypt	Encrypt data using a key size of 112 bits, in cipher feed back mode.
3des_ks112_cfb_decrypt	Decrypt data using a key size of 112 bits, in cipher feed back mode.
3des_ks112_ofb_encrypt	Encrypt data using a key size of 112 bits, in output feed back mode.
3des_ks112_ofb_decrypt	Decrypt data using a key size of 112 bits, in output feed back mode.
3des_ks168_ecb_encrypt	Encrypt data using a key size of 168 bits, in electronic code book mode.
3des_ks168_ecb_decrypt	Decrypt data using a key size of 168 bits, in electronic code book mode.
3des_ks168_cbc_encrypt	Encrypt data using a key size of 168 bits, in cipher block chaining mode.
3des_ks168_cbc_decrypt	Decrypt data using a key size of 168 bits, in cipher block chaining mode.
3des_ks168_cfb_encrypt	Encrypt data using a key size of 168 bits, in cipher feed back mode.
3des_ks168_cfb_decrypt	Decrypt data using a key size of 168 bits, in cipher feed back mode.
3des_ks168_ofb_encrypt	Encrypt data using a key size of 168 bits, in output feed back mode.
3des_ks168_ofb_decrypt	Decrypt data using a key size of 168 bits, in output feed back mode.

Most of these algorithms use the same two parameters:

- *IV* (Initialization Vector)

  This parameter isn't used by the listed electronic code book (ECB) mode algorithms. Specify a hex encoded value to use to alter the first plaintext block of data before it's encrypted. This value serves as an encryption seed value, which must be applied for both encryption and decryption. The value must be the length of the cipher's blocksize — eight bytes for triple DES. It should be random but its secrecy isn't critical. For example: *0x0102030405060708*

- *SYMMETRIC_KEY*

  Specify as a string the keyset ID of the symmetric encryption key to be used with this algorithm. This parameter must identify a key that's stored in the PET keyset database.

Digital Signature Handling

Following are the supported OpenSSL algorithms for generating signatures.

Algorithm Name	Description
rsa_md5_sign	Generate an RSA signature using an MD5 hash.
rsa_sha1_sign	Generate an RSA signature using an SHA1 hash.
dsa_sha1_sign	Generate a DSA signature.

The signing algorithms all use the same parameters:

- *SIGNERPRIVATEKEY*

  Specify as a string the keyset ID that represents the signer's private key in the PET keyset database. The actual key value in the keyset database should begin "-----BEGIN *xxx* PRIVATE KEY-----" where *xxx* is either *RSA* or *DSA*, depending on the algorithm.

- *SIGNERPKPASSPHRASE*

  Specify the passphrase used to decrypt and unlock the signer's private key. This parameter's value is the actual passphrase.

Following are the supported OpenSSL algorithms for verifying signatures.

Algorithm Name	Description
rsa_md5_verify	Verify an RSA signature based on an MD5 hash.
rsa_sha1_verify	Verify an RSA signature based on an SHA1 hash.
dsa_sha1_verify	Verify a DSA-hashed signature.

The verifying algorithms all use the same parameters:

- *SIGNERPUBLICKEY*

  Specify as a string the keyset ID that represents the signer's public key in the PET keyset database. The actual key value in the keyset database should begin "-----BEGIN *xxx* PUBLIC KEY -----" where *xxx* is either *RSA* or *DSA*, depending on the algorithm.

- *SIGNATURE*

Specify as a string the hex encoded signature that's delivered with the input data or that's returned as the result of invoking a signing algorithm.

Secure Messaging — pkcs7_signed_sign

The pkcs7_signed_sign algorithm generates a signed PKCS7 message. The parameters are as follows:

- *SIGNERCERT*

  Specify as a string the keyset ID that represents the signer's certificate in the PET keyset database. The actual certificate stored in the keyset database is an X.509 certificate. Its value should begin "-----BEGIN CERTIFICATE-----".

- *SIGNERPRIVATEKEY*

  Specify as a string the keyset ID that represents the signer's private key in the PET keyset database. The actual key value in the keyset database should begin "-----BEGIN *xxx* PRIVATE KEY-----" where *xxx* is either *RSA* or *DSA*.

- *SIGNERPKPASSPHRASE*

  Specify the passphrase used to decrypt and unlock the signer's private key. This parameter's value is the actual passphrase.

Secure Messaging — pkcs7_signed_verify

The pkcs7_signed_verify algorithm verifies a signed PKCS7 message. The parameters are as follows:

- *RECIPIENT*

  Specify as a string the keyset ID that represents the recipient's certificate in the PET keyset database. The actual certificate stored in the keyset database is an X.509 certificate. Its value should begin "-----BEGIN CERTIFICATE-----".

- *SYMMETRIC_ALGORITHM*

  Specify the name of the symmetric algorithm used for content encryption. This must be a symmetric encryption algorithm supported by an encryption plug-in.

Secure Messaging — pkcs7_encrypted_encrypt

The pkcs7_encrypted_encrypt algorithm generates an encrypted PKCS7 message.

This algorithm has one parameter: *SIGNERCERT*, which is the keyset ID that represents the signer's X.509 certificate in the PET keyset database. The value stored in the keyset database should begin with the line "-----BEGIN CERTIFICATE-----".

Secure Messaging — pkcs7_encrypted_decrypt

The pkcs7_encrypted_decrypt algorithm decrypts an encrypted PKCS7 message. The parameters are as follows:

- *RECIPIENTCERT*

  Specify as a string the keyset ID that represents the recipient's certificate in the PET keyset database. The actual certificate in the keyset database should begin with the line "-----BEGIN CERTIFICATE-----"

- *RECIPIENTPRIVATEKEY*

  Specify as a string the keyset ID that represents the recipient's private key in the PET keyset database. The actual key value in the keyset database should begin "-----BEGIN *xxx* PRIVATE KEY-----" where *xxx* is either *RSA* or *DSA*.

- *RECIPIENTPKPASSPHRASE*

Specify the passphrase used to decrypt and unlock the recipient's private key. This parameter's value is the actual passphrase.

Secure Messaging — pkcs7_signandencrypt_signandencrypt

The pkcs7_signandencrypt_signandencrypt algorithm generates a signed and encrypted PKCS7 message. The parameters are as follows:

- *SIGNERCERT*

  Specify as a string the keyset ID that represents the signer's certificate in the PET keyset database. The actual certificate stored in the keyset database is an X.509 certificate. Its value should begin "-----BEGIN CERTIFICATE-----".

- *SIGNERPRIVATEKEY*

  Specify as a string the keyset ID that represents the signer's private key in the PET keyset database. The actual key value in the keyset database should begin "-----BEGIN *xxx* PRIVATE KEY-----" where *xxx* is either *RSA* or *DSA*.

- *SIGNERPKPASSPHRASE*

  Specify the passphrase used to decrypt and unlock the signer's private key. This parameter's value is the actual passphrase.

- *RECIPIENT*

  Specify as a string the keyset ID that represents the recipient's certificate in the PET keyset database. The actual certificate stored in the keyset database is an X.509 certificate. Its value should begin "-----BEGIN CERTIFICATE-----".

- *SYMMETRIC_ALGORITHM*

  Specify the name of the symmetric algorithm used for content encryption. This must be a symmetric encryption algorithm supported by an encryption plug-in.

Secure Messaging — pkcs7_signandencrypt_decryptandverify

The pkcs7_signandencrypt_decryptandverify algorithm decrypts and verifies an encrypted PKCS7 message. The parameters are as follows:

- *SIGNERCERT*

  Specify as a string the keyset ID that represents the signer's certificate in the PET keyset database. The actual certificate stored in the keyset database is an X.509 certificate. Its value should begin "-----BEGIN CERTIFICATE-----".

- *RECIPIENTCERT*

  Specify as a string the keyset ID that represents the recipient's certificate in the PET keyset database. The actual certificate in the keyset database should begin with the line "-----BEGIN CERTIFICATE-----".

- *RECIPIENTPRIVATEKEY*

  Specify as a string the keyset ID that represents the recipient's private key in the PET keyset database. The actual key value in the keyset database should begin "-----BEGIN *xxx* PRIVATE KEY-----" where *xxx* is either *RSA* or *DSA*.

- *RECIPIENTPKPASSPHRASE*

  Specify the passphrase used to decrypt and unlock the recipient's private key. This parameter's value is the actual passphrase.

PGP Algorithms

This section describes the secure messaging algorithms supported by the delivered PGP glue code. They're available when you license the PGP encryption library from PGP Corporation, compile the glue code, and load the library into the PET database.

pgp_signed_sign

The pgp_signed_sign algorithm generates a signed PGP message. The parameters are as follows:

- *SIGNERPRIVATEKEY*

  Specify as a string the keyset ID that represents the signer's private key in the PET keyset database. The actual key value in the keyset database should begin "-----BEGIN PGP PRIVATE KEY BLOCK-----".

- *SIGNERKID*

  Specify as a string the PGP key ID for the signer's key. It's a hex encoded 32 bit value, for example, *0xAB01D6A5*. You can obtain this value from the PGP-based tool that created the key.

- *SIGNERPKPASSPHRASE*

  Specify the passphrase used to decrypt the signer's private key. This parameter's value is the actual passphrase.

- *CLEARSIGN*

  Specify a numeric value indicating whether the message is to be *clearsigned.* A clearsigned message should remain readable. If you specify a value of *1*, the message remains as is and a radix 64 armored signature block is appended to the message. If you specify a value of *0*, the signature block is appended and the entire message is radix 64 armored.

pgp_signed_verify

The pgp_signed_verify algorithm verifies a signed PGP message.

This algorithm has one parameter: *SIGNERPUBLICKEY*, which is the keyset ID that represents the signer's PGP Public key in the PET keyset database. The value stored in the keyset database should begin with the line "-----BEGIN PGP PUBLIC KEY BLOCK-----".

pgp_encrypted_encrypt

The pgp_encrypted_encrypt algorithm generates an encrypted PGP message. The parameters are as follows:

- *RECIPIENTPUBLICKEY*

  Specify as a string the keyset ID that represents the recipient's public key in the PET keyset database. The actual key value in the keyset database should begin "-----BEGIN PGP PUBLIC KEY BLOCK-----".

- *RECIPIENTKID*

  Specify as a string the PGP key ID for the recipient's key. It's a hex encoded 32 bit value, for example, *0xAB01D6A5*. You can obtain this value from the PGP-based tool that created the key.

pgp_encrypted_decrypt

The pgp_encrypted_decrypt algorithm decrypts an encrypted PGP message. The parameters are as follows:

- *RECIPIENTPRIVATEKEY*

  Specify as a string the keyset ID that represents the recipient's private key in the PET keyset database. The actual value in the keyset database should begin "-----BEGIN PGP PRIVATE KEY BLOCK-----".

- *RECIPIENTPKPASSPHRASE*

Specify the passphrase used to decrypt the recipient's private key. This parameter's value is the actual passphrase.

- *RECIPIENTPUBLICKEY*

  Specify as a string the keyset ID that represents the recipient's public key in the PET keyset database. The actual value in the keyset database should begin "-----BEGIN PGP PUBLIC KEY BLOCK-----".

- *RECIPIENTKID*

  Specify as a string the PGP key ID for the recipient's key. It's a hex encoded 32 bit value, for example, *0xAB01D6A5*. You can obtain this value from the PGP-based tool that created the key.

pgp_signedandencrypted_signandencrypt

The pgp_signedandencrypted_signandencrypt algorithm generates a signed and encrypted PGP message. The parameters are as follows:

- *SIGNERPRIVATEKEY*

  Specify as a string the keyset ID that represents the signer's private key in the PET keyset database. The actual key value in the keyset database should begin "-----BEGIN PGP PRIVATE KEY BLOCK-----".

- *SIGNERKID*

  Specify as a string the PGP key ID for the signer's key. It's a hex encoded 32 bit value, for example, *0xAB01D6A5*. You can obtain this value from the PGP-based tool that created the key.

- *SIGNERPKPASSPHRASE*

  Specify the passphrase used to decrypt the signer's private key. This parameter's value is the actual passphrase.

- *RECIPIENTPUBLICKEY*

  Specify as a string the keyset ID that represents the recipient's public key in the PET keyset database. The actual value in the keyset database should begin "-----BEGIN PGP PUBLIC KEY BLOCK-----".

- *RECIPIENTKID*

  Specify as a string the PGP key ID for the recipient's key. It's a hex encoded 32 bit value, for example, *0xAB01D6A5*. You can obtain this value from the PGP-based tool that created the key.

- *CLEARSIGN*

  Specify a numeric value indicating whether the message is to be *clearsigned.* A clearsigned message should remain readable. If you specify a value of *1*, the message remains as is and a radix 64 armored signature block is appended to the message. If you specify a value of *0*, the signature block is appended and the entire message is radix 64 armored.

pgp_signedandencrypted_decryptandverify

The pgp_signedandencrypted_decryptandverify algorithm decrypts and verifies a signed and encrypted PGP message. The parameters are as follows:

- *RECIPIENTPRIVATEKEY*

  Specify as a string the keyset ID that represents the recipient's private key in the PET keyset database. The actual value in the keyset database should begin "-----BEGIN PGP PRIVATE KEY BLOCK-----".

- *RECIPIENTPKPASSPHRASE*

  Specify the passphrase used to decrypt the recipient's private key. This parameter's value is the actual passphrase.

- *RECIPIENTPUBLICKEY*

Specify as a string the keyset ID that represents the recipient's public key in the PET keyset database. The actual value in the keyset database should begin "-----BEGIN PGP PUBLIC KEY BLOCK-----".

- *RECIPIENTKID*

  Specify as a string the PGP key ID for the recipient's key. It's a hex encoded 32 bit value, for example, *0xAB01D6A5*. You can obtain this value from the PGP-based tool that created the key.

- *SIGNERPUBLICKEY*

  Specify as a string the keyset ID that represents the signer's public key in the PET keyset database. The actual key value in the keyset database should begin "-----BEGIN PGP PUBLIC KEY BLOCK-----".

- *SIGNERKID*

  Specify as a string the PGP key ID for the signer's key. It's a hex encoded 32 bit value, for example, *0xAB01D6A5*. You can obtain this value from the PGP-based tool that created the key.

See Also

Chapter 9, "Securing Data with Pluggable Cryptography," Loading Encryption Libraries, page 171

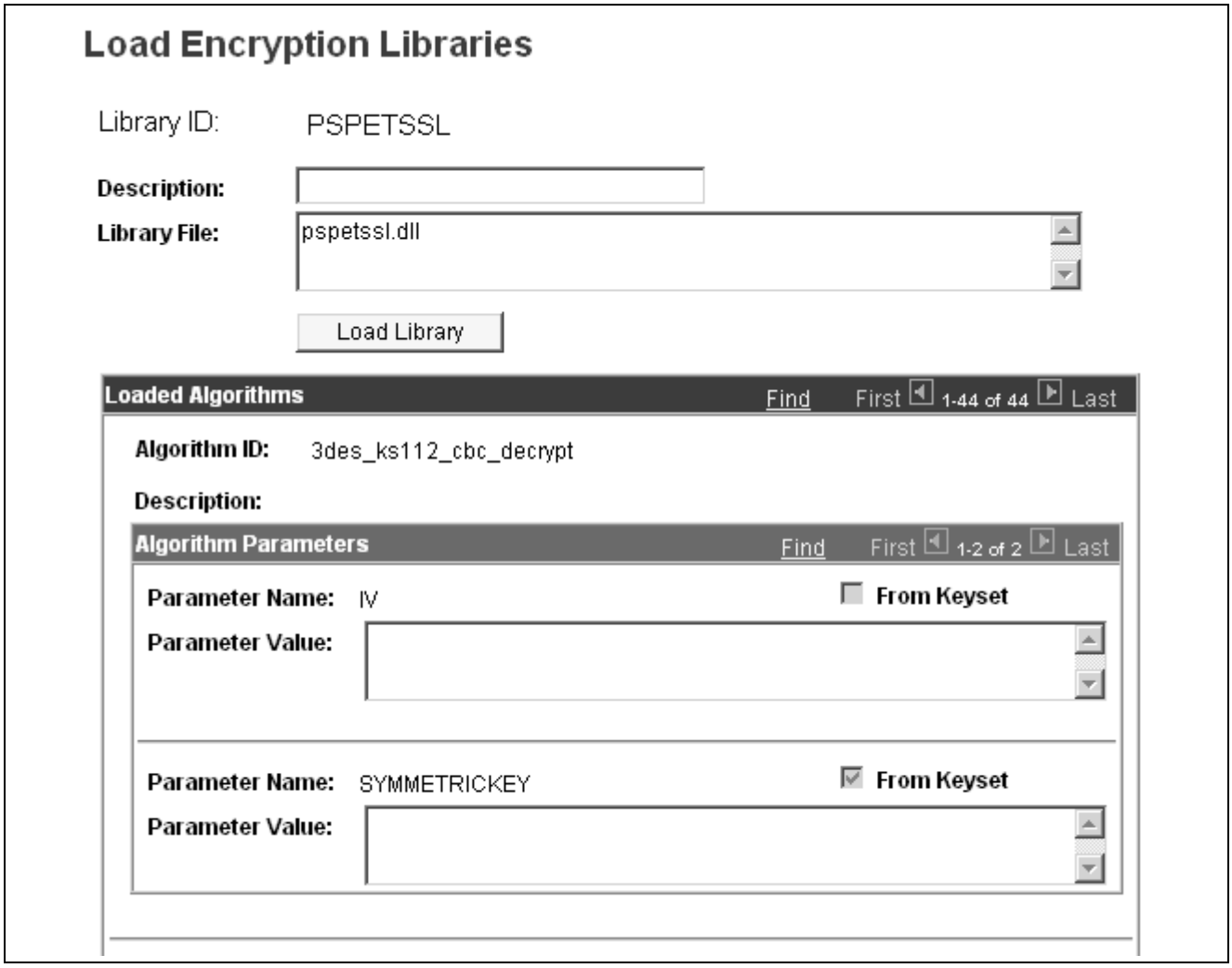
Algorithm Chain Considerations

Although you can select any sequence of algorithms to define a chain, many possible sequences don't work because the cumulative effect of the algorithms doesn't make any sense. You must define sequences of compatible algorithms.

To apply any of the supported algorithms for symmetric encryption, hashing, encoding, or secure messaging, the input data must be in ASCII text format. Because PeopleSoft stores data in Unicode format, the first algorithm in most chains must be PSUnicodeToAscii, and the last algorithm must be PSAsciiToUnicode.

Loading Encryption Libraries

Select PeopleTools, Security, Encryption, Load Encryption Libraries to access the Load Encryption Libraries page.



Load Encryption Libraries page

Library File

Enter the filename of the selected encryption library for your operating system platform. The names of the delivered OpenSSL and PGP library files depend on the operating system platform where your application is installed.

Following are the encryption library filenames for each supported platform:

- Microsoft Windows

  OpenSSL: *pspetssl.dll*

  PGP: *pspetpgp.dll*
- Red Hat Linux

  OpenSSL: *libpspetssl.so*

  PGP: *libpspetpgp.so*
- Sun Solaris

  OpenSSL: *libpspetssl.so*

  PGP: *libpspetpgp.so*
- HP Tru64 Unix

OpenSSL: *libpspetssl.so*

- HP-UX

  OpenSSL: *libpspetssl.sl*

- IBM AIX

  OpenSSL: *libpspetssl.a*

Note. Use of the PGP® encryption functionality accessible through the PeopleTools PGP plug-in requires a specific license grant from PGP Corporation. Please contact peopletools@pgp.com to inquire about purchasing the required license.

Load Library Click to load the specified encryption library.

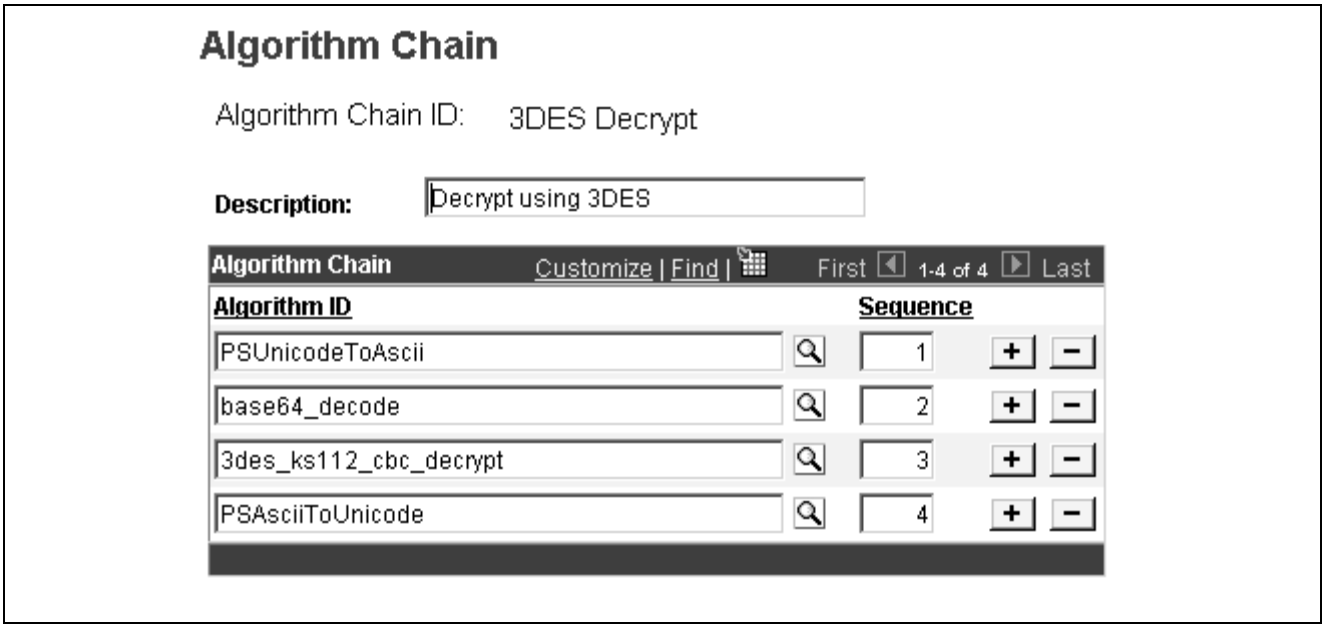
Each algorithm provided by the library appears in its own row with its algorithm ID. Its parameters each appear in a row, displaying the parameter's name and its default value.

If the From Keyset check box is selected, the parameter represents an encryption key. The pluggable cryptography facility uses the parameter's value to access the encryption key from the PET keystore.

Important! If the library you specified fails to load, you must sign out of your application, then shut down and restart the application server before signing back in.

Defining Algorithm Chains

Select PeopleTools, Security, Encryption, Algorithm Chain to access the Algorithm Chain page.



Algorithm Chain page

Although you can select any sequence of algorithms to define a chain, many possible sequences don't work because the cumulative effect of the algorithms doesn't make any sense. You must define sequences of compatible algorithms.

To apply any of the supported algorithms for symmetric encryption, hashing, encoding, or secure messaging, the input data must be in ASCII text format. Because PeopleSoft stores data in Unicode format, the first algorithm in most chains must be PSUnicodeToAscii, and the last algorithm must be PSAsciiToUnicode.

To define an algorithm chain:

1. Open an existing algorithm chain or create a new one.
2. Select the algorithm IDs of the algorithms you want to use in your chain.

   Add a new row for each algorithm. The available algorithms depend on the encryption libraries you previously loaded. You can select the algorithms in any order.
3. Specify the operation sequence for your algorithm chain.

   Enter a number in the Sequence box for each algorithm. The lowest number designates the first algorithm, and the highest number designates the last. When you save the chain, the rows are resorted according to their sequence numbers.
4. Save your algorithm chain definition.

Delivered Algorithm Chains

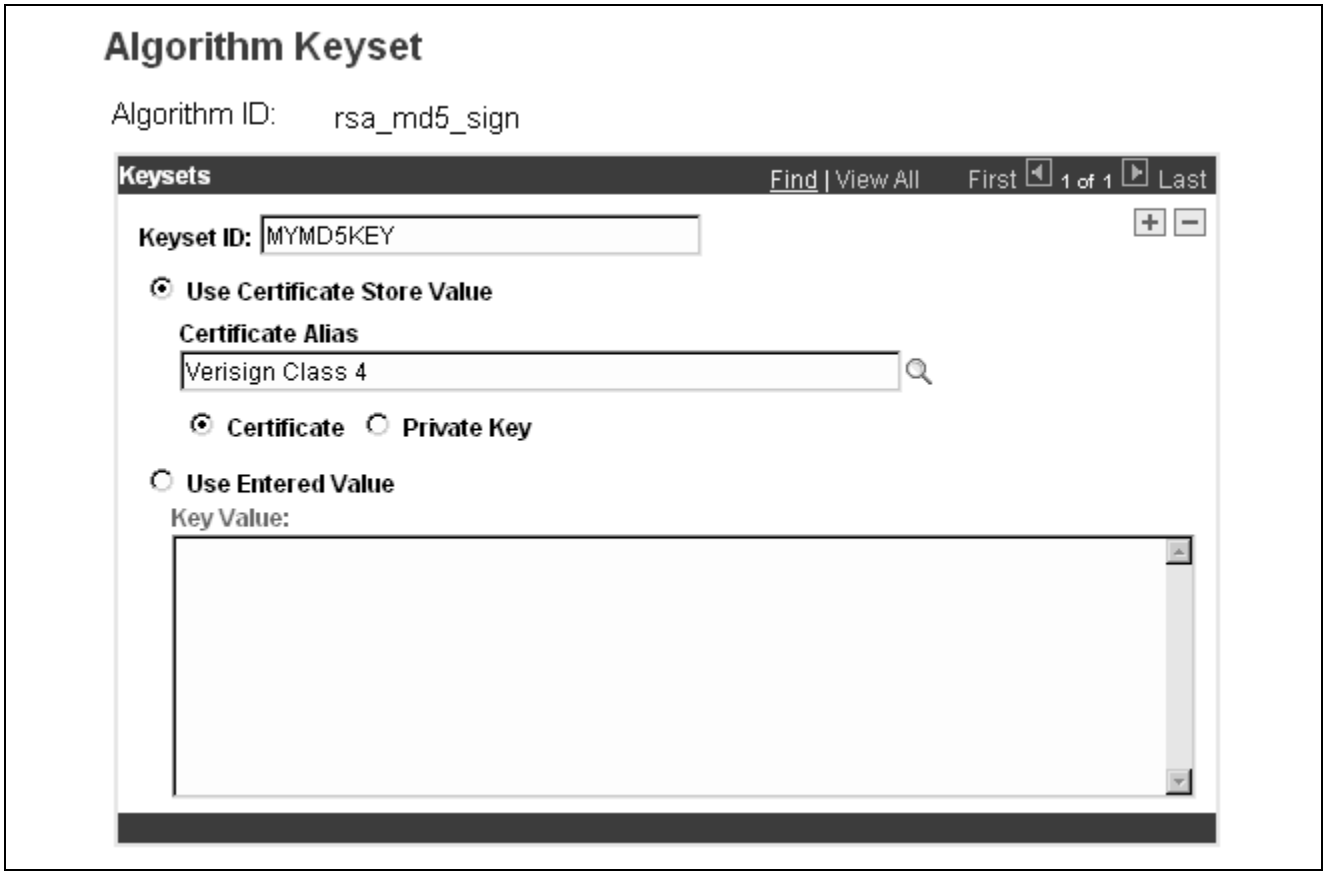
PeopleSoft delivers pluggable cryptography with the following predefined algorithm chains:

Algorithm Chain	Algorithms
3DES CBC B64 ENCRYPT	PSUnicodeToAscii 3des_ks168_cbc_encrypt base64_encode PSAsciiToUnicode
3DES CBC B64 DECRYPT	PSUnicodeToAscii base64_decode 3des_ks168_cbc_decrypt PSAsciiToUnicode
3DES CBC HEX ENCRYPT	PSUnicodeToAscii 3des_ks168_cbc_encrypt PSHexEncode PSAsciiToUnicode
3DES CBC HEX DECRYPT	PSUnicodeToAscii PSHexDecode 3des_ks168_cbc_decrypt PSAsciiToUnicode

Algorithm Chain	Algorithms
PKCS7_ENCRYPTED	PSUnicodeToAscii pkcs7_encrypted_encrypt PSAsciiToUnicode
PKCS7_DECRYPTED	PSUnicodeToAscii pkcs7_encrypted_decrypt PSAsciiToUnicode
PKCS7_ENCRYPTED_SIGNED	PSUnicodeToAscii pkcs7_signedandencrypted_signandencrypt PSAsciiToUnicode
PKCS7_DECRYPTED_VERIFY	PSUnicodeToAscii pkcs7_signedandencrypted_decryptandverify PSAsciiToUnicode
PGP_ENCRYPTED	PSUnicodeToAscii pgp_encrypted_encrypt PSAsciiToUnicode
PGP_DECRYPTED	PSUnicodeToAscii pgp_encrypted_decrypt PSAsciiToUnicode
PGP_ENCRYPTED_SIGNED	PSUnicodeToAscii pgp_signedandencrypted_signandencrypt PSAsciiToUnicode
PGP_DECRYPTED_VERIFY	PSUnicodeToAscii pgp_signedandencrypted_decryptandverify PSAsciiToUnicode

Defining Algorithm Keysets

Select PeopleTools, Security, Encryption, Algorithm Keyset to access the Algorithm Keyset page.



Algorithm Keyset page

Specify an algorithm ID or description to view the keyset of any algorithm in the PET database. Each row displays a key value. You can add, modify, or remove key values.

Keyset ID Enter a name for the key value in the current row. each row must have a unique keyset ID for this algorithm.

Use Certificate Store Value This option enables you to take advantage of key values already stored in the PeopleSoft keystore. Select a certificate alias from the keystore, then indicate whether the alias represents a certificate (for encryption) or a private key (for signing).

Warning! Certificates in the PeopleSoft keystore are in standard X.509 format, which is compatible for use with the internal and OpenSSL algorithms, but is *not* compatible with the PGP encryption library. If you're defining the keyset for a PGP algorithm, you must select the Use Entered Value radio button.

Use Entered Value Select this option to use key values that aren't in the PeopleSoft keystore. Enter a key value that's formatted appropriately for the algorithm that you're configuring. This value will be entered into the PET keyset table, not the PeopleSoft keystore.

The value that you enter has a length that depends on the keysize of the cipher. For triple DES with keysize 112, this is 16 bytes. For a keysize of 168, this is 24 bytes. This value should be represented in hex notation.

You must generate the key value that you enter here. You can use any key generation utility capable of producing hex encoded keys of the required length. PeopleSoft delivers the core OpenSSL command line program precompiled and ready to use. You can use it to generate key values and perform other encryption-related tasks. The executable program is *PS_HOME*\bin\server\WINX86\openssl.exe on Windows, and *PS_HOME*/bin/openssl on Unix and Linux platforms.

Note. The key value that you enter here is stored in the PET keyset table using a combination of the algorithm ID and the keyset ID as its identifier. Because this combination is unique for each algorithm, you can create identically defined keyset rows for multiple algorithms.

See Also

Chapter 9, “Securing Data with Pluggable Cryptography,” OpenSSL Library Considerations, page 163

http://www.openssl.org/

Defining Encryption Profiles

Select PeopleTools, Security, Encryption, Encryption Profile to access the Encryption Profile page.

Encryption Profile page

To define a new encryption profile, specify a new profile ID, then select an algorithm chain ID. Each algorithm in the chain appears in order, in its own row with its algorithm ID and chain sequence number. Its parameters each appear in a row, displaying the parameter's name and default value, and indicating whether the parameter represents a key. You can override a parameter's default value by editing it in the Parameter Value edit box.

Deleting an Encryption Profile

To delete an encryption profile, select PeopleTools, Security, Encryption, Delete Encryption Profile. Select the profile you want to delete, and click Delete on the Delete Encryption Profile page.

Testing Encryption Profiles

Select PeopleTools, Security, Encryption, Test Encryption Profile to access the Test Encryption Profile page.

Test Encryption Profile page

Use this page ensure that your encryption profiles produce the expected results. To test an encryption profile:

1. Select the profile's encryption profile ID.
2. In the Text to be Encrypted field, enter or paste the input text.
3. Click Run Encryption Profile.

   The resulting output text appears in the Encrypted Text field.

You can use this page to test decryption as well. You can also test complementary pairs of profiles — one to encrypt, and the other to decrypt. By copying the result of the encryption profile test and pasting it as input to the decryption profile test, you can determine whether the text you get out is the same as the text you put in.

Invoking Encryption Profiles from PeopleCode

You access the encryption profile using the PeopleCode crypt class.

Following is an example of PET PeopleCode:

```
&cry = CreateObject("Crypt");
&bar = QE_CRYPT_WRK.CRYPT_PRFL_ID;
&cry.Open(&bar);
&cry.UpdateData(QE_CRYPT_WRK.DESCRLONG);
QE_CRYPT_WRK.LARGECHAR = &cry.Result;
```

See Also

Enterprise PeopleTools 8.45 PeopleBook: PeopleCode API Reference, "Crypt Class"

CHAPTER 10

Implementing Query Security

This chapter discusses how to:

- Define query profiles.
- Build query access group trees.
- Work with query trees.
- Define row-level security and query security records.

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

Defining Query Profiles

Query takes advantage of user's security settings, row-level security, and primary permission list. 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 Query Access Group Manager, and then you assign users to those groups with Query permissions. Keep in mind that Query permissions are enforced only when using Query; it doesn't control run-time *page* access to table data.

Building Query Access Group Trees

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

You create and update query access group trees using Query Access Manager. To get you started, we've included some sample query access group trees with your PeopleSoft applications. Which trees you have depend on which PeopleSoft applications you've installed. Each tree contains access groups and record definitions categorized by function.

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

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

Query Access Group Tree Considerations

You should create your own query access group trees based on your organization's needs and on any customizations you've made. Remember that the sample trees we provide may be replaced when you upgrade to a subsequent PeopleSoft release, so if you modify the samples rather than create your own trees, you may lose your customizations.

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

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

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

Working with Query Trees

This section provides an overview of Query access group trees and discusses how to:

- Open Query access group trees.
- Define your Query tree.
- View and modify definitions.

Understanding Query Access Group Trees

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

Nodes

Regarding nodes, consider the following:

- Query access group trees contain two types of Nodes: groups and records.
- Groups are a logical representation of a set of child groups or records. It is similar to folder in Windows.
- Records represent a PeopleSoft record definition.

Structure

Regarding structure, consider the following:

- Always use the ACCESS_GROUP Tree Structure.
- Do not use SetID or UKV/BU.

- Do not have Details.
- Do not use Levels.
- No Branches.

Requirements

Regarding requirements, consider the following:

- The Root Node is always a group.
- Groups must be unique in a given Tree while records definitions can be repeated.
- Groups and records could have Child Groups and Child Records.
- Each record needs a unique fully qualified path in the tree. You can't add the same record under the same parent node (group or record).

Opening Query Access Group Trees

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

To open a Query tree definition:

1. Select PeopleTools, Security, Query Access Manager.
2. On the Basic Search page select your search criteria.

   You can search by Tree Name, Tree Category, or Tree Description.
3. Click Search.

   After clicking Search, a list appears containing the definitions that meet your criteria.
4. Double-click on the appropriate definition.

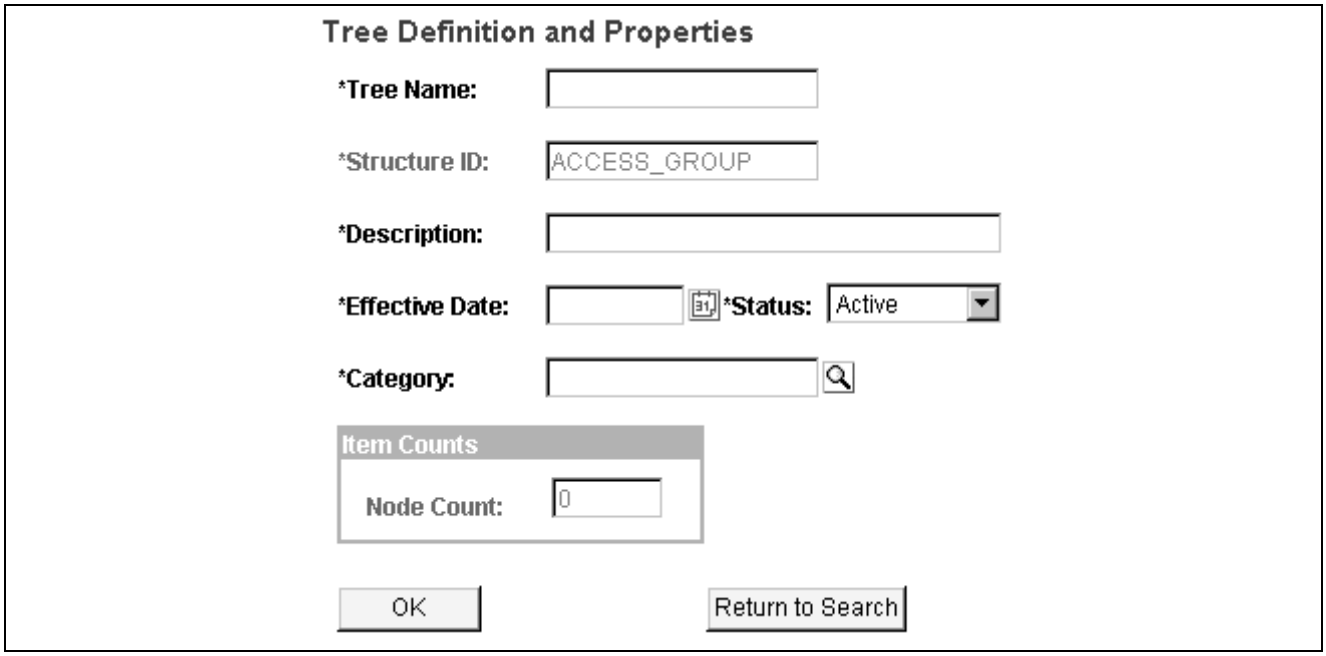
   The list of trees in the lower part of the page also serves as a maintenance utility enabling you to Delete or Copy a tree. If you click Delete, the system prompts you to confirm the action, and if you click Copy, the system displays the Copy Tree page where you can select a name for the copied tree.

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

Defining Your Query Tree

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

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



Tree Definition and Properties page

Tree Name For the tree name, we recommend that you start the name with QRY_ so that you can easily identify the tree as a custom query tree. The standard query trees we deliver with the system start with QUERY_.

Structure ID The Structure ID is read only and always reads ACCESS_GROUPS for Query access trees.

Description This description will appear along with the name and effective date in the list box whenever you select from a list of trees.

Effective Date The status default is set to Active. Query trees are available immediately if the effective date is active; you don't need to run an SQR utility like you do for organizational security trees.

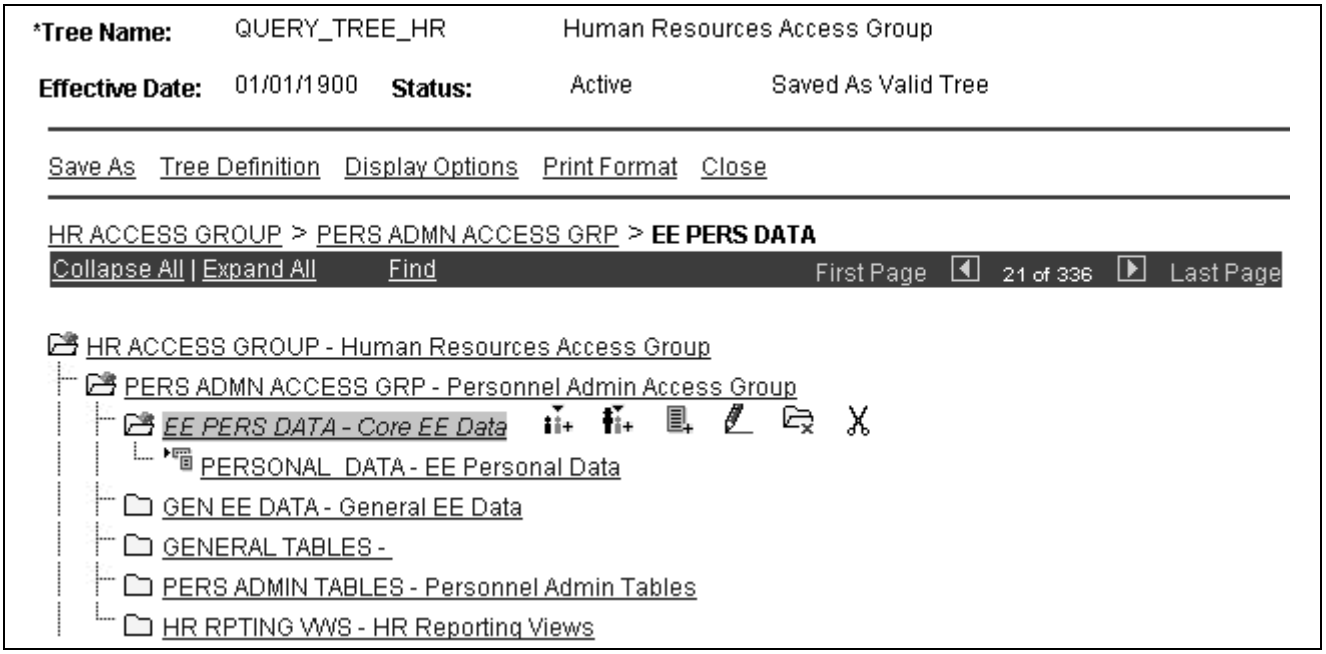
Category If necessary add a category, which are groupings of the definitions.

Item Counts Item Counts shows the number of nodes within the access group.

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

Viewing and Modifying Definitions

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



Maintain Security. Setup, Query Access Group Manager

Tree Name Shows the name of the current tree.

Effective Date Shows the current effective date.

Status Shows either Active or Inactive.

Save, Save As These are the two save options. Each option appears only if it relates to your current activity. Save enables you to save your changes to the database. Save As enables you to clone tree definitions at save time.

Tree Definition Shows the Tree Definition and Properties page that you modified when you created the definition.

Display Options Shows the Configure User Options page where you can adjust the presentation of the trees. For example, you can choose whether the Node ID appears and how many lines of the definition appear at a time. Most of these don't apply for Query Access Trees so they're disabled.

Print Format Shows what your tree definition will look like when you print it. Essentially, this is a print preview.

Close Closes the definition and returns you to the search page.

Bread Crumbs Once you have drilled down into a definition, a bread crumb display appears just above the Collapse/Expand All controls. This is to provide orientation, especially within large trees.

Collapse All Collapses all nodes of the tree into their parent groups so that you see only the root node and the first layer of child groups.

Expand All Expands all nodes of the tree so that each child object is visible.

Find If you are looking for a specific access group or a record you can use the Find Value page rather than drilling down into your tree. You specify an

access group or a record or its description. You can select a case sensitive search and specify that an exact match must be found.

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

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

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

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

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

Collapse Node When a node folder is open, you click on it to collapse the node.

Expand Node When a node folder is closed, you click on it to expand the node.

Node/Record Controls When you have a node or record selected, the actions you perform are controlled by the icons that appear to the right of the definition. The descriptions of the actions are below. You can roll the mouse over the icon to reveal a label.

Insert Sibling Group Inserts an access group node at the same level as the currently selected node.

Insert Child Group Inserts an access group node at the next level lower than the currently selected node.

Insert Child Record Inserts a record definition within an access group node.

Edit Data For access groups you can edit the Description and the Definition (long description) on the Access Group Table.

Delete You can delete both access groups and records. You can't delete the root node.

Cut/Paste as Child You can cut and paste access groups and records to move them within the tree. Once a cut has been executed, then the Paste as Child icon becomes enabled. You can't cut the root node.

Note. After you perform the "cut" function, only navigation and search features are available until you execute the "paste" function. This protects the node in the clipboard.

Defining Row-Level Security and Query Security Records

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

This section describes the relationship between row-level security and Query security record definitions.

Row-Level Security

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

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

Query Security Record Definitions

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

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

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

To apply row level security:

1. Select PeopleTools, Application Designer to open the Application Designer, and open the record on which you want to apply row-level security.
2. With the record definition open in the Application Designer, click the Properties button, and select the Use tab from the Record Properties dialog box.

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

   ---

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

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

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

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

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

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

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

CHAPTER 11

Implementing Definition Security

This chapter provides an overview of definition security and discusses how to:

- Work with definition groups.
- View definition groups.
- Add and remove definitions.
- Assign definition groups to permission lists.
- Enable display only mode.
- View definition access by user and permission list.

Understanding Definition Security

This section discusses:

- Definition security.
- Definition groups and permission lists.
- Definition security rules.

Definition Security

You can restrict developer access to the record definitions, menu definitions, page definitions, and others that make up your applications. Just as you use Security to control who can access the PeopleSoft pages in your system, you use Definition Security to control who can access and update PeopleTools definitions.

There are two tasks involved with definition security:

- Creating definition groups.
- Linking definition groups to predefined permission lists.

Definition security leverages the permission lists created in PeopleTools Security to restrict access to individual PeopleTools database definitions created using a PeopleTools designer utility, such as PeopleSoft Application Designer or PeopleSoft Tree Manager. Definition types include all of the definitions that appear in the following table. Most definition types are created in PeopleSoft Application Designer.

Definition Type	Associated Designer Tool
Activities	PeopleSoft Application Designer
Application Engine Programs	PeopleSoft Application Designer
Application Packages	PeopleSoft Application Designer
Approval Rule Sets	PeopleSoft Application Designer
Business Interlinks	PeopleSoft Application Designer
Business Processes	PeopleSoft Application Designer
Components	PeopleSoft Application Designer
Component Interfaces	PeopleSoft Application Designer
Fields	PeopleSoft Application Designer
File Layouts	PeopleSoft Application Designer
HTML	PeopleSoft Application Designer
Images	PeopleSoft Application Designer
Menus	PeopleSoft Application Designer
Message Channels	PeopleSoft Application Designer
Messages	PeopleSoft Application Designer
Mobile Pages	PeopleSoft Application Designer
Pages	PeopleSoft Application Designer
Problem Types	PeopleSoft Application Designer
Projects	PeopleSoft Application Designer

Definition Type	Associated Designer Tool
Queries	PeopleSoft Query
Records	PeopleSoft Application Designer
SQL	PeopleSoft Application Designer
Style Sheets	PeopleSoft Application Designer
Tree Structures	PeopleSoft Tree Manager
Trees	PeopleSoft Tree Manager
Translate Tables	PeopleSoft Application Designer

Note. You can restrict access to an entire definition type, such as records or pages, using the PeopleTools page in Security. This works by controlling access to the PeopleSoft Application Designer functionality that works with a particular definition type. For example, if you don't want developers to use application engine programs, don't allow them to access PeopleSoft Application Engine.

Definition 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 access to every record definition that contains the EMPLID field. 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 definitions are not well secured, problems may result.

Before you start using Definition Security, it's a good idea to define the definition security needs of your users. For example, should all developers have access to all PeopleTools definitions? Should payroll developers have access only to payroll definitions? Who will be allowed to access PeopleSoft Application Designer? These are the types of questions you need to consider.

Definition Groups and Permission Lists

Use Definition Security to define definition groups and link them to permission lists that you created in Security.

A definition group is a collection of one or more definitions that form a logical group for security purposes. For example, suppose you've created a permission list for analysts that support the PeopleSoft Payroll module, and you call it PAYROLL_DEV. These analysts are allowed to update only payroll definitions. Using Definition Security, you would create a definition group containing only payroll definitions, and give it a name, such as PAYROLL_OBJ. Then you link that definition group to the corresponding permission list. In this case, you link PAYROLL_OBJ to PAYROLL_DEV.

You can assign multiple definition groups to a single permission list.

You can't declare directly that a particular permission list can modify a specific definition type. You do so indirectly by creating a definition group that consists solely of the desired definition type. Also, remember that you can assign a definition to multiple groups as needed. To ensure total definition security, assign every definition to at least one definition group.

Note. PeopleTools databases are delivered with a predefined definition group called PEOPLETOOLS that contains all the PeopleTools definitions. Until you create definition groups of your own, the PEOPLETOOLS definitions are the only definitions that you can secure.

Definition Security Rules

To set up Definition Security properly, it's helpful to understand how the system interprets definition security settings. The system applies the following rules to determine whether a user is authorized to update a definition:

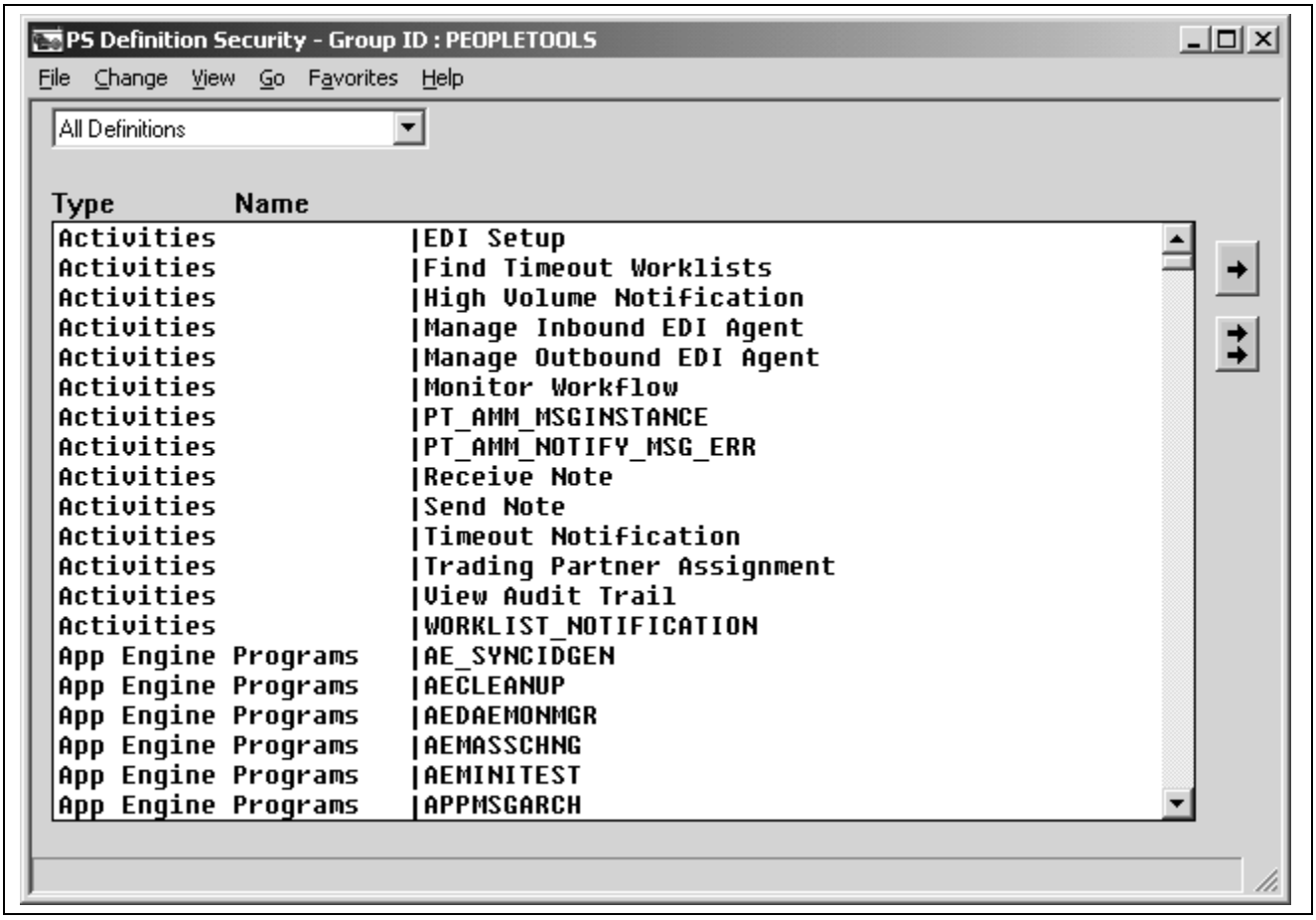
Rule	Description
1	Is the definition type assigned to any definition group? If not, then anyone has update access to it. For this reason, you should add all definition types to at least one definition group.
2	Is the definition type a part of a definition group assigned to the user's permission lists? If not, the system denies access and displays a message, such as: <*definition_name*> is not a definition that you are authorized to access.
3	Do all the definition groups of which the definition type is a member have the display-only option enabled? If so, then the system displays the message: <*definition_name*> is not a definition that you are authorized to update. The definition type would then appear, but with the Save command disabled.

If the definition passes these system checks, the user is allowed to access and update it—unless it's a PeopleSoft Application Designer definition, in which case several other security checks are performed first. PeopleSoft Application Designer definitions are also controlled by the PeopleTools in permission lists.

Important! A user gets definition security permissions from the primary permission list, not through roles.

Working With Definition Groups

PeopleSoft Definition Security is a Windows-based application that you can access from PeopleSoft Application Designer. To launch PeopleSoft Definition Security, select Go, Definition Security. The PS Definition Security window appears.



PS Definition Security displaying all definitions

To open an existing definition group:

1. Select File, Open, Group.

   The Definition Security Open dialog box appears.
2. Select a group ID.
3. Click OK.

To create a new definition group:

1. Select File, New Group.
2. Add definitions to the group.
3. Save the group and give it a name in the Save Group As dialog box.

To clone a definition group:

1. Open the definition group you want to clone.
2. Select File, Save As.

   The Save Group As dialog appears.
3. Enter a group ID and click OK.

To rename a definition group:

1. Select File, Rename.

   The Rename Group ID dialog box appears.
2. From the Rename list, select the group that you want to rename.
3. Enter a new group ID in the To edit box.
4. Click OK.

To delete a definition group:

1. Select File, Delete.

   The Definition Security Delete dialog box appears.
2. Select the group ID for the group you want to delete.
3. Click OK.

   You are prompted to confirm the deletion.

Viewing Definition Groups

This section discusses how to:

- Select a view.
- View all definitions.
- View definitions of a specific type.

Selecting a View

You can select how you view a definition group by using the View menu, or by selecting an item from the drop-down list box that appears at the top of the application window when you have a definition group open.

Viewing All Definitions

To see the entire definition group, select View, All Definitions.

You see every definition, regardless of type, assigned to the definition group. There are two columns: Type and Name.

- Type identifies the definition type, as in page, query, and so on.
- Name refers to the name given to the definition when it was created.

Viewing Definitions of a Specific Type

To view definitions of a particular type that belong to a definition group, select View, Pages.

The view window is split vertically into two list boxes. The box on the left contains a list of definitions that belong to the definition group and are of the selected type.

The list box on the right is the Excluded <*Definition Type*> list. The label for the definition type changes according to the definition type you are viewing. For example, when you view pages, the label is Excluded Pages, and when you view menus, the label reads Excluded Menus, and so on. The Excluded <*Definition Type*> list box displays the names of all the definitions of the selected type that are not included in the current definition group.

Adding and Removing Definitions

This section discusses how to:

- Add and remove definitions.
- Remove definitions from a definition group.

Adding and Removing Definitions

To add definition types to a definition group, you need to view by the type of definition that you want to add. To add pages to a definition group, select View, Pages.

To add definitions to a definition group:

1. Open the definition group.
2. Select the definition type to view by.

   Use the View menu or the drop-down list box at the top of the application window.
3. Select the definitions to be added.

   In the Excluded *definition_type* list box, select the definitions to add to the active definition group. To select multiple definitions, use CTRL or SHIFT keys as you click.
4. Click a left-arrow button to move the definitions into the group.

   To move just the selected definitions, use the single left arrow. To move all excluded definitions into the group, use the double left arrow.

Removing Definitions From a Definition Group

To remove definitions from a definition group:

1. Open the definition group.
2. Select the definition type to view by.

   Use the View menu or the drop-down list box at the top of the application window.
3. Select the definitions to be removed in the list box on the left.

   To select multiple definitions, press CTRL key while you click.
4. Click one of the right-arrow buttons to move the definitions out of the group.

   To move just the selected definitions, use the single right arrow. To remove all definitions from the group, use the double right arrow.

Assigning Definition Groups to Permission Lists

To link a definition group to a permission list, the permission list must already exist.

To link definition groups to a permission list:

1. Select File, Open, Permission List.

   The Definition Security Open dialog box appears.

2. Select a permission list and click OK

   The window displays two list boxes, similar to what you see when adding or removing definitions.

   The list box on the right shows the existing definition 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. The group ID is the name that you specified when saving a definition group.

3. Specify the included and excluded groups.

   To enable access to a definition 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 arrows

   The All Definitions group includes all system definitions. Use it to grant unrestricted access to all databases.

4. Select File, Save to save your changes

Enabling Display Only Mode

Enabling display-only access to a definition group means the definitions in that group can be viewed but not modified. You need to link the definition group to the permission list before you specify a display-only value.

For the All Definitions group, display-only mode applies only to the definition groups in the Excluded Group ID list.

The following example shows a permission list (INVPANLS) with access to all definitions, or All Definitions 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. This means that the INVPANLS permission list has read and write access to all definitions in the system except for those that appear in the Excluded Group ID list. For those definitions, INVPANLS only has read access.

To enable or disable display-only access:

1. Select Change, Display Only.

   The Definition Security List dialog box appears.

   This dialog box lists all the definition groups assigned to the current permission list.

2. Select the groups in the list that you want to make display-only.

   You can use the All button to select all the groups in the list.

3. Click OK.

Viewing Definition Access by User and Permission List

To view a report showing what definitions a user or a permission list can access, use the User Profiles - User ID Queries and Permission Lists - Permission List Queries page, respectively.

On the User Profiles - User ID Queries page, click the User ID's Application Designer Object Access link.

On the Permission Lists - Permission List Queries page, click the Permission List's Application Designer Object Access link.

See Also

Chapter 5, "Administering User Profiles," Running User ID Queries, page 78

Chapter 3, "Setting Up Permission Lists," Running Permission List Queries, page 27

CHAPTER 12

Managing PeopleSoft Personalizations

This chapter provides an overview of personalizations and discusses how to:

- Work with personalization options.
- Define personalization options.
- Work with category groups.
- Work with categories.
- Work with locale-based personalizations
- Add personalizations to permission lists.
- Create custom personalization options.
- Work with the My Personalizations interface.

Understanding 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. You select, customize, and define personalizations using the Personalization PeopleTool.

To access the Personalization PeopleTool, select PeopleTools, Personalization.

Personalizations are grouped in three levels of categories to aid in development, organization, and deployment. The levels are:

- The first level is the Option Category level. This level divides personalizations between functional area, such as PeopleTools personalizations and HCM personalizations. Also, there is a category for custom personalizations, which are those personalizations you develop and deploy in addition to the delivered personalizations.
- The second level is the Category Groups, which represent individual products within a Category Level. For example, within the PeopleTools Category Level some Category Groups are Application Designer, Process Scheduler, Security, and so on. Or, within the HCM Category Level one Category Group could be Payroll.
- The third level is the Personalization Categories themselves. This is the level that the end user sees. A category represents a product feature, such as navigation or system messages. A category contains a set of related personalizations.

After you have selected the personalizations for your site, you assign them to a user, or role, by way of the Personalizations page in the permission lists component in PeopleTools Security. The Personalizations tab enables the security administrator to assign role-based personalizations and enable user control for selected personalization options, if needed.

End users can view their personalization options and, if allowed, customize them. They use the My Personalization page to access and customize personalizations.

The following sections provide more details on defining, customizing, and deploying PeopleSoft Personalizations.

Working with Personalization Options

Before you begin defining and deploying personalization options, you first need to be familiar with the types of personalization options delivered by PeopleSoft and the pages used to view and modify them. This section discusses:

- Navigation options.
- International and regional options.
- General options.
- System and application messages.
- Internal options.
- Pages used to define and modify personalizations.

Note. PeopleSoft Mobile applications use the standard personalizations.

Understanding Navigation Options

The following table presents the delivered navigation options.

Note. PTPT1000 is a delivered permission list that you can use as a starting point for a user permission list. The column shows whether PTPT1000 allows a user to modify the option.

Item	Option Code	Initial Setting	PTPT1000	Description
Tab over Add /Delete buttons	ADBTN	No	No	Tab over the + and - buttons within grids and scrolls. This is a Yes/No option.
Automatic Menu Collapse	AUTOMENU	No	Yes	Enabling this personalization causes the menu to automatically collapse when a transaction is selected. You expand the menu either by using Ctrl-X or the show menu icon.

Item	Option Code	Initial Setting	PTPT1000	Description
Show browser address location	BADDRESSBAR	Yes	No	Enable the display of the browser's address bar.
Show browser navigation bar	BBUTTONS	Yes	No	Enable the display of the browser's navigation bar, which usually contains the Back, Forward, Home, and Refresh buttons among others, depending on the browser in use.
Show browser links	BLINKS	Yes	No	Enable the display of any links displayed by the browser.
Show browser menu	BMENU	Yes	No	Enable the display of the browser's menu bar.
Tab over calendar buttons	CALBTN	No	Yes	Tab over the calendar controls on pages. Calendar controls appear as a calendar button. This is a Yes/No option.
Tab over grid tabs	GRDTAB	No	Yes	Enable users to tab over the tabs or headings within grids. This is a Yes/No option.
Max rows for View All	GRDRWS	100	No	Specify the maximum number of rows that will be displayed in a grid or scroll area.

Item	Option Code	Initial Setting	PTPT1000	Description
Tab over header icons	HDRICN	No	Yes	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	LKPBTN	No	Yes	Enable users to tab over the lookup buttons to the right of edit boxes that have an associated list of Valid Values. This is a Yes/No option.
Tab over navigation bar	NBAR	No	Yes	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.
Tab over Non-PeopleSoft elements	NONPS	No	Yes	You can restrict tabbing to the PeopleSoft elements of the page only. This is a Yes/No option.
Tab over page links	PGLNK	No	Yes	Enable users to tab over links to other pages in the same component. This is a Yes/No option.

Item	Option Code	Initial Setting	PTPT1000	Description
Tab over related page links	POPUP	No	Yes	Enable users to tab over the Pop-up icon. The Pop-up icon opens a page of related links. This is a Yes/No option.
Tab over toolbar	TBAR	No	Yes	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.

Understanding International and Regional Options

The following table presents the delivered Locale options.

Note. PTPT1000 is a delivered permission list that you can use as a starting point for a user permission list. The column shows whether PTPT1000 allows a user to modify the option.

Item	Option Code	Initial Setting	PTPT1000	Description
Afternoon designator (PM, pm)	ADES	PM	Yes	Designate the the string to use to indicate PM on a 12 hour display, such as *PM* or *pm*. The value has a 5-character limit.
Date Format	DFRMT	MDY	Yes	Specify how the date is expressed. You have the following options: • *DDMMYY* (Day First). • *MMDDYY* (Month First). • *YYMMDD* (Year First).

Item	Option Code	Initial Setting	PTPT1000	Description
Decimal Separator	DCSP	.	No	Specify the decimal character for values with decimals, such as *1.00* or *1,00*.
Date Separator	DTSP	/	No	Specify how you want to separate the month, day, and year. For example, you can use a '-' for 01-01-2001, or a '/' for 01/01/2001.
Local Time Zone	LTZONE	Pacific Time (US), Tijuana	Yes	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. This alters the *display* of the time for the end user, but does not affect the Base Time Zone setting on the PeopleTools Options page.
Morning Designator (AM, am)	MDES	AM	Yes	Specify the string to use to indicate AM in a 12–hour clock display, such as *AM* or *am*. The value has a 5-character limit.

Item	Option Code	Initial Setting	PTPT1000	Description
Time Format	TFRMT	12 hour clock	Yes	Specify how you want time to appear. You have two choices: 12 hour clock (01:05:00 PM) or military time 24 hour clock (13:05:00). Whether or not microseconds appear is not a personalization option.
Time Separator	TMSP	:	No	Specify how you want to separate hours, minutes, and seconds, such as with a ':' or a '.'. This field has a 1-character limit.
Digit Group Separator	TSEP	,	No	Specify how you want numerical values over 999 expressed — grouped with a comma as in 1,000 or with a period as in 1.000. In order to use a space for the digit group separator, use a space between single quotes (for example, ' ')
Use local time zone	TZONE	No	Yes	Specify whether transactions are to use the local time zone of the client machine or that of the server, where the server may in turn be set to a corporate time zone.

Understanding General Options

The following table presents the delivered general options.

Note. PTPT1000 is a delivered permission list that you can use as a starting point for a user permission list. The column shows whether PTPT1000 allows a user to modify the option.

Item	Option Code	Initial Setting	PTPT1000	Description
Accessibility	ACCESS	Accessibility features off	Yes	Provides better support for assistive technologies. • Option A [Use accessible mode layout] is for use with screen readers. Page elements (fields, links, buttons, and so on.) are presented linearly to assistive software. • Option S [Use standard mode layout] supports assistive technologies without altering the page design. • Option N [Accessibility Features disabled] is the default.

Item	Option Code	Initial Setting	PTPT1000	Description
Excel 97 grid download	EXCEL97	N	Yes	If you plan to download a page grid to Microsoft Excel 97, and you want to use the character set defined in the user language — that is, you want to use a character set other than the default UTF-8 character set — you must specify a value of *Y* for this option. **Note.** This option is recommended only for non-English users who use Excel 97. It isn't recommended for Excel in Microsoft Office 2000 and above.
Customize Page Settings	CUSTOMPGSET	Yes	No	When Customize Page Settings is enabled, the Customize Page pagebar link appears at runtime. End users can define, share, and copy page personalizations. When disabled, all existing page personalizations for the end users are deleted. However, grid personalizations aren't affected.

Item	Option Code	Initial Setting	PTPT1000	Description
Time Page Held in Cache	METAXP	900	Yes	Enable browser caching for the navigation pages that remain relatively static. This option applies to the portal homepage and navigation pages. You need to explicitly specify the appropriate time in minutes for your site.
Multi Language Entry	MLTLNG	No	Yes	When Multi Language Entry is enabled, users can enter data in the language specified for pages where multiple language entry is available. The user selects the preferred language from the Data Language dropdown list.
Spell Check Dictionary	SCLANG	Use Session Language	Yes	Enable the end user to set the default language for the Spell Check Dictionary.

See Also

Enterprise PeopleTools 8.45 PeopleBook: Internet Technology, "Using Portal Caching Features"

Understanding System and Application Messages

System messages are those that the system displays for the user when certain events occur such as a save or a request to view another page.

Note. PTPT1000 is a delivered permission list that you can use as a starting point for a user permission list. The column shows whether PTPT1000 allows a user to modify the option.

Item	Option Code	Initial Setting	PTPT1000	Description
Save Confirm message	SCNFRM	Yes	No	Provides a brief message confirming a Save action.
Save Warning message	SWARN	Yes	Yes	Displays a warning when the user makes a change and attempts to leave the transaction without saving.

Understanding Internal Options

The following table presents the delivered internal options for using Query.

Item	Option Code	Initial Setting	Description
Display of query names	NAMESTYLE	N	Used with PeopleSoft Query. Name Style is either 'Name and Description' or 'Description only'. It refers to how records and field names are displayed. Used mostly for global users where the record names are in English but the descriptions are in another language.
Enable Auto Join	AUTOJOIN	Y	Used with PeopleSoft Query. Query automatically determines the join conditions for you when a new record component is added.
Display of records	DICTIONARY	N/A	Not currently used in PIA Query.
Ways to sort	SORTBY	N/A	Not currently used in PIA Query.

Pages Used to Define and Modify Personalizations

Page Name	Object Name	Navigation	Usage
Define Personalizations	PSUSEROPTNDEFN	PeopleTools, Personalization, Personalization Options	View, modify, or add personalization option definitions and their formats. View or modify the explanations that end users see in the My Personalization interface.
Category Groups	USEROPTN_CAT_GRP	PeopleTools, Personalization, Category Groups	View or modify the grouping of options for administrative and ownership purposes.
Category	USEROPTN_CAT	PeopleTools, Personalization, Categories	View or modify the categories in which personalization options are grouped for end users.
Locale Definition	PSLOCALEDEFN	PeopleTools, Personalization, Locales	Control the locales for which you can specify defaults.
Locale Defaults	PSLOCALEOPTNDFLTS	PeopleTools, Personalizations, Locale Defaults	Specify defaults for locales appearing on the Locale Definition page.
My Personalizations	PSUSERPRSNLCAT	My Personalizations	End users access this page to view and modify personalizations

Defining Personalization Options

This section covers topics related to selecting, modifying, and creating personalization options for your site.

This section provides an overview of the Search page and discusses how to:

- Use the Definition tab.
- Use the Format tab.
- Use the Explanation tab.

Note. Adding personalization options involves setting up your options in the Personalizations interface, implementing the behavior using PeopleCode, and adding the appropriate permissions through PeopleTools Security. Adding a row to the table using the following interface is only one part of the process.

Understanding the Search Page

To access the personalization definition pages, select PeopleTools, Personalization, Personalization Options. On the search page, you have the option to search by Option Category Level or Description. If you select Option Category Level and click Search, the following result set appears.

- Customer Relationship Management (CRM).

- Custom (CSTM).
- Enterprise Performance Management (EPM).
- Financials (FIN).
- Human Resources (HCM).
- Learning Solutions (LS).
- PeopleTools (PPLT).
- Supply Chain Management (SCM).

Note. These are the only available Option Category Levels. You can't add custom Option Category Levels.

This list corresponds directly to the collection of PeopleSoft applications. In addition, there is a Custom category where you store any personalization options you create for applications you have built using PeopleTools. You can also add, or extend, the personalizations for each category. For instance, if you wanted to add a new personalization to the HCM category, you add it to the list and define it.

This high-level separation of the personalization options enables you to take a modular approach in deploying the options to your user base. It also helps you to avoid collisions by separating equivalent personalization options by application. For example, you can assign different default values for the same personalization for your Human Resources and Financials applications.

Before adding or modifying personalizations, you select the appropriate category. For instance, for CRM personalizations, select the CRM category.

Note. Regardless of whether you have installed all of the applications listed in the Option Category Level options, the same category levels appear. Ignore any categories that do not apply to your site.

You add and modify the delivered personalization options using the Define Personalizations component.

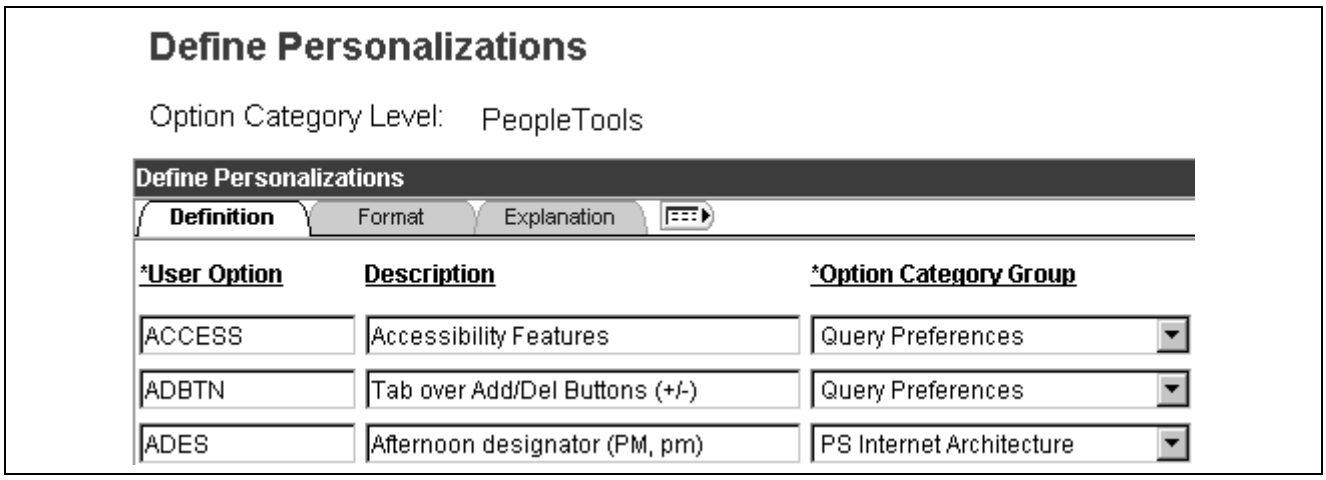
To access this interface, select PeopleTools, Personalization, Personalization Options. This interface contains the following grid tabs.

- Definition
- Format
- Explanation

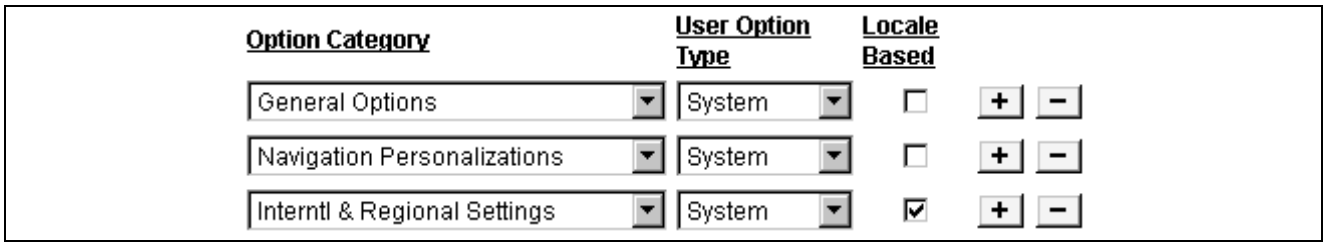
You use this grid to view and to modify the personalizations within the Category Level you selected on the search page.

Using the Definition Tab

Access the Definition tab.



Definition Tab (1 of 2)



Definition Tab (2 of 2)

User Option Displays the code associated with the user option. This is the code that the system (PeopleCode) recognizes at run time.

Description This is the description of the option that the end user sees on the My Personalizations interface. The description should be unique within the same category. When adding custom personalizations, special attention needs to be paid to this field. Make sure the description is meaningful to end users.

Option Category Group Specify the product or functional groupings of options. This value acts as an administrative attribute providing ownership for maintenance purposes. It further divides the Option Category Level.

Option Category Categorizes and encompasses a set of options for the end user. The option you select determines the button the end user clicks to view and modify the option.

You add new Categories using the Category page.

User Option Type Enables you to set where an option is exposed to the end user for override purposes. There are two options:

- *Functional.* These are options that users set within an application or PeopleTool, such as the Application Designer preferences. Functional personalizations are not exposed to the end user through the personalizations pages. If the users have access to the tool or component, then they are able to override the settings.
- *System.* Options that are exposed directly to the user through the personalization pages. A user can override default values if permission lists grant they authority.

Locale Based Indicates that the option derives the default values based on the Locale of the browser.

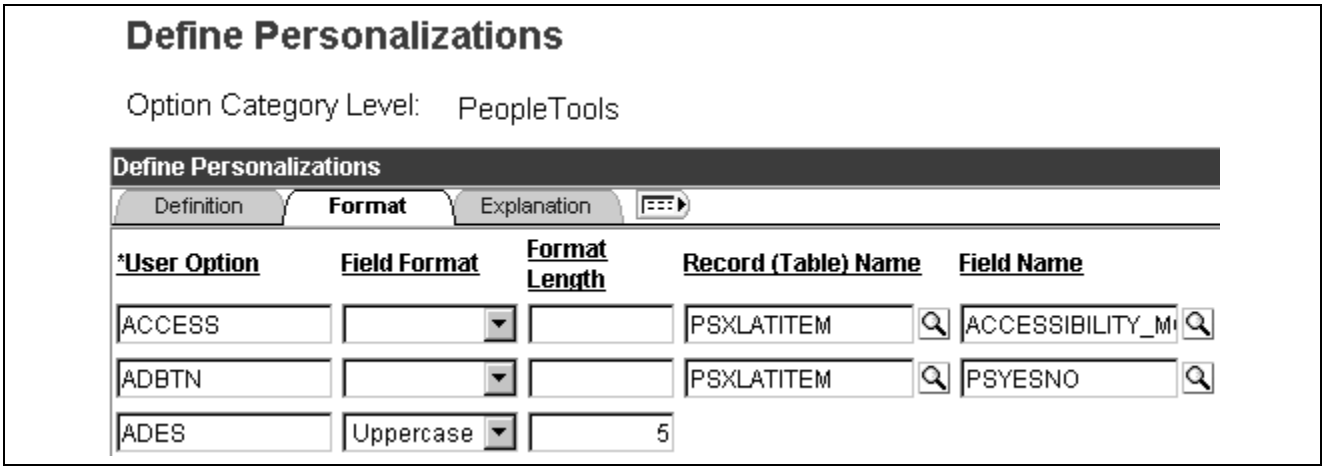
To add an option, use the plus sign button. To delete an option, use the minus sign button.

Note. If you add any custom values for these fields, complete all the appropriate planning beforehand. There is no built-in mechanism to prevent collisions.

Note. In the My Personalizations interface, end users only see options that posses the following attributes: the User Option Type is set to System *and* the option to override is allowed by way of the users permission list(s).

Using the Format Tab

Access the Format tab.



Format Tab (1 of 2)

User Option Shows the code associated with the option.

Field Format and Field Format Length Defines the field characteristic of the option. Used for the Option Default Value for options that are not validated against the database.

Record (Table) Name Specify the lookup table that holds the personalization options values.

Field Name Specify the field on the lookup table containing the valid option values.

Option Default Value Shows the current default for the option. This value is set through the Set Option Default Value.

Set Option Default Value This is a link to the secondary page used to set Option Default Values.

Set Option Default Value

The following items appear on the Set Option Default Value page.

Option Category Level Shows the high-level category to which the option belongs, such as PeopleTools or HCM.

User Option Shows the code associated with the option.

Description Shows the description of the option.

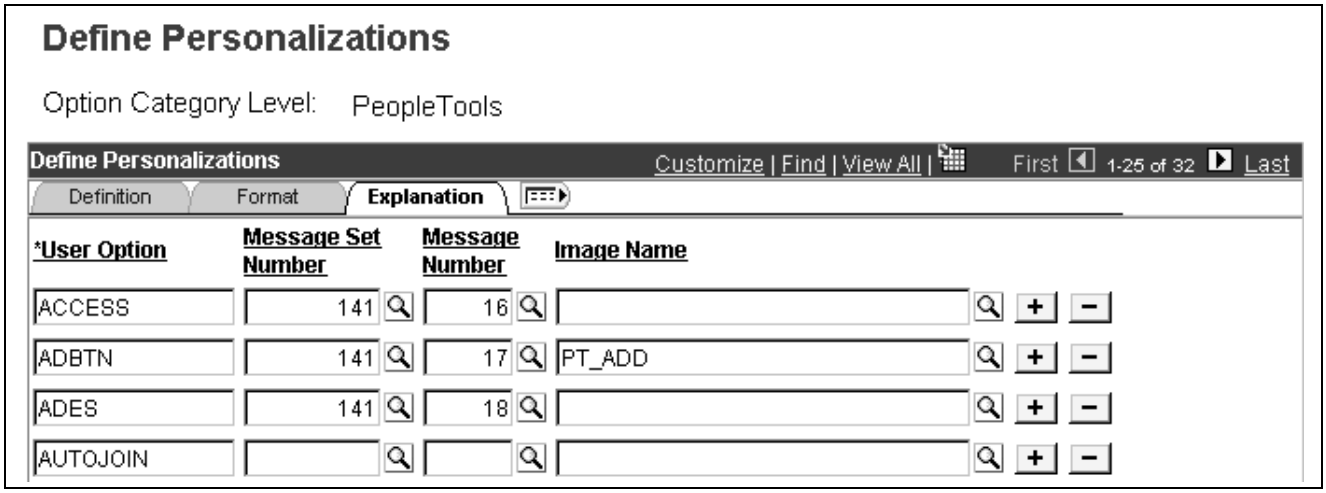
Current Default Value Displays the current default value

Option Default Value Select the appropriate value from the dropdown list, or add the appropriate option manually. Depending on the whether the option gets its default values from a prompt table determines if a dropdown list or an edit box appears. For options that derive default values from a prompt table, the system displays a dropdown list.

Using the Explanation Tab

The Explanation tab enables you to reference the message text and the image (if needed) that the end user sees after clicking the Explain button in the My Personalizations interface.

If you are adding a custom personalization, you'll need to create the message in the message catalog and create the image (if needed).



Explanation Tab

User Option Displays the code associated with an option.

Message Set Number Specify the message set containing the message that contains the explain text.

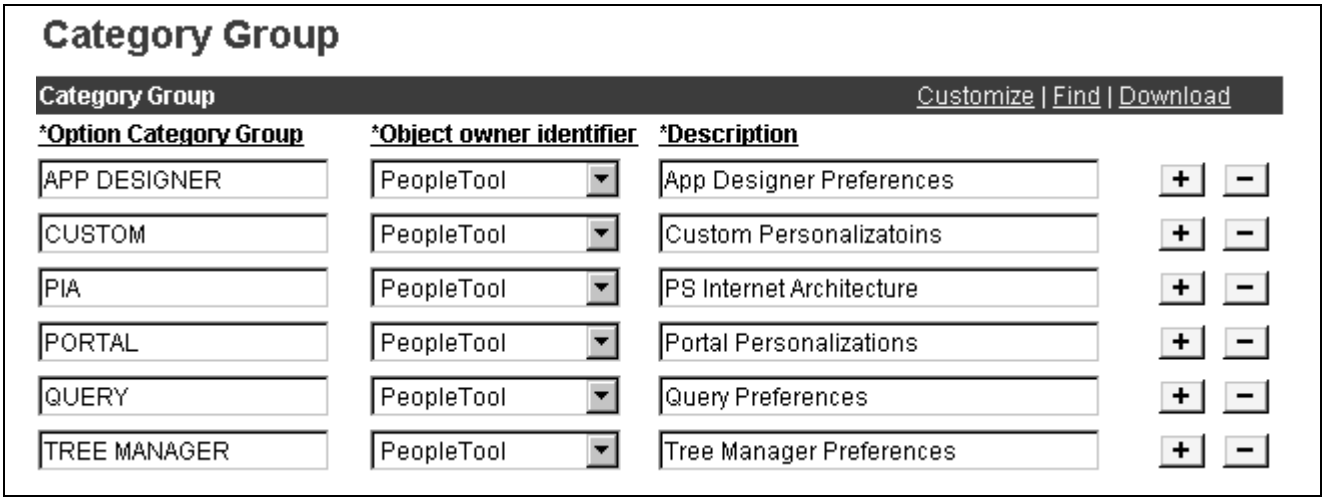
Message Number Specify the message number of the message containing the explain text.

Image Name Points to the image that the system displays to the end user to provide clarification and context for the personalization. For example, for the "Tab over add button" option, the image of the "add" button is included so the user can recognize the object.

Working with Category Groups

Category groups can represent products, such as Query or Tree Manager, or functional groupings. A category group is an attribute that enables you to designate ownership of personalizations for administrative duties, such as maintenance.

Note. All options created within the category level of Custom, by default, appear in the Custom category group.



Category Group Page

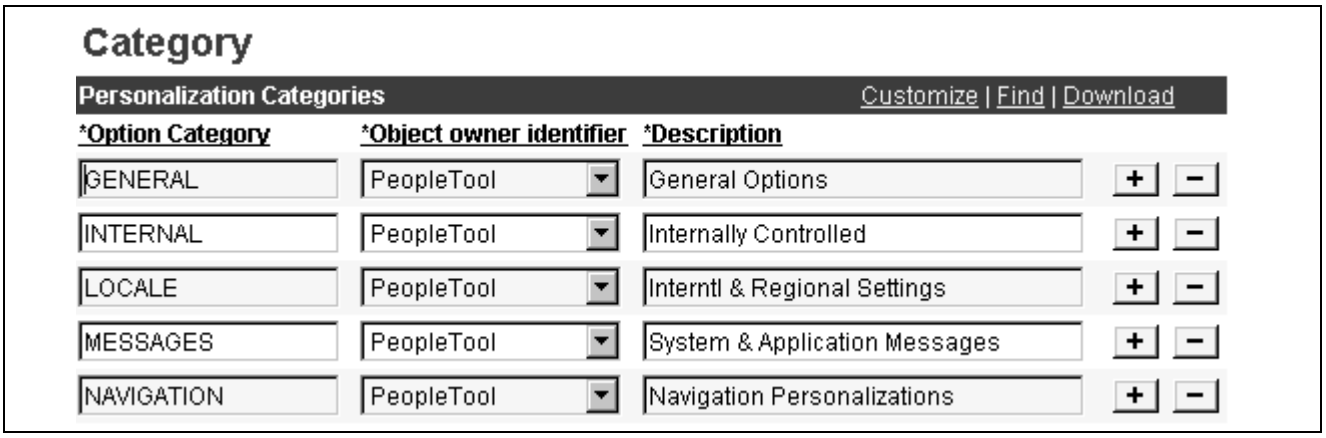
Option Category Group Displays the name of the category group.

Object owner identifier Displays the name of the group responsible for the maintenance of the category group.

Description Provides a description of the category group for identification purposes. If adding a new description, this field has a 30-character limit.

Working with Categories

Categories are the way that you group and present personalization options to your end users. For example, for the Navigation option category the end user sees the description (Navigation Personalizations) on the My Personalizations page. When the end user clicks the adjacent Personalize Options button, they access the options you have grouped in the Navigation category.



Category Page

Option Category Shows the name of the category in which options appear for display on the My Personalizations page.

Object owner identifier Displays the name of the group responsible for the maintenance of the category group.

Description Provides a description of the category for identification purposes. If adding a new description, this field has a 30-character limit.

Important! This is the text that appears on the My Personalization page. If you add custom categories make sure the text is meaningful for end users.

Working with Locale-Based Personalizations

Locale-based personalizations enable you to handle settings for globalization. Locale-based personalizations are treated separately than the other personalizations.

You use the following pages to manage these personalization options:

- Locale Definition.
- Locale Defaults.

The system derives the locale information based on the locale specified in the browser. PeopleSoft delivers these pages populated with the codes that represent the current browser locales.

This topic is discussed in more detail in the Globalization PeopleBook.

See Also

Enterprise PeopleTools 8.45 PeopleBook: Global Technology, "Controlling International Preferences," Setting Up

Adding Personalizations to Permission Lists

You assign personalizations to users by way of permission lists in PeopleTools Security. Before doing so, make sure you have added or modified all the necessary personalizations in the Define Personalizations pages. PeopleTools Security only recognizes personalizations that have been defined in the Define Personalizations interface. This topic is covered in the PeopleTools Security documentation.

See Also

Chapter 3, "Setting Up Permission Lists," Setting Personalization Permissions, page 44

Creating Custom Personalization Options

Creating custom personalization options involve the following steps:

1. Define the option using the Define Personalization interface.

   See Chapter 12, "Managing PeopleSoft Personalizations," Defining Personalization Options, page 210.

2. Implement the behavior using PeopleCode personalization options (discussed in the following section).

See Chapter 12, “Managing PeopleSoft Personalizations,” Working with the My Personalizations Interface, page 217.

3. If users will be able to control the personalization, you need to make the option accessible on the appropriate permission list through PeopleTools Security.

Personalization PeopleCode Functions

There are two PeopleCode functions related to personalizations. These functions are:

- GetUserOption.
- SetUserOption.

If you intend to modify or create custom personalizations, you may need to employ the use of these functions. Refer to the PeopleCode documentation for use and syntax.

See Also

Enterprise PeopleTools 8.45 PeopleBook: PeopleCode API Reference

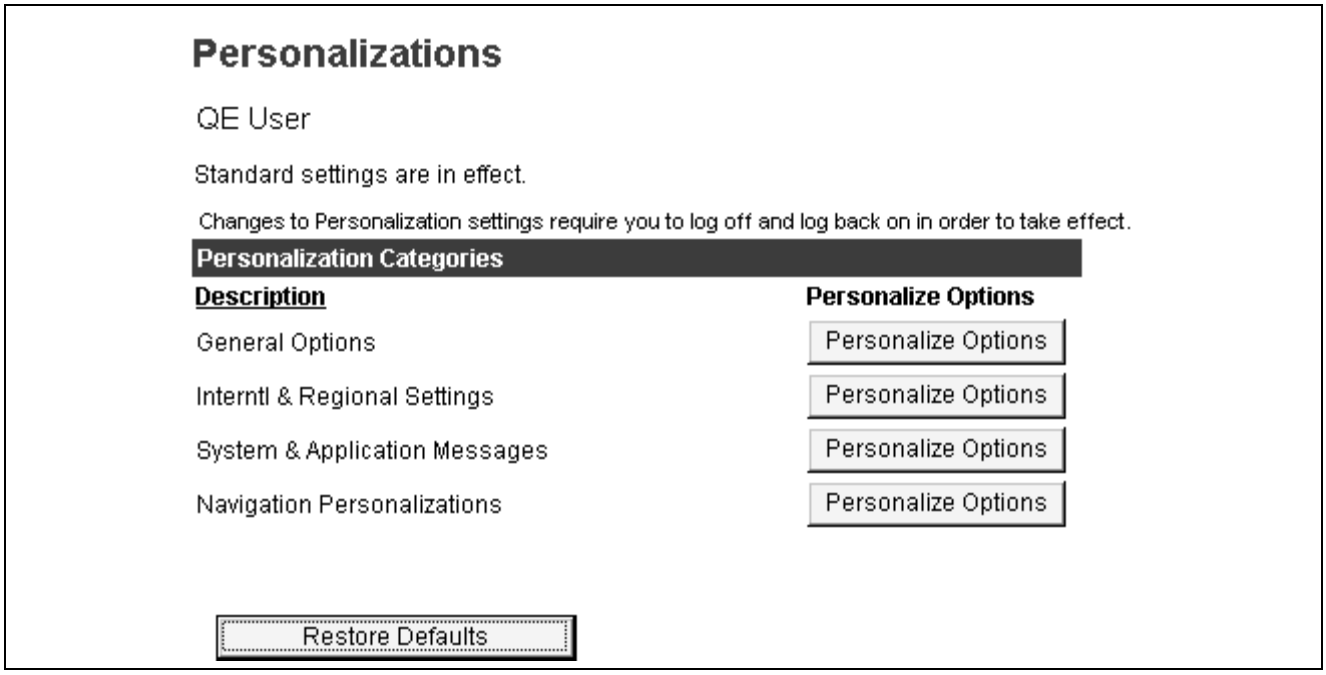
Working with the My Personalizations Interface

This section discusses how to:

- Use the Personalizations page.
- Setting personalize options.
- Use the Personalization Explanation page.
- Modify a personalization option.

Using the Personalizations Page

Access the My Personalizations page.



Personalizations Page

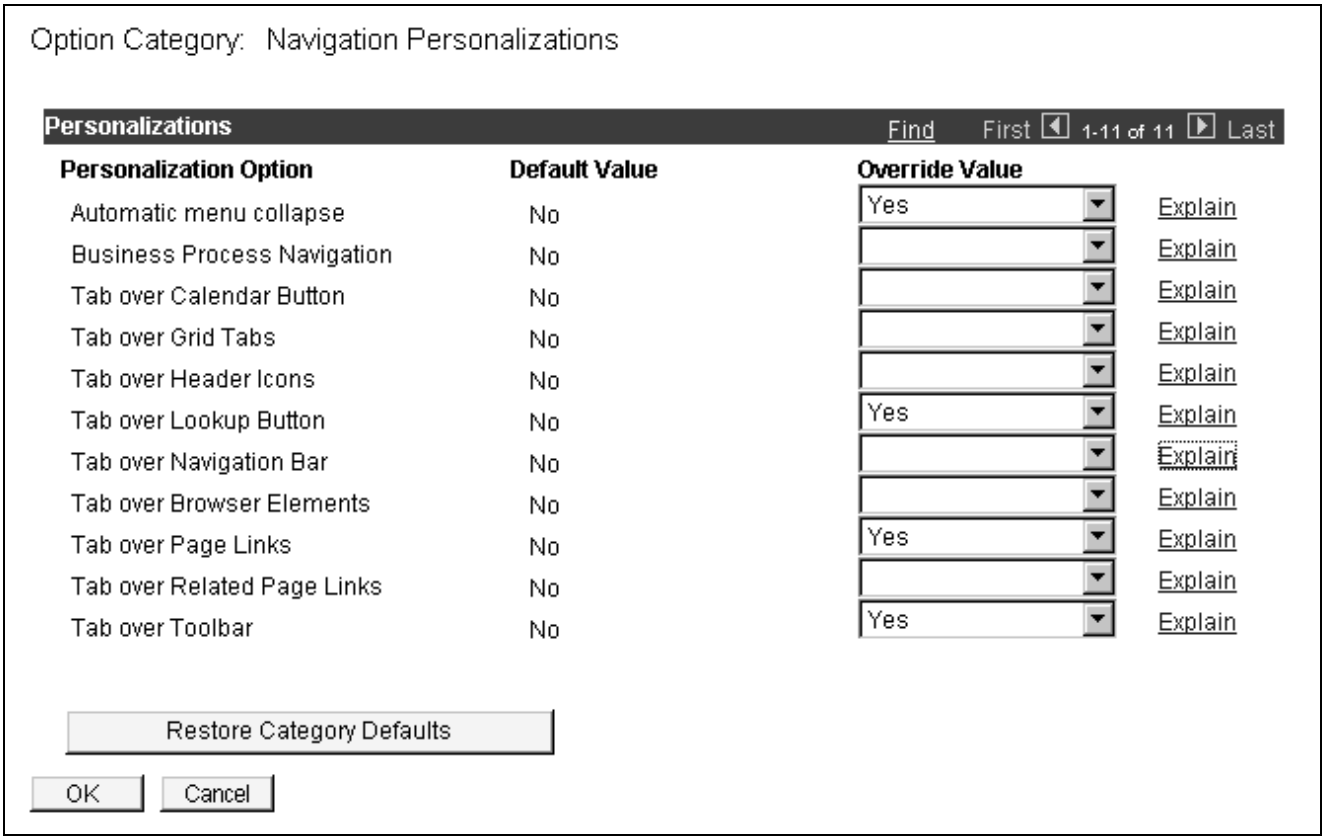
Description The description column contains a brief description for identifying a particular category of personalization options.

Personalize Options To view and modify the options within a category, click this button.

Restore Defaults Click this button to restore the default values for all options in each personalization category. Defaults refer to the initial values that your system administrator has set for each available option—before you modified the option. So, you only use this feature if you have modified one or more personalization option and you want to revert to the initial settings.

Setting Personalize Options

Access the My Personalizations - Personalize Options page.



Personalize Options

Option Category Shows the description of the category of personalizations. This helps you to make sure that you have the correct category open.

Personalization Option This column lists all of the personalization options available for you to modify. The text that appears in the list is a brief description of the option. For more information on the option, click the Explain link.

Default Value Refers to the initial settings that your administrator has specified for the option. If you do not modify the default value, the option assumes the value provided by the system administrator.

Override Value Enter any custom value you want to assign to the personalization option. To "override" a default setting means to "use in place of" the default setting.

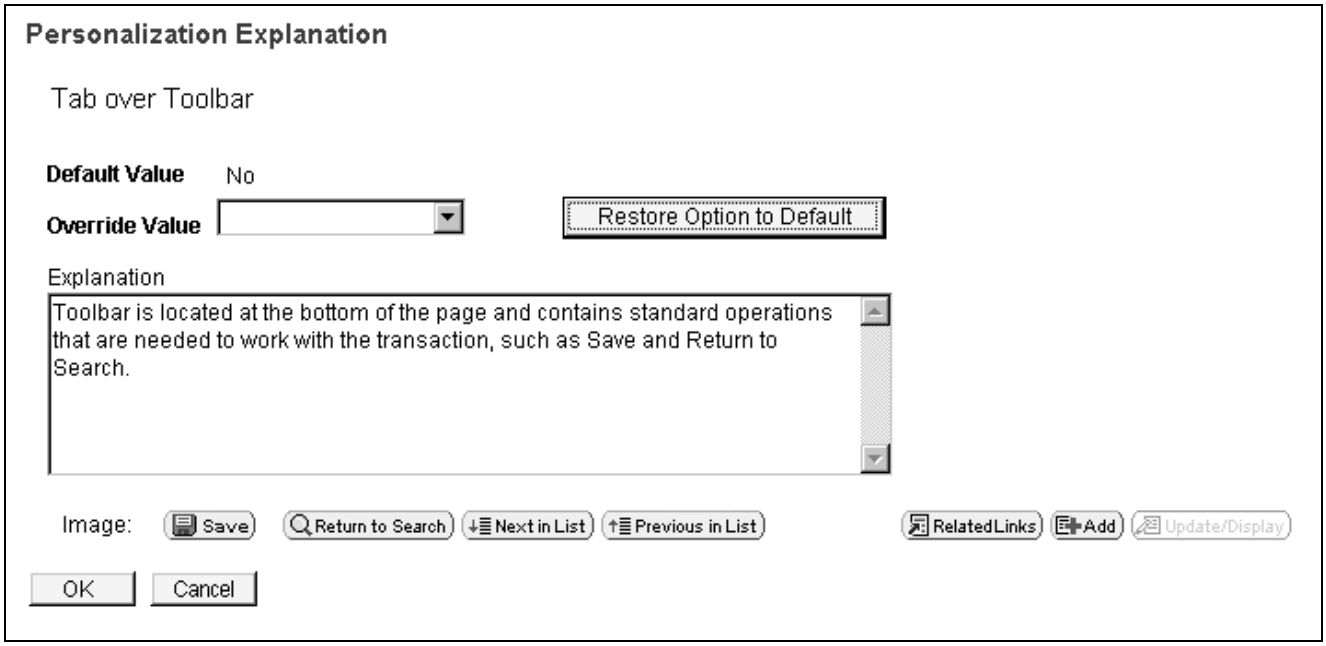
Explain Click this link to view more information on what the personalization option provides. See the following section for more information on the Explanation page.

Restore Category Defaults Returns all modified options to the default values. This button applies only to the current category, as in the category you have open.

OK/Cancel After you have made any modifications, click OK so that the system records your changes. If you do not want your changes recorded click Cancel. If you have not made any changes and just viewed the options, you can use either button to return to the Personalizations page.

Using the Personalization Explanation Page

Access the My Personalizations - Personalization Explanation page.



Personalization Explanation Page

Personalization Name The name of the individual personalization appears at the top of this page so that you can make sure you are viewing or modifying the appropriate option.

Default Value Shows the value that your system administrator has set as the default value for an option. The personalization assumes the default value unless you override it (modify it).

Override Value Overrides (or changes) the default value. For instance, if the default value for an option is No, you can override the default value to be Yes.

Restore Option to Default Enables you to change any option value that you've modified to assume the original default value specified by your system administrator.

Explanation This box contains the description of what the personalization option provides when activated. For longer descriptions, use the scroll bar to view. This box is "read-only", which means you can't add text to it.

Image In many cases, especially with the Navigation options, an image appears to provide further clarification as to a specific control or item that the option affects.

For example, on the explanation page for the Tab Over Toolbar option, an image of the toolbar appears in the image section to show exactly the area on the page that the personalization affects.

OK/Cancel Returns you to the current Option Category page. If you've made changes to the personalization option that you want to keep, click OK. If you do not want to keep the changes you have made, click Cancel. If you have made no changes, user either button.

Modifying a Personalization Option

The following procedure describes the steps you need to complete to modify a personalization option.

To modify a personalization option:

1. Select My Personalizations from the portal menu.
2. On the Personalizations page, click the Personalize Options button adjacent to the category of personalization options you want to modify.
3. In the Personalization Option list, locate the option you want to modify.
4. In the corresponding Override Value edit box specify the appropriate override value.

   Depending on the option, you will see one of the following controls.

   - A drop-down list box. Select the appropriate option from the drop-down list.
   - An edit box. Manually add (type in) the override value.
5. Click OK.

   This saves the change to the system.
6. Sign off and then sign on again so that the system recognizes your changes.

APPENDIX A

ISO Country and Currency Codes

PeopleBooks use International Organization for Standardization (ISO) country and currency codes to identify country-specific information and monetary amounts.

This appendix discusses:

- ISO country codes.
- ISO currency codes.

See Also

"About These PeopleBooks Preface," Typographical Conventions and Visual Cues

ISO Country Codes

This table lists the ISO country codes that may appear as country identifiers in PeopleBooks:

ISO Country Code	Country Name
ABW	Aruba
AFG	Afghanistan
AGO	Angola
AIA	Anguilla
ALB	Albania
AND	Andorra
ANT	Netherlands Antilles
ARE	United Arab Emirates
ARG	Argentina
ARM	Armenia
ASM	American Samoa
ATA	Antarctica

ISO Country Code	Country Name
ATF	French Southern Territories
ATG	Antigua and Barbuda
AUS	Australia
AUT	Austria
AZE	Azerbaijan
BDI	Burundi
BEL	Belgium
BEN	Benin
BFA	Burkina Faso
BGD	Bangladesh
BGR	Bulgaria
BHR	Bahrain
BHS	Bahamas
BIH	Bosnia and Herzegovina
BLR	Belarus
BLZ	Belize
BMU	Bermuda
BOL	Bolivia
BRA	Brazil
BRB	Barbados
BRN	Brunei Darussalam
BTN	Bhutan
BVT	Bouvet Island
BWA	Botswana
CAF	Central African Republic
CAN	Canada
CCK	Cocos (Keeling) Islands

ISO Country Code	Country Name
CHE	Switzerland
CHL	Chile
CHN	China
CIV	Cote D'Ivoire
CMR	Cameroon
COD	Congo, The Democratic Republic
COG	Congo
COK	Cook Islands
COL	Colombia
COM	Comoros
CPV	Cape Verde
CRI	Costa Rica
CUB	Cuba
CXR	Christmas Island
CYM	Cayman Islands
CYP	Cyprus
CZE	Czech Republic
DEU	Germany
DJI	Djibouti
DMA	Dominica
DNK	Denmark
DOM	Dominican Republic
DZA	Algeria
ECU	Ecuador
EGY	Egypt
ERI	Eritrea
ESH	Western Sahara

ISO Country Code	Country Name
ESP	Spain
EST	Estonia
ETH	Ethiopia
FIN	Finland
FJI	Fiji
FLK	Falkland Islands (Malvinas)
FRA	France
FRO	Faroe Islands
FSM	Micronesia, Federated States
GAB	Gabon
GBR	United Kingdom
GEO	Georgia
GHA	Ghana
GIB	Gibraltar
GIN	Guinea
GLP	Guadeloupe
GMB	Gambia
GNB	Guinea-Bissau
GNQ	Equatorial Guinea
GRC	Greece
GRD	Grenada
GRL	Greenland
GTM	Guatemala
GUF	French Guiana
GUM	Guam
GUY	Guyana
GXA	GXA - GP Core Country

ISO Country Code	Country Name
GXB	GXB - GP Core Country
GXC	GXC - GP Core Country
GXD	GXD - GP Core Country
HKG	Hong Kong
HMD	Heard and McDonald Islands
HND	Honduras
HRV	Croatia
HTI	Haiti
HUN	Hungary
IDN	Indonesia
IND	India
IOT	British Indian Ocean Territory
IRL	Ireland
IRN	Iran (Islamic Republic Of)
IRQ	Iraq
ISL	Iceland
ISR	Israel
ITA	Italy
JAM	Jamaica
JOR	Jordan
JPN	Japan
KAZ	Kazakstan
KEN	Kenya
KGZ	Kyrgyzstan
KHM	Cambodia
KIR	Kiribati
KNA	Saint Kitts and Nevis

ISO Country Code	Country Name
KOR	Korea, Republic of
KWT	Kuwait
LAO	Lao People’s Democratic Rep
LBN	Lebanon
LBR	Liberia
LBY	Libyan Arab Jamahiriya
LCA	Saint Lucia
LIE	Liechtenstein
LKA	Sri Lanka
LSO	Lesotho
LTU	Lithuania
LUX	Luxembourg
LVA	Latvia
MAC	Macao
MAR	Morocco
MCO	Monaco
MDA	Moldova, Republic of
MDG	Madagascar
MDV	Maldives
MEX	Mexico
MHL	Marshall Islands
MKD	Fmr Yugoslav Rep of Macedonia
MLI	Mali
MLT	Malta
MMR	Myanmar
MNG	Mongolia
MNP	Northern Mariana Islands

ISO Country Code	Country Name
MOZ	Mozambique
MRT	Mauritania
MSR	Montserrat
MTQ	Martinique
MUS	Mauritius
MWI	Malawi
MYS	Malaysia
MYT	Mayotte
NAM	Namibia
NCL	New Caledonia
NER	Niger
NFK	Norfolk Island
NGA	Nigeria
NIC	Nicaragua
NIU	Niue
NLD	Netherlands
NOR	Norway
NPL	Nepal
NRU	Nauru
NZL	New Zealand
OMN	Oman
PAK	Pakistan
PAN	Panama
PCN	Pitcairn
PER	Peru
PHL	Philippines
PLW	Palau

ISO Country Code	Country Name
PNG	Papua New Guinea
POL	Poland
PRI	Puerto Rico
PRK	Korea, Democratic People’s Rep
PRT	Portugal
PRY	Paraguay
PSE	Palestinian Territory, Occupie
PYF	French Polynesia
QAT	Qatar
REU	Reunion
ROU	Romania
RUS	Russian Federation
RWA	Rwanda
SAU	Saudi Arabia
SDN	Sudan
SEN	Senegal
SGP	Singapore
SGS	Sth Georgia & Sth Sandwich Is
SHN	Saint Helena
SJM	Svalbard and Jan Mayen
SLB	Solomon Islands
SLE	Sierra Leone
SLV	El Salvador
SMR	San Marino
SOM	Somalia
SPM	Saint Pierre and Miquelon
STP	Sao Tome and Principe

ISO Country Code	Country Name
SUR	Suriname
SVK	Slovakia
SVN	Slovenia
SWE	Sweden
SWZ	Swaziland
SYC	Seychelles
SYR	Syrian Arab Republic
TCA	Turks and Caicos Islands
TCD	Chad
TGO	Togo
THA	Thailand
TJK	Tajikistan
TKL	Tokelau
TKM	Turkmenistan
TLS	East Timor
TON	Tonga
TTO	Trinidad and Tobago
TUN	Tunisia
TUR	Turkey
TUV	Tuvalu
TWN	Taiwan, Province of China
TZA	Tanzania, United Republic of
UGA	Uganda
UKR	Ukraine
UMI	US Minor Outlying Islands
URY	Uruguay
USA	United States

ISO Country Code	Country Name
UZB	Uzbekistan
VAT	Holy See (Vatican City State)
VCT	St Vincent and the Grenadines
VEN	Venezuela
VGB	Virgin Islands (British)
VIR	Virgin Islands (U.S.)
VNM	Viet Nam
VUT	Vanuatu
WLF	Wallis and Futuna Islands
WSM	Samoa
YEM	Yemen
YUG	Yugoslavia
ZAF	South Africa
ZMB	Zambia
ZWE	Zimbabwe

ISO Currency Codes

This table lists the ISO country codes that may appear as currency identifiers in PeopleBooks:

ISO Currency Code	Description
ADP	Andorran Peseta
AED	United Arab Emirates Dirham
AFA	Afghani
AFN	Afghani
ALK	Old Lek
ALL	Lek
AMD	Armenian Dram

ISO Currency Code	Description
ANG	Netherlands Antilles Guilder
AOA	Kwanza
AOK	Kwanza
AON	New Kwanza
AOR	Kwanza Reajustado
ARA	Austral
ARP	Peso Argentino
ARS	Argentine Peso
ARY	Peso
ATS	Schilling
AUD	Australian Dollar
AWG	Aruban Guilder
AZM	Azerbaijanian Manat
BAD	Dinar
BAM	Convertible Marks
BBD	Barbados Dollar
BDT	Taka
BEC	Convertible Franc
BEF	Belgian Franc
BEL	Financial Belgian Franc
BGJ	Lev A/52
BGK	Lev A/62
BGL	Lev
BGN	Bulgarian LEV
BHD	Bahraini Dinar
BIF	Burundi Franc
BMD	Bermudian Dollar

ISO Currency Code	Description
BND	Brunei Dollar
BOB	Boliviano
BOP	Peso
BOV	Mvdol
BRB	Cruzeiro
BRC	Cruzado
BRE	Cruzeiro
BRL	Brazilian Real
BRN	New Cruzado
BRR	Brazilian Real Dollar
BSD	Bahamian Dollar
BTN	Ngultrum
BUK	N/A
BWP	Pula
BYB	Belarussian Ruble
BYR	Belarussian Ruble
BZD	Belize Dollar
CAD	Canadian Dollar
CDF	Franc Congolais
CHF	Swiss Franc
CLF	Unidades de fomento
CLP	Chilean Peso
CNX	Peoples Bank Dollar
CNY	Yuan Renminbi
COP	Colombian Peso
CRC	Costa Rican Colon
CSD	Serbia Dinar

ISO Currency Code	Description
CSJ	Krona A/53
CSK	Koruna
CUP	Cuban Peso
CVE	Cape Verde Escudo
CYP	Cyprus Pound
CZK	Czech Koruna
DEM	Deutsche Mark
DJF	Djibouti Franc
DKK	Danish Krone
DOP	Dominican Peso
DZD	Algerian Dinar
ECS	Sucre
ECV	Unidad de Valor
EEK	Kroon
EGP	Egyptian Pound
EQE	Ekwele
ERN	Nakfa
ESA	Spanish Peseta
ESB	Convertible Peseta
ESP	Spanish Peseta
ETB	Ethiopian Birr
EUR	euro
FIM	Markka
FJD	Fiji Dollar
FKP	Falklands Isl. Pound
FRF	French Franc
GBP	Pound Sterling

ISO Currency Code	Description
GEK	Georgian Coupon
GEL	Lari
GHC	Cedi
GIP	Gibraltar Pound
GMD	Dalasi
GNE	Syli
GNF	Guinea Franc
GNS	Syli
GQE	Ekwele
GRD	Drachma
GTQ	Quetzal
GWE	Guinea Escudo
GWP	Guinea-Bissau Peso
GYD	Guyana Dollar
HKD	Hong Kong Dollar
HNL	Lempira
HRD	Dinar
HRK	Kuna
HTG	Gourde
HUF	Forint
IDR	Rupiah
IEP	Irish Pound
ILP	Pound
ILR	Old Shekel
ILS	New Israeli Sheqel
INR	Indian Rupee
IQD	Iraqi Dinar

ISO Currency Code	Description
IRR	Iranian Rial
ISJ	Old Krona
ISK	Iceland Krona
ITL	Italian Lira
JMD	Jamaican Dollar
JOD	Jordanian Dinar
JPY	Yen
KES	Kenyan Shilling
KGS	Som
KHR	Riel
KMF	Comoro Franc
KPW	North Korean Won
KRW	Won
KWD	Kuwaiti Dinar
KYD	Cayman Islands dollar
KZT	Tenge
LAJ	Kip Pot Pol
LAK	Kip
LBP	Lebanese Pound
LKR	Sri Lanka Rupee
LRD	Liberian Dollar
LSL	Loti
LSM	Maloti
LTL	Lithuanian Litas
LTT	Talonas
LUC	Convertib Francl
LUF	Luxembourg Franc

ISO Currency Code	Description
LUL	Financial Franc
LVL	Latvian Lats
LVR	Latvian Ruble
LYD	Libyan Dinar
MAD	Moroccan Dirham
MAF	Mali Franc
MDL	Moldovan Leu
MGF	Malagasy Franc
MKD	Denar
MLF	Mali Franc
MMK	Kyat
MNT	Tugrik
MOP	Pataca
MRO	Ouguiya
MTL	Maltese Lira
MTP	Maltese Pound
MUR	Mauritius Rupee
MVQ	Maldive Rupee
MVR	Rufiyaa
MWK	Malawian Kwacha
MXN	Mexican Peso
MXP	Mexican Peso
MXV	Mexican UDI
MYR	Malaysian Ringgit
MZE	Mozambique Escudo
MZM	Metical
NAD	Namibia Dollar

ISO Currency Code	Description
NGN	Naira
NIC	Cordoba
NIO	Cordoba Oro
NLG	Netherlands Guilder
NOK	Norwegian Krone
NPR	Nepalese Rupee
NZD	New Zealand Dollar
OMR	Rial Omani
PAB	Balboa
PEI	Inti
PEN	Nuevo Sol
PES	Sol
PGK	Kina
PHP	Philippine Peso
PKR	Pakistan Rupee
PLN	Zloty
PLZ	Zloty
PTE	Portuguese Escudo
PYG	Guarani
QAR	Qatari Rial
ROK	Leu A/52
ROL	Leu
RUB	Russian Ruble
RUR	Russian Federation Rouble
RWF	Rwanda Franc
SAR	Saudi Riyal
SBD	Solomon Islands

ISO Currency Code	Description
SCR	Seychelles Rupee
SDD	Sudanese Dinar
SDP	Sudanese Pound
SEK	Swedish Krona
SGD	Singapore Dollar
SHP	St Helena Pound
SIT	Tolar
SKK	Slovak Koruna
SLL	Leone
SOS	Somali Shilling
SRG	Surinam Guilder
STD	Dobra
SUR	Rouble
SVC	El Salvador Colon
SYP	Syrian Pound
SZL	Lilangeni
THB	Baht
TJR	Tajik Ruble
TJS	Somoni
TMM	Manat
TND	Tunisian Dinar
TOP	Pa’anga
TPE	Timor Escudo
TRL	Turkish Lira
TTD	Trinidad Dollar
TWD	New Taiwan Dollar
TZS	Tanzanian Shilling

ISO Currency Code	Description
UAH	Hryvnia
UAK	Karbovanet
UGS	Uganda Shilling
UGW	Old Shilling
UGX	Uganda Shilling
USD	US Dollar
USN	US Dollar (Next day)
USS	US Dollar (Same day)
UYN	Old Uruguay Peso
UYP	Uruguayan Peso
UYU	Peso Uruguayo
UZS	Uzbekistan Sum
VEB	Bolivar
VNC	Old Dong
VND	Dong
VUV	Vatu
WST	Tala
XAF	CFA Franc BEAC
XAG	Silver
XAU	GOLD
XBA	European Composite Unit
XBB	European Monetary Unit
XBC	European Unit of Account 9
XBD	European Unit of Account 17
XCD	East Caribbean Dollar
XDR	SDR
XEU	EU Currency (E.C.U)

ISO Currency Code	Description
XFO	Gold-Franc
XFU	UIC-Franc
XOF	CFA Franc BCEAO
XPD	Palladium
XPF	CFP Franc
XPT	Platinum
XTS	For Testing Purposes
XXX	Non Currency Transaction
YDD	Yemeni Din
YER	Yemeni Rial
YUD	New Yugoslavian Dinar
YUM	New Dinar
YUN	Yugoslavian Dinar
ZAL	Financial Rand
ZAR	Rand
ZMK	Zambian Kwacha
ZRN	New Zaire
ZRZ	Zaire
ZWC	Rhodesian Dollar
ZWD	Zimbabwe Dollar

Glossary of PeopleSoft Terms

absence entitlement This element defines rules for granting paid time off for valid absences, such as sick time, vacation, and maternity leave. An absence entitlement element defines the entitlement amount, frequency, and entitlement period.

absence take This element defines the conditions that must be met before a payee is entitled to take paid time off.

accounting class In PeopleSoft Enterprise Performance Management, the accounting class defines how a resource is treated for generally accepted accounting practices. The Inventory class indicates whether a resource becomes part of a balance sheet account, such as inventory or fixed assets, while the Non-inventory class indicates that the resource is treated as an expense of the period during which it occurs.

accounting date The accounting date indicates when a transaction is recognized, as opposed to the date the transaction actually occurred. The accounting date and transaction date can be the same. The accounting date determines the period in the general ledger to which the transaction is to be posted. You can only select an accounting date that falls within an open period in the ledger to which you are posting. The accounting date for an item is normally the invoice date.

accounting split The accounting split method indicates how expenses are allocated or divided among one or more sets of accounting ChartFields.

accumulator You use an accumulator to store cumulative values of defined items as they are processed. You can accumulate a single value over time or multiple values over time. For example, an accumulator could consist of all voluntary deductions, or all company deductions, enabling you to accumulate amounts. It allows total flexibility for time periods and values accumulated.

action reason The reason an employee's job or employment information is updated. The action reason is entered in two parts: a personnel action, such as a promotion, termination, or change from one pay group to another—and a reason for that action. Action reasons are used by PeopleSoft Human Resources, PeopleSoft Benefits Administration, PeopleSoft Stock Administration, and the COBRA Administration feature of the Base Benefits business process.

action template In PeopleSoft Receivables, outlines a set of escalating actions that the system or user performs based on the period of time that a customer or item has been in an action plan for a specific condition.

activity In PeopleSoft Enterprise Learning Management, an instance of a catalog item (sometimes called a class) that is available for enrollment. The activity defines such things as the costs that are associated with the offering, enrollment limits and deadlines, and waitlisting capacities.

In PeopleSoft Enterprise Performance Management, the work of an organization and the aggregation of actions that are used for activity-based costing.

In PeopleSoft Project Costing, the unit of work that provides a further breakdown of projects—usually into specific tasks.

In PeopleSoft Workflow, a specific transaction that you might need to perform in a business process. Because it consists of the steps that are used to perform a transaction, it is also known as a step map.

agreement In PeopleSoft eSettlements, provides a way to group and specify processing options, such as payment terms, pay from a bank, and notifications by a buyer and supplier location combination.

allocation rule In PeopleSoft Enterprise Incentive Management, an expression within compensation plans that enables the system to assign transactions to nodes and participants. During transaction allocation, the allocation engine traverses the compensation structure from the current node to the root node, checking each node for plans that contain allocation rules.

alternate account A feature in PeopleSoft General Ledger that enables you to create a statutory chart of accounts and enter statutory account transactions at the detail transaction level, as required for recording and reporting by some national governments.

AR specialist Abbreviation for *receivables specialist.* In PeopleSoft Receivables, an individual in who tracks and resolves deductions and disputed items.

arbitration plan In PeopleSoft Enterprise Pricer, defines how price rules are to be applied to the base price when the transaction is priced.

assessment rule In PeopleSoft Receivables, a user-defined rule that the system uses to evaluate the condition of a customer's account or of individual items to determine whether to generate a follow-up action.

asset class An asset group used for reporting purposes. It can be used in conjunction with the asset category to refine asset classification.

attribute/value pair In PeopleSoft Directory Interface, relates the data that makes up an entry in the directory information tree.

authentication server A server that is set up to verify users of the system.

base time period In PeopleSoft Business Planning, the lowest level time period in a calendar.

benchmark job In PeopleSoft Workforce Analytics, a benchmark job is a job code for which there is corresponding salary survey data from published, third-party sources.

book In PeopleSoft Asset Management, used for storing financial and tax information, such as costs, depreciation attributes, and retirement information on assets.

branch A tree node that rolls up to nodes above it in the hierarchy, as defined in PeopleSoft Tree Manager.

budgetary account only An account used by the system only and not by users; this type of account does not accept transactions. You can only budget with this account. Formerly called "system-maintained account."

budget check In commitment control, the processing of source transactions against control budget ledgers, to see if they pass, fail, or pass with a warning.

budget control In commitment control, budget control ensures that commitments and expenditures don't exceed budgets. It enables you to track transactions against corresponding budgets and terminate a document's cycle if the defined budget conditions are not met. For example, you can prevent a purchase order from being dispatched to a vendor if there are insufficient funds in the related budget to support it.

budget period The interval of time (such as 12 months or 4 quarters) into which a period is divided for budgetary and reporting purposes. The ChartField allows maximum flexibility to define operational accounting time periods without restriction to only one calendar.

business event In PeopleSoft Receivables, defines the processing characteristics for the Receivable Update process for a draft activity.

	In PeopleSoft Sales Incentive Management, an original business transaction or activity that may justify the creation of a PeopleSoft Enterprise Incentive Management event (a sale, for example).
business unit	A corporation or a subset of a corporation that is independent with regard to one or more operational or accounting functions.
buyer	In PeopleSoft eSettlements, an organization (or business unit, as opposed to an individual) that transacts with suppliers (vendors) within the system. A buyer creates payments for purchases that are made in the system.
catalog item	In PeopleSoft Enterprise Learning Management, a specific topic that a learner can study and have tracked. For example, “Introduction to Microsoft Word.” A catalog item contains general information about the topic and includes a course code, description, categorization, keywords, and delivery methods. A catalog item can have one or more learning activities.
catalog map	In PeopleSoft Catalog Management, translates values from the catalog source data to the format of the company’s catalog.
catalog partner	In PeopleSoft Catalog Management, shares responsibility with the enterprise catalog manager for maintaining catalog content.
categorization	Associates partner offerings with catalog offerings and groups them into enterprise catalog categories.
channel	In PeopleSoft MultiChannel Framework, email, chat, voice (computer telephone integration [CTI]), or a generic event.
ChartField	A field that stores a chart of accounts, resources, and so on, depending on the PeopleSoft application. ChartField values represent individual account numbers, department codes, and so forth.
ChartField balancing	You can require specific ChartFields to match up (balance) on the debit and the credit side of a transaction.
ChartField combination edit	The process of editing journal lines for valid ChartField combinations based on user-defined rules.
ChartKey	One or more fields that uniquely identify each row in a table. Some tables contain only one field as the key, while others require a combination.
checkbook	In PeopleSoft Promotions Management, enables you to view financial data (such as planned, incurred, and actual amounts) that is related to funds and trade promotions.
Class ChartField	A ChartField value that identifies a unique appropriation budget key when you combine it with a fund, department ID, and program code, as well as a budget period. Formerly called *sub-classification.*
clone	In PeopleCode, to make a unique copy. In contrast, to *copy* may mean making a new reference to an object, so if the underlying object is changed, both the copy and the original change.
collection	To make a set of documents available for searching in Verity, you must first create at least one collection. A collection is set of directories and files that allow search application users to use the Verity search engine to quickly find and display source documents that match search criteria. A collection is a set of statistics and pointers to the source documents, stored in a proprietary format on a file server. Because a collection can only store information for a single location, PeopleSoft maintains a set of collections (one per language code) for each search index object.

collection rule In PeopleSoft Receivables, a user-defined rule that defines actions to take for a customer based on both the amount and the number of days past due for outstanding balances.

compensation object In PeopleSoft Enterprise Incentive Management, a node within a compensation structure. Compensation objects are the building blocks that make up a compensation structure's hierarchical representation.

compensation structure In PeopleSoft Enterprise Incentive Management, a hierarchical relationship of compensation objects that represents the compensation-related relationship between the objects.

condition In PeopleSoft Receivables, occurs when there is a change of status for a customer's account, such as reaching a credit limit or exceeding a user-defined balance due.

configuration parameter catalog Used to configure an external system with PeopleSoft. For example, a configuration parameter catalog might set up configuration and communication parameters for an external server.

configuration plan In PeopleSoft Enterprise Incentive Management, configuration plans hold allocation information for common variables (not incentive rules) and are attached to a node without a participant. Configuration plans are not processed by transactions.

content reference Content references are pointers to content registered in the portal registry. These are typically either URLs or iScripts. Content references fall into three categories: target content, templates, and template pagelets.

context In PeopleCode, determines which buffer fields can be contextually referenced and which is the current row of data on each scroll level when a PeopleCode program is running.

In PeopleSoft Enterprise Incentive Management, a mechanism that is used to determine the scope of a processing run. PeopleSoft Enterprise Incentive Management uses three types of context: plan, period, and run-level.

control table Stores information that controls the processing of an application. This type of processing might be consistent throughout an organization, or it might be used only by portions of the organization for more limited sharing of data.

cost profile A combination of a receipt cost method, a cost flow, and a deplete cost method. A profile is associated with a cost book and determines how items in that book are valued, as well as how the material movement of the item is valued for the book.

cost row A cost transaction and amount for a set of ChartFields.

current learning In PeopleSoft Enterprise Learning Management, a self-service repository for all of a learner's in-progress learning activities and programs.

data acquisition In PeopleSoft Enterprise Incentive Management, the process during which raw business transactions are acquired from external source systems and fed into the operational data store (ODS).

data elements Data elements, at their simplest level, define a subset of data and the rules by which to group them.

For Workforce Analytics, data elements are rules that tell the system what measures to retrieve about your workforce groups.

dataset A data grouping that enables role-based filtering and distribution of data. You can limit the range and quantity of data that is displayed for a user by associating dataset rules with user roles. The result of dataset rules is a set of data that is appropriate for the user's roles.

delivery method In PeopleSoft Enterprise Learning Management, identifies the primary type of delivery method in which a particular learning activity is offered. Also provides default values for the learning activity, such as cost and language. This is primarily used to help learners search the catalog for the type of delivery from which they learn best. Because PeopleSoft Enterprise Learning Management is a blended learning system, it does not enforce the delivery method.

In PeopleSoft Supply Chain Management, identifies the method by which goods are shipped to their destinations (such as truck, air, rail, and so on). The delivery method is specified when creating shipment schedules.

delivery method type In PeopleSoft Enterprise Learning Management, identifies how learning activities can be delivered—for example, through online learning, classroom instruction, seminars, books, and so forth—in an organization. The type determines whether the delivery method includes scheduled components.

directory information tree In PeopleSoft Directory Interface, the representation of a directory's hierarchical structure.

document sequencing A flexible method that sequentially numbers the financial transactions (for example, bills, purchase orders, invoices, and payments) in the system for statutory reporting and for tracking commercial transaction activity.

dynamic detail tree A tree that takes its detail values—dynamic details—directly from a table in the database, rather than from a range of values that are entered by the user.

edit table A table in the database that has its own record definition, such as the Department table. As fields are entered into a PeopleSoft application, they can be validated against an edit table to ensure data integrity throughout the system.

effective date A method of dating information in PeopleSoft applications. You can predate information to add historical data to your system, or postdate information in order to enter it before it actually goes into effect. By using effective dates, you don't delete values; you enter a new value with a current effective date.

EIM ledger Abbreviation for *Enterprise Incentive Management ledger.* In PeopleSoft Enterprise Incentive Management, an object to handle incremental result gathering within the scope of a participant. The ledger captures a result set with all of the appropriate traces to the data origin and to the processing steps of which it is a result.

elimination set In PeopleSoft General Ledger, a related group of intercompany accounts that is processed during consolidations.

entry event In PeopleSoft General Ledger, Receivables, Payables, Purchasing, and Billing, a business process that generates multiple debits and credits resulting from single transactions to produce standard, supplemental accounting entries.

equitization In PeopleSoft General Ledger, a business process that enables parent companies to calculate the net income of subsidiaries on a monthly basis and adjust that amount to increase the investment amount and equity income amount before performing consolidations.

event A predefined point either in the Component Processor flow or in the program flow. As each point is encountered, the event activates each component, triggering any PeopleCode program that is associated with that component and that event. Examples of events are FieldChange, SavePreChange, and RowDelete.

In PeopleSoft Human Resources, also refers to an incident that affects benefits eligibility.

event propagation process In PeopleSoft Sales Incentive Management, a process that determines, through logic, the propagation of an original PeopleSoft Enterprise Incentive Management event and creates a derivative (duplicate) of the original event to be processed by other objects.

	Sales Incentive Management uses this mechanism to implement splits, roll-ups, and so on. Event propagation determines who receives the credit.
exception	In PeopleSoft Receivables, an item that either is a deduction or is in dispute.
exclusive pricing	In PeopleSoft Order Management, a type of arbitration plan that is associated with a price rule. Exclusive pricing is used to price sales order transactions.
fact	In PeopleSoft applications, facts are numeric data values from fields from a source database as well as an analytic application. A fact can be anything you want to measure your business by, for example, revenue, actual, budget data, or sales numbers. A fact is stored on a fact table.
forecast item	A logical entity with a unique set of descriptive demand and forecast data that is used as the basis to forecast demand. You create forecast items for a wide range of uses, but they ultimately represent things that you buy, sell, or use in your organization and for which you require a predictable usage.
fund	In PeopleSoft Promotions Management, a budget that can be used to fund promotional activity. There are four funding methods: top down, fixed accrual, rolling accrual, and zero-based accrual.
generic process type	In PeopleSoft Process Scheduler, process types are identified by a generic process type. For example, the generic process type SQR includes all SQR process types, such as SQR process and SQR report.
group	In PeopleSoft Billing and Receivables, a posting entity that comprises one or more transactions (items, deposits, payments, transfers, matches, or write-offs). In PeopleSoft Human Resources Management and Supply Chain Management, any set of records that are associated under a single name or variable to run calculations in PeopleSoft business processes. In PeopleSoft Time and Labor, for example, employees are placed in groups for time reporting purposes.
incentive object	In PeopleSoft Enterprise Incentive Management, the incentive-related objects that define and support the PeopleSoft Enterprise Incentive Management calculation process and results, such as plan templates, plans, results data, user interaction objects, and so on.
incentive rule	In PeopleSoft Sales Incentive Management, the commands that act on transactions and turn them into compensation. A rule is one part in the process of turning a transaction into compensation.
incur	In PeopleSoft Promotions Management, to become liable for a promotional payment. In other words, you owe that amount to a customer for promotional activities.
item	In PeopleSoft Inventory, a tangible commodity that is stored in a business unit (shipped from a warehouse). In PeopleSoft Demand Planning, Inventory Policy Planning, and Supply Planning, a noninventory item that is designated as being used for planning purposes only. It can represent a family or group of inventory items. It can have a planning bill of material (BOM) or planning routing, and it can exist as a component on a planning BOM. A planning item cannot be specified on a production or engineering BOM or routing, and it cannot be used as a component in a production. The quantity on hand will never be maintained. In PeopleSoft Receivables, an individual receivable. An item can be an invoice, a credit memo, a debit memo, a write-off, or an adjustment.
KPI	An abbreviation for *key performance indicator.* A high-level measurement of how well an organization is doing in achieving critical success factors. This defines the data value or calculation upon which an assessment is determined.

LDIF file Abbreviation for *Lightweight Directory Access Protocol (LDAP) Data Interchange Format file.* Contains discrepancies between PeopleSoft data and directory data.

learner group In PeopleSoft Enterprise Learning Management, a group of learners who are linked to the same learning environment. Members of the learner group can share the same attributes, such as the same department or job code. Learner groups are used to control access to and enrollment in learning activities and programs. They are also used to perform group enrollments and mass enrollments in the back office.

learning components In PeopleSoft Enterprise Learning Management, the foundational building blocks of learning activities. PeopleSoft Enterprise Learning Management supports six basic types of learning components: web-based, session, webcast, test, survey, and assignment. One or more of these learning component types compose a single learning activity.

learning environment In PeopleSoft Enterprise Learning Management, identifies a set of categories and catalog items that can be made available to learner groups. Also defines the default values that are assigned to the learning activities and programs that are created within a particular learning environment. Learning environments provide a way to partition the catalog so that learners see only those items that are relevant to them.

learning history In PeopleSoft Enterprise Learning Management, a self-service repository for all of a learner's completed learning activities and programs.

ledger mapping You use ledger mapping to relate expense data from general ledger accounts to resource objects. Multiple ledger line items can be mapped to one or more resource IDs. You can also use ledger mapping to map dollar amounts (referred to as *rates*) to business units. You can map the amounts in two different ways: an actual amount that represents actual costs of the accounting period, or a budgeted amount that can be used to calculate the capacity rates as well as budgeted model results. In PeopleSoft Enterprise Warehouse, you can map general ledger accounts to the EW Ledger table.

library section In PeopleSoft Enterprise Incentive Management, a section that is defined in a plan (or template) and that is available for other plans to share. Changes to a library section are reflected in all plans that use it.

linked section In PeopleSoft Enterprise Incentive Management, a section that is defined in a plan template but appears in a plan. Changes to linked sections propagate to plans using that section.

linked variable In PeopleSoft Enterprise Incentive Management, a variable that is defined and maintained in a plan template and that also appears in a plan. Changes to linked variables propagate to plans using that variable.

load In PeopleSoft Inventory, identifies a group of goods that are shipped together. Load management is a feature of PeopleSoft Inventory that is used to track the weight, the volume, and the destination of a shipment.

local functionality In PeopleSoft HRMS, the set of information that is available for a specific country. You can access this information when you click the appropriate country flag in the global window, or when you access it by a local country menu.

location Locations enable you to indicate the different types of addresses—for a company, for example, one address to receive bills, another for shipping, a third for postal deliveries, and a separate street address. Each address has a different location number. The primary location—indicated by a *1*—is the address you use most often and may be different from the main address.

logistical task In PeopleSoft Services Procurement, an administrative task that is related to hiring a service provider. Logistical tasks are linked to the service type on the work order so that different types of services can have different logistical tasks. Logistical tasks include both preapproval tasks (such as assigning a new badge or ordering a new

	laptop) and postapproval tasks (such as scheduling orientation or setting up the service provider email). The logistical tasks can be mandatory or optional. Mandatory preapproval tasks must be completed before the work order is approved. Mandatory postapproval tasks, on the other hand, must be completed before a work order is released to a service provider.
market template	In PeopleSoft Enterprise Incentive Management, additional functionality that is specific to a given market or industry and is built on top of a product category.
match group	In PeopleSoft Receivables, a group of receivables items and matching offset items. The system creates match groups by using user-defined matching criteria for selected field values.
MCF server	Abbreviation for *PeopleSoft MultiChannel Framework server.* Comprises the universal queue server and the MCF log server. Both processes are started when *MCF Servers* is selected in an application server domain configuration.
merchandising activity	In PeopleSoft Promotions Management, a specific discount type that is associated with a trade promotion (such as off-invoice, billback or rebate, or lump-sum payment) that defines the performance that is required to receive the discount. In the industry, you may know this as an offer, a discount, a merchandising event, an event, or a tactic.
meta-SQL	Meta-SQL constructs expand into platform-specific Structured Query Language (SQL) substrings. They are used in functions that pass SQL strings, such as in SQL objects, the SQLExec function, and PeopleSoft Application Engine programs.
metastring	Metastrings are special expressions included in SQL string literals. The metastrings, prefixed with a percent (%) symbol, are included directly in the string literals. They expand at run time into an appropriate substring for the current database platform.
multibook	In PeopleSoft General Ledger, multiple ledgers having multiple-base currencies that are defined for a business unit, with the option to post a single transaction to all base currencies (all ledgers) or to only one of those base currencies (ledgers).
multicurrency	The ability to process transactions in a currency other than the business unit's base currency.
national allowance	In PeopleSoft Promotions Management, a promotion at the corporate level that is funded by nondiscretionary dollars. In the industry, you may know this as a national promotion, a corporate promotion, or a corporate discount.
node-oriented tree	A tree that is based on a detail structure, but the detail values are not used.
pagelet	Each block of content on the home page is called a pagelet. These pagelets display summary information within a small rectangular area on the page. The pagelet provide users with a snapshot of their most relevant PeopleSoft and non-PeopleSoft content.
participant	In PeopleSoft Enterprise Incentive Management, participants are recipients of the incentive compensation calculation process.
participant object	Each participant object may be related to one or more compensation objects. See also *compensation object.*
partner	A company that supplies products or services that are resold or purchased by the enterprise.
pay cycle	In PeopleSoft Payables, a set of rules that define the criteria by which it should select scheduled payments for payment creation.
pending item	In PeopleSoft Receivables, an individual receivable (such as an invoice, a credit memo, or a write-off) that has been entered in or created by the system, but hasn't been posted.

PeopleCode PeopleCode is a proprietary language, executed by the PeopleSoft application processor. PeopleCode generates results based upon existing data or user actions. By using business interlink objects, external services are available to all PeopleSoft applications wherever PeopleCode can be executed.

PeopleCode event An action that a user takes upon an object, usually a record field, that is referenced within a PeopleSoft page.

PeopleSoft Internet Architecture The fundamental architecture on which PeopleSoft 8 applications are constructed, consisting of a relational database management system (RDBMS), an application server, a web server, and a browser.

performance measurement In PeopleSoft Enterprise Incentive Management, a variable used to store data (similar to an aggregator, but without a predefined formula) within the scope of an incentive plan. Performance measures are associated with a plan calendar, territory, and participant. Performance measurements are used for quota calculation and reporting.

period context In PeopleSoft Enterprise Incentive Management, because a participant typically uses the same compensation plan for multiple periods, the period context associates a plan context with a specific calendar period and fiscal year. The period context references the associated plan context, thus forming a chain. Each plan context has a corresponding set of period contexts.

plan In PeopleSoft Sales Incentive Management, a collection of allocation rules, variables, steps, sections, and incentive rules that instruct the PeopleSoft Enterprise Incentive Management engine in how to process transactions.

plan context In PeopleSoft Enterprise Incentive Management, correlates a participant with the compensation plan and node to which the participant is assigned, enabling the PeopleSoft Enterprise Incentive Management system to find anything that is associated with the node and that is required to perform compensation processing. Each participant, node, and plan combination represents a unique plan context—if three participants are on a compensation structure, each has a different plan context. Configuration plans are identified by plan contexts and are associated with the participants that refer to them.

plan template In PeopleSoft Enterprise Incentive Management, the base from which a plan is created. A plan template contains common sections and variables that are inherited by all plans that are created from the template. A template may contain steps and sections that are not visible in the plan definition.

planned learning In PeopleSoft Enterprise Learning Management, a self-service repository for all of a learner's planned learning activities and programs.

planning instance In PeopleSoft Supply Planning, a set of data (business units, items, supplies, and demands) constituting the inputs and outputs of a supply plan.

portal registry In PeopleSoft applications, the portal registry is a tree-like structure in which content references are organized, classified, and registered. It is a central repository that defines both the structure and content of a portal through a hierarchical, tree-like structure of folders useful for organizing and securing content references.

price list In PeopleSoft Enterprise Pricer, enables you to select products and conditions for which the price list applies to a transaction. During a transaction, the system either determines the product price based on the predefined search hierarchy for the transaction or uses the product's lowest price on any associated, active price lists. This price is used as the basis for any further discounts and surcharges.

price rule In PeopleSoft Enterprise Pricer, defines the conditions that must be met for adjustments to be applied to the base price. Multiple rules can apply when conditions of each rule are met.

price rule condition In PeopleSoft Enterprise Pricer, selects the price-by fields, the values for the price-by fields, and the operator that determines how the price-by fields are related to the transaction.

price rule key In PeopleSoft Enterprise Pricer, defines the fields that are available to define price rule conditions (which are used to match a transaction) on the price rule.

process category In PeopleSoft Process Scheduler, processes that are grouped for server load balancing and prioritization.

process group In PeopleSoft Financials, a group of application processes (performed in a defined order) that users can initiate in real time, directly from a transaction entry page.

process definition Process definitions define each run request.

process instance A unique number that identifies each process request. This value is automatically incremented and assigned to each requested process when the process is submitted to run.

process job You can link process definitions into a job request and process each request serially or in parallel. You can also initiate subsequent processes based on the return code from each prior request.

process request A single run request, such as a Structured Query Report (SQR), a COBOL or Application Engine program, or a Crystal report that you run through PeopleSoft Process Scheduler.

process run control A PeopleTools variable used to retain PeopleSoft Process Scheduler values needed at runtime for all requests that reference a run control ID. Do not confuse these with application run controls, which may be defined with the same run control ID, but only contain information specific to a given application process request.

product category In PeopleSoft Enterprise Incentive Management, indicates an application in the Enterprise Incentive Management suite of products. Each transaction in the PeopleSoft Enterprise Incentive Management system is associated with a product category.

programs In PeopleSoft Enterprise Learning Management, a high-level grouping that guides the learner along a specific learning path through sections of catalog items. PeopleSoft Enterprise Learning Systems provides two types of programs—curricula and certifications.

progress log In PeopleSoft Services Procurement, tracks deliverable-based projects. This is similar to the time sheet in function and process. The service provider contact uses the progress log to record and submit progress on deliverables. The progress can be logged by the activity that is performed, by the percentage of work that is completed, or by the completion of milestone activities that are defined for the project.

project transaction In PeopleSoft Project Costing, an individual transaction line that represents a cost, time, budget, or other transaction row.

promotion In PeopleSoft Promotions Management, a trade promotion, which is typically funded from trade dollars and used by consumer products manufacturers to increase sales volume.

publishing In PeopleSoft Enterprise Incentive Management, a stage in processing that makes incentive-related results available to participants.

record group A set of logically and functionally related control tables and views. Record groups help enable TableSet sharing, which eliminates redundant data entry. Record groups ensure that TableSet sharing is applied consistently across all related tables and views.

record input VAT flag Abbreviation for *record input value-added tax flag*. Within PeopleSoft Purchasing, Payables, and General Ledger, this flag indicates that you are recording input VAT

	on the transaction. This flag, in conjunction with the record output VAT flag, is used to determine the accounting entries created for a transaction and to determine how a transaction is reported on the VAT return. For all cases within Purchasing and Payables where VAT information is tracked on a transaction, this flag is set to Yes. This flag is not used in PeopleSoft Order Management, Billing, or Receivables, where it is assumed that you are always recording only output VAT, or in PeopleSoft Expenses, where it is assumed that you are always recording only input VAT.
record output VAT flag	Abbreviation for *record output value-added tax flag*. See *record input VAT flag*.
reference data	In PeopleSoft Sales Incentive Management, system objects that represent the sales organization, such as territories, participants, products, customers, channels, and so on.
reference object	In PeopleSoft Enterprise Incentive Management, this dimension-type object further defines the business. Reference objects can have their own hierarchy (for example, product tree, customer tree, industry tree, and geography tree).
reference transaction	In commitment control, a reference transaction is a source transaction that is referenced by a higher-level (and usually later) source transaction, in order to automatically reverse all or part of the referenced transaction's budget-checked amount. This avoids duplicate postings during the sequential entry of the transaction at different commitment levels. For example, the amount of an encumbrance transaction (such as a purchase order) will, when checked and recorded against a budget, cause the system to concurrently reference and relieve all or part of the amount of a corresponding pre-encumbrance transaction, such as a purchase requisition.
regional sourcing	In PeopleSoft Purchasing, provides the infrastructure to maintain, display, and select an appropriate vendor and vendor pricing structure that is based on a regional sourcing model where the multiple ship to locations are grouped. Sourcing may occur at a level higher than the ship to location.
relationship object	In PeopleSoft Enterprise Incentive Management, these objects further define a compensation structure to resolve transactions by establishing associations between compensation objects and business objects.
remote data source data	Data that is extracted from a separate database and migrated into the local database.
REN server	Abbreviation for *real-time event notification server* in PeopleSoft MultiChannel Framework.
requester	In PeopleSoft eSettlements, an individual who requests goods or services and whose ID appears on the various procurement pages that reference purchase orders.
role	Describes how people fit into PeopleSoft Workflow. A role is a class of users who perform the same type of work, such as clerks or managers. Your business rules typically specify what user role needs to do an activity.
role user	A PeopleSoft Workflow user. A person's role user ID serves much the same purpose as a user ID does in other parts of the system. PeopleSoft Workflow uses role user IDs to determine how to route worklist items to users (through an email address, for example) and to track the roles that users play in the workflow. Role users do not need PeopleSoft user IDs.
roll up	In a tree, to roll up is to total sums based on the information hierarchy.
run control	A run control is a type of online page that is used to begin a process, such as the batch processing of a payroll run. Run control pages generally start a program that manipulates data.
run control ID	A unique ID to associate each user with his or her own run control table entries.

run-level context In PeopleSoft Enterprise Incentive Management, associates a particular run (and batch ID) with a period context and plan context. Every plan context that participates in a run has a separate run-level context. Because a run cannot span periods, only one run-level context is associated with each plan context.

search query You use this set of objects to pass a query string and operators to the search engine. The search index returns a set of matching results with keys to the source documents.

section In PeopleSoft Enterprise Incentive Management, a collection of incentive rules that operate on transactions of a specific type. Sections enable plans to be segmented to process logical events in different sections.

security event In commitment control, security events trigger security authorization checking, such as budget entries, transfers, and adjustments; exception overrides and notifications; and inquiries.

serial genealogy In PeopleSoft Manufacturing, the ability to track the composition of a specific, serial-controlled item.

serial in production In PeopleSoft Manufacturing, enables the tracing of serial information for manufactured items. This is maintained in the Item Master record.

session In PeopleSoft Enterprise Learning Management, a single meeting day of an activity (that is, the period of time between start and finish times within a day). The session stores the specific date, location, meeting time, and instructor. Sessions are used for scheduled training.

session template In PeopleSoft Enterprise Learning Management, enables you to set up common activity characteristics that may be reused while scheduling a PeopleSoft Enterprise Learning Management activity—characteristics such as days of the week, start and end times, facility and room assignments, instructors, and equipment. A session pattern template can be attached to an activity that is being scheduled. Attaching a template to an activity causes all of the default template information to populate the activity session pattern.

setup relationship In PeopleSoft Enterprise Incentive Management, a relationship object type that associates a configuration plan with any structure node.

share driver expression In PeopleSoft Business Planning, a named planning method similar to a driver expression, but which you can set up globally for shared use within a single planning application or to be shared between multiple planning applications through PeopleSoft Enterprise Warehouse.

single signon With single signon, users can, after being authenticated by a PeopleSoft application server, access a second PeopleSoft application server without entering a user ID or password.

source transaction In commitment control, any transaction generated in a PeopleSoft or third-party application that is integrated with commitment control and which can be checked against commitment control budgets. For example, a pre-encumbrance, encumbrance, expenditure, recognized revenue, or collected revenue transaction.

SpeedChart A user-defined shorthand key that designates several ChartKeys to be used for voucher entry. Percentages can optionally be related to each ChartKey in a SpeedChart definition.

SpeedType A code representing a combination of ChartField values. SpeedTypes simplify the entry of ChartFields commonly used together.

staging A method of consolidating selected partner offerings with the offerings from the enterprise’s other partners.

statutory account Account required by a regulatory authority for recording and reporting financial results. In PeopleSoft, this is equivalent to the Alternate Account (ALTACCT) ChartField.

step In PeopleSoft Sales Incentive Management, a collection of sections in a plan. Each step corresponds to a step in the job run.

storage level In PeopleSoft Inventory, identifies the level of a material storage location. Material storage locations are made up of a business unit, a storage area, and a storage level. You can set up to four storage levels.

subcustomer qualifier A value that groups customers into a division for which you can generate detailed history, aging, events, and profiles.

Summary ChartField You use summary ChartFields to create summary ledgers that roll up detail amounts based on specific detail values or on selected tree nodes. When detail values are summarized using tree nodes, summary ChartFields must be used in the summary ledger data record to accommodate the maximum length of a node name (20 characters).

summary ledger An accounting feature used primarily in allocations, inquiries, and PS/nVision reporting to store combined account balances from detail ledgers. Summary ledgers increase speed and efficiency of reporting by eliminating the need to summarize detail ledger balances each time a report is requested. Instead, detail balances are summarized in a background process according to user-specified criteria and stored on summary ledgers. The summary ledgers are then accessed directly for reporting.

summary time period In PeopleSoft Business Planning, any time period (other than a base time period) that is an aggregate of other time periods, including other summary time periods and base time periods, such as quarter and year total.

summary tree A tree used to roll up accounts for each type of report in summary ledgers. Summary trees enable you to define trees on trees. In a summary tree, the detail values are really nodes on a detail tree or another summary tree (known as the *basis* tree). A summary tree structure specifies the details on which the summary trees are to be built.

syndicate To distribute a production version of the enterprise catalog to partners.

system function In PeopleSoft Receivables, an activity that defines how the system generates accounting entries for the general ledger.

TableSet A means of sharing similar sets of values in control tables, where the actual data values are different but the structure of the tables is the same.

TableSet sharing Shared data that is stored in many tables that are based on the same TableSets. Tables that use TableSet sharing contain the SETID field as an additional key or unique identifier.

target currency The value of the entry currency or currencies converted to a single currency for budget viewing and inquiry purposes.

template A template is HTML code associated with a web page. It defines the layout of the page and also where to get HTML for each part of the page. In PeopleSoft, you use templates to build a page by combining HTML from a number of sources. For a PeopleSoft portal, all templates must be registered in the portal registry, and each content reference must be assigned a template.

territory In PeopleSoft Sales Incentive Management, hierarchical relationships of business objects, including regions, products, customers, industries, and participants.

TimeSpan A relative period, such as year-to-date or current period, that can be used in various PeopleSoft General Ledger functions and reports when a rolling time frame, rather

	than a specific date, is required. TimeSpans can also be used with flexible formulas in PeopleSoft Projects.
trace usage	In PeopleSoft Manufacturing, enables the control of which components will be traced during the manufacturing process. Serial- and lot-controlled components can be traced. This is maintained in the Item Master record.
transaction allocation	In PeopleSoft Enterprise Incentive Management, the process of identifying the owner of a transaction. When a raw transaction from a batch is allocated to a plan context, the transaction is duplicated in the PeopleSoft Enterprise Incentive Management transaction tables.
transaction state	In PeopleSoft Enterprise Incentive Management, a value assigned by an incentive rule to a transaction. Transaction states enable sections to process only transactions that are at a specific stage in system processing. After being successfully processed, transactions may be promoted to the next transaction state and "picked up" by a different section for further processing.
Translate table	A system edit table that stores codes and translate values for the miscellaneous fields in the database that do not warrant individual edit tables of their own.
tree	The graphical hierarchy in PeopleSoft systems that displays the relationship between all accounting units (for example, corporate divisions, projects, reporting groups, account numbers) and determines roll-up hierarchies.
unclaimed transaction	In PeopleSoft Enterprise Incentive Management, a transaction that is not claimed by a node or participant after the allocation process has completed, usually due to missing or incomplete data. Unclaimed transactions may be manually assigned to the appropriate node or participant by a compensation administrator.
universal navigation header	Every PeopleSoft portal includes the universal navigation header, intended to appear at the top of every page as long as the user is signed on to the portal. In addition to providing access to the standard navigation buttons (like Home, Favorites, and signoff) the universal navigation header can also display a welcome message for each user.
user interaction object	In PeopleSoft Sales Incentive Management, used to define the reporting components and reports that a participant can access in his or her context. All Sales Incentive Management user interface objects and reports are registered as user interaction objects. User interaction objects can be linked to a compensation structure node through a compensation relationship object (individually or as groups).
variable	In PeopleSoft Sales Incentive Management, the intermediate results of calculations. Variables hold the calculation results and are then inputs to other calculations. Variables can be plan variables that persist beyond the run of an engine or local variables that exist only during the processing of a section.
VAT exception	Abbreviation for *value-added tax exception.* A temporary or permanent exemption from paying VAT that is granted to an organization. This terms refers to both VAT exoneration and VAT suspension.
VAT exempt	Abbreviation for *value-added tax exempt.* Describes goods and services that are not subject to VAT. Organizations that supply exempt goods or services are unable to recover the related input VAT. This is also referred to as exempt without recovery.
VAT exoneration	Abbreviation for *value-added tax exoneration.* An organization that has been granted a permanent exemption from paying VAT due to the nature of that organization.
VAT suspension	Abbreviation for *value-added tax suspension.* An organization that has been granted a temporary exemption from paying VAT.
warehouse	A PeopleSoft data warehouse that consists of predefined ETL maps, data warehouse tools, and DataMart definitions.

work order In PeopleSoft Services Procurement, enables an enterprise to create resource-based and deliverable-based transactions that specify the basic terms and conditions for hiring a specific service provider. When a service provider is hired, the service provider logs time or progress against the work order.

worksheet A way of presenting data through a PeopleSoft Business Analysis Modeler interface that enables users to do in-depth analysis using pivoting tables, charts, notes, and history information.

worklist The automated to-do list that PeopleSoft Workflow creates. From the worklist, you can directly access the pages you need to perform the next action, and then return to the worklist for another item.

XML schema An XML definition that standardizes the representation of application messages, component interfaces, or business interlinks.

yield by operation In PeopleSoft Manufacturing, the ability to plan the loss of a manufactured item on an operation-by-operation basis.

zero-rated VAT Abbreviation for *zero-rated value-added tax.* A VAT transaction with a VAT code that has a tax percent of zero. Used to track taxable VAT activity where no actual VAT amount is charged. Organizations that supply zero-rated goods and services can still recover the related input VAT. This is also referred to as exempt with recovery.

Index

A

B

C

D

E

F

M

N

O

P

Q

R

S

T

U