

---

# Enterprise PeopleTools 8.50 PeopleBook: Security Administration

---

**September 2009**

Copyright © 1988, 2009, Oracle and/or its affiliates. All rights reserved.

## **Trademark Notice**

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

## **License Restrictions Warranty/Consequential Damages Disclaimer**

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

## **Warranty Disclaimer**

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

## **Restricted Rights Notice**

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

### *U.S. GOVERNMENT RIGHTS*

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

## **Hazardous Applications Notice**

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

## **Third Party Content, Products, and Services Disclaimer**

This software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products or services.

# Contents

## Preface

<b>Security Administration Preface .....</b>	<b>xiii</b>
Security Administration .....	xiii

## Chapter 1

<b>Getting Started with Security Administration .....</b>	<b>1</b>
Security Administration Overview .....	1
User Security .....	1
LDAP .....	2
Authentication and Single Signon .....	2
Data Encryption .....	3
Query and Definition Security .....	4
PeopleSoft Personalizations .....	4
Security Administration Integration Points .....	4
Component Interfaces .....	4
Service Operations .....	5
Application Engine Programs .....	7
Security Administration Implementation .....	8
Preparing to Use PeopleSoft Security .....	8
Administering Security from Applications .....	8
Reviewing and Monitoring Your Security Implementation .....	10

## Chapter 2

<b>Understanding PeopleSoft Security .....</b>	<b>11</b>
Security Basics .....	11
PeopleSoft Online Security .....	13
Sign-in and Time-out Security .....	13
Page and Dialog Box Security .....	14
Batch Environment Security .....	14
Definition Security .....	15
Application Data Security .....	15
PeopleSoft Internet Architecture Security .....	16
PeopleSoft Authorization IDs .....	17

User IDs .....	18
Connect ID .....	18
Access IDs .....	18
Symbolic IDs .....	19
Administrator Access .....	19
PeopleSoft Sign-in .....	20
PeopleSoft Sign-in .....	20
Directory Server Integration .....	21
Authentication and Signon PeopleCode .....	21
Single Signon .....	22
Implementation Options .....	22
Authentication .....	22
Role Assignments .....	23
Cross-System Synchronization .....	24

### Chapter 3

<b>Setting Up Permission Lists .....</b>	<b>25</b>
Understanding Permission Lists .....	25
Managing Permission Lists .....	26
Creating New Permission Lists .....	27
Copying Permission Lists .....	27
Deleting Permission Lists .....	27
Viewing Related Content References .....	28
Defining Permissions .....	29
Pages Used to Define Permission Lists .....	29
Setting General Permissions .....	30
Setting Page Permissions .....	33
Setting PeopleTools Permissions .....	39
Setting Process Permissions .....	47
Setting Sign-on Time Permissions .....	52
Setting Component Interface Permissions .....	53
Setting Web Library Permissions .....	55
Setting Web Services Permissions .....	57
Setting Personalization Permissions .....	59
Setting Query Permissions .....	60
Setting Mass Change Permissions .....	65
Displaying Additional Links .....	65
Viewing When a Permission List Was Last Updated .....	66
Running Permission List Queries .....	67

## Chapter 4

<b>Setting Up Roles .....</b>	<b>69</b>
Understanding Roles .....	69
Managing Roles .....	70
Copying Roles .....	70
Deleting Roles .....	70
Removing Users From Roles .....	70
Defining Role Options .....	71
Pages Used to Define Role Options .....	71
Assigning Permissions to Roles .....	72
Displaying Static Role Members .....	73
Displaying Dynamic Role Members .....	73
Setting User Routing Options .....	79
Decentralizing Role Administration .....	80
Displaying Additional Links .....	80
Running Role Queries .....	81
Viewing When a Role Was Last Updated .....	83
Creating a NEWUSER Role .....	83
Using the PeopleSoft Administrator Role .....	84

## Chapter 5

<b>Administering User Profiles .....</b>	<b>85</b>
Understanding User Profiles .....	85
Setting Up Access Profiles .....	86
Understanding Access Profiles .....	86
Using the Access Profiles Dialog Box .....	86
Setting Access Profile Properties .....	87
Working with Access Profiles .....	88
Setting Up User Profile Types .....	89
Understanding User Profile Types .....	89
Page Used to Set Up User Profile Types .....	90
Defining User Profile Types .....	91
Working With User Profiles .....	92
Creating a New User Profile .....	92
Copying a User Profile .....	93
Deleting a User Profile .....	93
Bypassing Tables During the Delete User Profile Process .....	94
Specifying User Profile Attributes .....	94
Pages Used to Specify User Profile Attributes .....	95

Setting General User Profile Attributes .....	95
Setting ID Type and Attribute Value .....	99
Setting Roles .....	100
Specifying Workflow Settings .....	101
Viewing When a User Profile Was Last Updated .....	103
Displaying Additional Links .....	104
Running User ID Queries .....	105
Working With Passwords .....	106
Setting Password Controls .....	106
Changing Passwords .....	109
Creating Email Text for Forgotten Passwords .....	110
Creating Hints for Forgotten Passwords .....	111
Deleting Hints for Forgotten Passwords .....	112
Setting Up the Site for Forgotten Passwords .....	112
Requesting New Passwords .....	112
Implementing Distributed User Profiles .....	113
Understanding Distributed User Profiles .....	114
Defining User Profile Access for Remote Security Administrators .....	114
Defining Remote Security Administrator Role Grant Capability .....	115
Administering Distributed User Profiles .....	116
Transferring Users Between Databases .....	117
Tracking User Sign-in and Sign-out Activity .....	118
Purging Inactive User Profiles .....	119
Preserving Historical User Profile Data .....	120

## Chapter 6

<b>Working with User Profiles Across Multiple PeopleSoft Databases .....</b>	<b>123</b>
Understanding User Profile Synchronization .....	123
Implementing Standard User Profile Synchronization .....	124
Understanding Standard User Profile Synchronization .....	126
Setting Up Standard User Profile Synchronization .....	126
Implementing Configurable User Profile Synchronization .....	127
Understanding Configurable User Profile Synchronization .....	127
Enabling Security PeopleCode Options .....	128
Setting Up Configurable User Profile Synchronization .....	130
Transferring Users Between Databases .....	117

## Chapter 7

<b>Employing LDAP Directory Services .....</b>	<b>135</b>
Understanding the PeopleSoft LDAP Solution .....	135

Configuring the LDAP Directory .....	136
Understanding LDAP Directory Configuration .....	136
Pages Used to Configure the Directory .....	137
Specifying Network Information for LDAP .....	137
Specifying Additional Connect DNs .....	138
Installing Selected PeopleSoft-Specific Schema Extensions .....	139
Testing Connectivity .....	140
Caching the Directory Schema .....	141
Page Used to Cache the Directory Schema .....	141
Creating a Cache of the Directory Schema .....	141
Creating Authentication Maps .....	142
Page Used to Create Authentication Maps .....	143
Defining an Authentication Map .....	143
Using the Search Attribute Field in Authentication Maps .....	145
Creating User Profile Maps .....	146
Understanding User Profile Options .....	146
Pages Used to Create User Profile Maps .....	147
Specifying Mandatory User Properties .....	147
Specifying Optional User Properties .....	149
Associating User IDs and User Profile Maps .....	151
Creating Role Membership Rules .....	151
Understanding Role Membership Rules .....	152
Page Used to Create Role Membership Rules .....	152
Defining Role Membership Rules .....	152
Deleting Directory Configurations .....	155
Page Used to Delete Directory Configurations .....	155
Deleting the Directory Configuration .....	155
Working with the Workflow Address Book .....	156
Enabling Signon PeopleCode for LDAP Authentication .....	158
Using LDAP Over SSL (LDAPS) .....	159
Understanding SSL .....	159
SSL Between PeopleSoft and LDAP .....	160
Viewing SSL for LDAP Transactions Setup Examples .....	161
Setting Up SSL for Oracle Internet Directory (OID) .....	162
Setting up SSL for Active Directory Server .....	163
Setting up SSL for Sunone Directory Server (iPlanet) .....	165
Setting Up SSL in PeopleSoft Applications .....	165

## Chapter 8

<b>Employing Signon PeopleCode and User Exits .....</b>	<b>169</b>
Understanding the Delivered External Authentication Solutions .....	169
WWW_Authentication Considerations .....	171

LDAP_Authentication Considerations .....	172
SSO_Authentication Considerations .....	172
LDAP_ProfileSynch Considerations .....	173
Using Signon PeopleCode .....	173
Understanding Signon PeopleCode .....	173
Understanding Signon PeopleCode Permissions .....	174
Page Used to Develop Signon PeopleCode .....	175
Modifying Signon PeopleCode .....	175
Enabling Signon PeopleCode .....	176
Accessing X.509 Certificates .....	178
Using the Web Server Security Exit .....	178
Understanding the Web Server Security Exit .....	179
Creating a Default User .....	179
Modifying the Web Profile .....	180
Writing a Signon PeopleCode Program .....	181
Signing In Through the Web Server .....	182
Using the Windows Security Exit .....	183
Understanding Windows Security Exits .....	183
Customizing PSUSER.DLL .....	185
Implementing a Customized PSUSER.DLL .....	188

## Chapter 9

<b>Implementing Single Signon .....</b>	<b>189</b>
Understanding Single Signon .....	189
Understanding Single Signon Options .....	189
Understanding the PS_TOKEN Cookie .....	190
Implementing PeopleSoft-Only Single Signon .....	191
Understanding PeopleSoft-Only Single Signon .....	192
Working with the Single Signon Page .....	192
Defining Nodes for Single Signon .....	194
Setting up Certificate Authentication .....	195
Sample Single Signon Transaction .....	197
PeopleSoft-Only Single Signon Configuration Considerations .....	200
PeopleSoft-Only Single Signon Configuration Examples .....	203
Making the PeopleSoft-Only Single Signon Token Secure .....	206
Using the Single Signon API .....	207
Configuring PeopleSoft-Only Single Signoff .....	209
Implementing Oracle Access Manager as the PeopleSoft Single Signon Solution .....	210

## Chapter 10

<b>Working with SSL and Digital Certificates .....</b>	<b>213</b>
Understanding SSL and Digital Certificates .....	213
Understanding SSL .....	213
Understanding Certificate Authorities .....	214
Configuring Digital Certificates .....	214

## Chapter 11

<b>Working with Web Service Security (WS-Security) .....</b>	<b>217</b>
Understanding WS-Security .....	217
Implementing WS-Security for WSRP .....	218
Implementing WS-Security for PeopleSoft Integration Broker .....	219

## Chapter 12

<b>Encrypting Text With PSCipher .....</b>	<b>221</b>
Understanding the Triple Data Encryption Standard (DES) Encryption Implementation .....	221
Using the PSCipher Utility .....	221
Generating a Unique Encryption Key .....	222
Updating the Encryption Key on IBM WebSphere .....	223
Generating the Encryption Key on IBM WebSphere .....	223
Updating the Web Profile .....	223
Updating the Integration Gateway .....	223
Updating WSRP/WSS .....	224
Updating the Encryption Key on Oracle WebLogic .....	225
Generating the Encryption Key on Oracle WebLogic .....	225
Updating the Web Profile .....	225
Updating the Integration Gateway .....	226
Updating WSRP/WSS .....	227
Securing the External Key File .....	227
Setting up Operating System File Security .....	227
Backing Up the Key File .....	227

## Chapter 13

<b>Securing Data with PeopleSoft Encryption Technology .....</b>	<b>229</b>
--	------------

Understanding Data Security .....	229
Privacy Through Encryption .....	230
Integrity Through Hashing .....	231
Authentication Using Digital Signatures .....	231
Understanding PeopleSoft Encryption Technology .....	232
PeopleSoft Encryption Technology Features .....	232
PeopleSoft Encryption Technology Development .....	232
PGP Library Considerations .....	233
Understanding the Supported Algorithms .....	234
Internal Algorithms .....	234
OpenSSL Algorithms .....	235
PGP Algorithms .....	241
Algorithm Chain Considerations .....	244
Cross Platform Algorithm Chain Considerations .....	244
Loading Encryption Libraries .....	244
Defining Algorithm Chains .....	247
Defining Algorithm Keysets .....	249
Defining Encryption Profiles .....	251
Testing Encryption Profiles .....	253
Invoking Encryption Profiles from PeopleCode .....	253
Using PeopleCode Encryption Methods .....	254
Using Application Engine Programs to Encrypt and Decrypt Tables .....	254

## Chapter 14

<b>Implementing Query Security .....</b>	<b>257</b>
Defining Query Profiles .....	257
Building Query Access Group Trees .....	257
Working with Query Trees .....	258
Understanding Query Access Group Trees .....	258
Opening Query Access Group Trees .....	259
Defining the Query Tree .....	260
Viewing and Modifying Definitions .....	261
Defining Row-Level Security and Query Security Records .....	264

## Chapter 15

<b>Implementing Definition Security .....</b>	<b>267</b>
Understanding Definition Security .....	267
Definition Security .....	267
Definition Groups and Permission Lists .....	269
Definition Security Rules .....	270

Working With Definition Groups .....	271
Viewing Definition Groups .....	272
Selecting a View .....	272
Viewing All Definitions .....	273
Viewing Definitions of a Specific Type .....	273
Adding and Removing Definitions .....	273
Adding and Removing Definitions .....	273
Removing Definitions From a Definition Group .....	274
Assigning Definition Groups to Permission Lists .....	274
Enabling Display Only Mode .....	275
Viewing Definition Access by User and Permission List .....	275

## Chapter 16

<b>Managing PeopleSoft Personalizations .....</b>	<b>277</b>
Understanding Personalizations .....	277
Working with Personalization Options .....	278
Understanding Navigation Personalizations .....	278
Understanding Regional Settings .....	281
Understanding General Options .....	284
Understanding System Messages .....	286
Understanding Internally Controlled Options .....	286
Pages Used to Define and Modify Personalizations .....	288
Defining Personalization Options .....	288
Understanding the Search Page .....	289
Using the Definition Tab .....	290
Using the Format Tab .....	291
Using the Explanation Tab .....	292
Working with Category Groups .....	293
Working with Categories .....	294
Working with Locale-Based Personalizations .....	295
Adding Personalizations to Permission Lists .....	296
Creating Custom Personalization Options .....	296
Working with the My Personalizations Interface .....	297
Using the Personalizations Page .....	297
Setting Personalize Options .....	298
Using the Personalization Explanation Page .....	299
Modifying a Personalization Option .....	300
<b>Index .....</b>	<b>301</b>



# Security Administration Preface

This preface provides an overview of the content discussed in the Security Administration PeopleBook and discusses PeopleBooks and the online PeopleSoft library.

---

## Security Administration

This PeopleBook covers a wide range of different tools and techniques for administering security on your PeopleSoft system, including:

- Permission lists.
- Roles
- User profiles.
- Lightweight Directory Access Protocol (LDAP).
- Single signon.
- Secure Socket Layer (SSL) and digital certificates.
- Web Service security.
- PeopleSoft Encryption Technology (PET).
- Query and definition security.
- Personalization features.

---

**Note.** Remember that your application documentation also contains security topics that are more specific to the applications you've purchased.

---

---

## PeopleBooks and the Online PeopleSoft Library

A companion PeopleBook called PeopleBooks and the Online PeopleSoft Library contains general information, including:

- Understanding the PeopleSoft online library and related documentation.
- How to send PeopleSoft documentation comments and suggestions to Oracle.
- How to access hosted PeopleBooks, downloadable HTML PeopleBooks, and downloadable PDF PeopleBooks as well as documentation updates.
- Understanding PeopleBook structure.
- Typographical conventions and visual cues used in PeopleBooks.

- ISO country codes and currency codes.
- PeopleBooks that are common across multiple applications.
- Common elements used in PeopleBooks.
- Navigating the PeopleBooks interface and searching the PeopleSoft online library.
- Displaying and printing screen shots and graphics in PeopleBooks.
- How to manage the PeopleSoft online library including full-text searching and configuring a reverse proxy server.
- Understanding documentation integration and how to integrate customized documentation into the library.
- Glossary of useful PeopleSoft terms that are used in PeopleBooks.

You can find this companion PeopleBook in your PeopleSoft online library.

## Chapter 1

# Getting Started with Security Administration

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

---

## Security Administration Overview

This section discusses:

- User security.
- Lightweight Directory Access Protocol (LDAP).
- Authentication and single signon.
- Data Encryption.
- Query and definition security.
- PeopleSoft personalizations.

## User Security

User security is the core of security administration in PeopleSoft applications. You administer user security 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 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 25](#).

## 2. Define roles.

A *role* is 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 69](#).

## 3. Define user profiles.

A *user profile* is a definition that represents one PeopleSoft user. Each user is 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 85](#).

# LDAP

LDAP is an internet protocol used to access a directory listing. Organizations typically store user profiles in a central repository, or *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 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 7, "Employing LDAP Directory Services," page 135](#).

## 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.

PeopleSoft also supports single signon between PeopleSoft and Oracle applications. A user can signon to either system and freely access the other without having to signon to the second system.

See [Chapter 8, "Employing Signon PeopleCode and User Exits," page 169](#) and [Chapter 9, "Implementing Single Signon," page 189](#).

## Data Encryption

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 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 PET with support for the *OpenSSL* and *PGP* encryption libraries.

To implement PET:

1. Load the algorithms of an encryption library 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.

---

**Note.** Along with the delivered OpenSSL and PGP encryption libraries, a PeopleSoft database may also contain encryption keys for internal use of the PeopleCode Crypt class. These encryption keys do not need to be modified.

---

See [Chapter 13, "Securing Data with PeopleSoft Encryption Technology," page 229](#).

## 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 14, "Implementing Query Security," page 257](#) and [Chapter 15, "Implementing Definition Security," page 267](#).

## 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 16, "Managing PeopleSoft Personalizations," page 277](#).

---

## Security Administration Integration Points

This section identifies the security integration points using:

- Component interfaces.
- Service operations.

## Component Interfaces

This section describes component interfaces that are delivered with PeopleSoft applications that you can use to manage and administer user profiles and roles.

## ***DELETE\_ROLE***

The DELETE\_ROLE component interface is based on the Delete Role (PURGE\_ROLEDEFN) component, and it is used to purge roles. It is keyed by RoleName and has the Get, Find, Save, and Cancel methods. The DELETE\_ROLE service operation calls this component interface.

## ***DELETE\_USER\_PROFILE***

The DELETE\_USER\_PROFILE component interface is based on the Purge Inactive User Profile (PURGE\_USR\_PROFILE) component, and it is used to remove unused User Profiles. It is keyed by User ID and has the Get, Find, Save, and Cancel methods. The DELETE\_USER\_PROFILE service operation and the PURGEOLDUSRS Application Engine program call this component interface.

## ***ROLE\_MAINT***

The ROLE\_MAINT component interface is based on the Roles (ROLEMAINT) component. It is keyed by RoleName and has the Cancel, Create, Find, Get, and Save methods.

## ***USERMAINT\_SELF***

This component interface is based on the My System Profile (USERMAINT\_SELF) component. It allows only the current user to access it.

The USERMAINT\_SELF component interface is used with the following components: Forgot My Password (EMAIL\_PSWD), Change Password (CHANGE\_PASSWORD), and Change Expired Password (EXPIRE\_CHANGE\_PSWD).

## ***USER\_PROFILE***

The USER\_PROFILE component interface is based on the User Profiles (USERMAINT) component. It is keyed by User ID.

The USER\_PROFILE component interface is used in User Profile Save As (USER\_SAVEAS) and with LDAP authentication.

## ***USER\_PROFILE\_SYNC***

The USER\_PROFILE\_SYNC component interface is based on the User Profiles (USERMAINT) component. It is keyed by User ID and has the Cancel, Get, and Save methods.

The USER\_PROFILE\_SYNC component interface is used in User Profile Save As (USER\_SAVEAS) and with LDAP authentication.

## **Service Operations**

This section describes service operations that are delivered with PeopleSoft applications that you can use to manage and administer user profiles and roles.

Keep the following in mind when dealing with these security service operations, except the USER\_PROFILE\_XFR service operation:

- Each service operation has a same-named service definition.
- The service operations are asynchronous one-way.
- A same-named message is defined in each service operation definition.
- At least one handler is defined within each service operation definition, if the node is supposed to consume an inbound service operation.

### ***DELETE\_ROLE***

This service operation is called from the Delete Role component. It is used to delete a role from subscribing databases. The service operation requires that the DELETE\_ROLE component interface be authorized.

### ***DELETE\_USER\_PROFILE***

This service operation is called from the Delete User Profile component. It is used to delete a user profile from subscribing databases. This service operation requires that the DELETE\_USER\_PROFILE component interface be authorized.

### ***ROLESYNCHEXT\_MSG***

This service operation is published when a Dynamic Role rule is run. It is called after the DYNROL\_PUBL application engine program successfully finishes.

---

**Note.** As of release 8.49, the ROLESYNCH\_MSG service operation is deprecated and replaced with ROLESYNCHEXT\_MSG service operation.

---

### ***ROLE\_MAINT***

This service operation publishes new roles and updates existing roles in the Roles component.

### ***USER\_PROFILE***

This service operation publishes user profile messages when adds, updates, and deletes occur through the User Profiles component (USERMAINT), the User Profile Save As component, the My System Profile component (USERMAINT\_SELF), the Distributed User Profile component (USERMAINT\_DIST), the USER\_PROFILE component interface, and the USERMAINT\_SELF component interface.

User Profile messages may also be published when Password is changed through the Change My Password component (CHANGE\_PASSWORD) or Expired Password component (EXPIRE\_CHANGE\_PSWD) by triggering the USERMAINT\_SELF component interface.

### ***USER\_PROFILE\_XFR***

This service operation changes the shape of the inbound USER\_PROFILE.VERSION\_84 message to an internal shape that you configure based on your needs for partial user profile synchronization.

## Application Engine Programs

This section describes the Application Engine programs that designed for use in your security implementation.

### ***DYNROLE***

The DYNROLE Application Engine program is called when Dynamic Role Rules are executed for a single user from the User Profile component.

You run this program from the Roles page in the Roles component. You can also schedule this program to run as needed through Process Scheduler.

### ***DYNROLE\_PUBL***

The DYNROLE\_PUBL Application Engine program is called when Dynamic Role Rules are executed for a single role from the Role component.

You run this program from the Roles page in the Roles component. You can also schedule this program to run as needed through Process Scheduler.

### ***DYNROLE\_SYNC***

The DYNROLE\_SYNC Application Engine program is designed to run in synchronous mode and is primarily used for the Role Maintenance Component Interface.

### ***PURGEOLDUSRS***

The PURGEOLDUSRS Application Engine program deletes users who have not signed on within a period specified in Password Controls.

You run this program by selecting PeopleTools, Security, User Profiles, Purge Inactive User Profiles or by selecting PeopleTools, Security, Password Configuration, Password Controls, and then clicking the Schedule button under Purge Inactive User Profiles. You can also schedule this program to run as needed through Process Scheduler.

### ***LDAPSCHEMA***

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

You run this program by selecting PeopleTools, Security, Directory, Cache Directory Schema.

### ***LDAPMAP***

Application Engine program used to import and export data to and from the LDAP directory into or from a PeopleSoft table. The process is based on an LDAP Map.

You run this program by selecting PeopleTools, Security, Directory, Authentication Map.

### ***USR\_PRFL\_XFR***

---

## Security Administration Implementation

This section discusses:

- Preparing to use PeopleSoft security.
- Administering security from applications.
- Reviewing and monitoring your security implementation.

### 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 xiii

*Enterprise PeopleTools 8.50 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, then you have the option of modifying the PeopleSoft security pages to include links to those application-specific pages. These links provide 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 Profiles component, My System Profile page, the Role component, or the Permission List (ACCESS\_CNTRL\_LISTX) component. To add links to a security profile, select the appropriate page in the Security Links (SEC\_OTHER\_SETTINGS) component and add the link information for the target page. After you save the link information, the link appears on the Links page for the appropriate security profile.

User	My Profile	Role	Permission List
------	------------	------	-----------------

User Security Links						Customize   Find   View All      	First	1 of 1	Last
Active Flag	Description	*Menu Name	*Menu Bar Name	Bar Item Name	Item Name	Test			
<input type="checkbox"/>		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<a href="#">Test</a>			

### Security Links - User page

<b>Active Flag</b>	Enables you to activate and deactivate links. Only those links with the Active Flag selected appear for system users.
<b>Description</b>	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.
<b>Menu Name</b>	From the drop-down list, add the menu name. This value is the application in which the page resides, such as Administer HR Security.
<b>Menu Bar Name</b>	From the drop-down list, add the menu bar name, such as Use, Setup, Process, and so on.
<b>Bar Item Name</b>	From the drop-down list, add the bar item name. For example, the bar item name for this page is Security Links.
<b>Item Name</b>	From the drop-down list, add the item name. For example, the item names for this component are User, Role, My Profile, and Permission List.
<b>Test</b>	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 links exist, click the plus sign button to add a new row.
4. Add the appropriate link information (Menu Name, Menu Bar name, and so on).
5. After you enter the appropriate link information, click Test to make sure the link points 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.

---

## Reviewing and Monitoring Your Security Implementation

PeopleSoft provides a collection of predefined queries that enable you to review, monitor, and audit system access by user, role, and permission list so that you can detect discrepancies. The Common Queries page enables you to run the following sets of queries:

- User ID queries.
- Role queries.
- Permission list queries.
- PeopleTools objects queries.
- Definition Security queries.
- Access log queries.

To run a query, click the link, enter the appropriate criteria (such as User ID), and click View Results.

## 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 software 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, 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.** A PeopleSoft security definition called an Access Profile also exists, 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 cannot 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**

OracleMetaLink 3 web site.

---

## **PeopleSoft Online Security**

The PeopleSoft system has many elements, such as batch processes, object definitions, and application data. Use PeopleTools security tools to control access to most of these elements. 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 in. 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 signing in, a user can stay connected as long as the sign-in time allows and as long as the browser does not sit idle for longer than the time-out interval. A time-out interval specifies how long the user's machine can remain idle—no keystrokes, no SQL—before the PeopleSoft system automatically signs the user out of the application.

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

---

**Note.** Other time-out intervals, unrelated to security, are controlled by your web server and by PeopleSoft Pure 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, your batch processes should be run in a secure environment.

The three levels of security for batch programs are:

- 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.
- PeopleSoft Process Scheduler enables you to 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 the PeopleSoft system 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 these 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 software 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 does not 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 software uses authentication tokens embedded in browser cookies to authorize users and enable single sign-in throughout the system. To secure links between elements of the system, including browsers, web servers, application servers, and database servers, PeopleSoft software incorporates a combination of SSL security and Oracle Tuxedo and Oracle 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 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 Oracle Tuxedo and Oracle Jolt encryption in these locations:

- Between the web server and the application server.
- Between the integration gateway and a PeopleSoft system (Oracle 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 8.50 PeopleBook: Internet Technology*

*Enterprise PeopleTools 8.50 PeopleBook: PeopleSoft Integration Broker*

---

## **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 20

## 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 do not 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.

---

---

**Note.** When performing a database compare or copy, both databases must have the same connect ID.

---

---

**Warning!** Without a connect ID specified, the system assumes the 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 the 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 PeopleSoft Pure Internet Architecture. During a PeopleSoft Pure Internet Architecture 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 cannot be readily referenced or 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 to create a new, full-access ID, 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 are prompted for an RDBMS system administrator ID and password. This information is used to automatically create a default access profile. If you will 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 signon PeopleCode.
- Single signon.

## PeopleSoft Sign-in

The most common direct sign-in to the PeopleSoft database is the application server sign-in.

These are the basic steps that are taken when the application server signs in to the database:

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 using 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 PeopleSoft Pure Internet Architecture and Microsoft 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.

---

**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 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 the PeopleSoft system 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 7, "Employing LDAP Directory Services," page 135](#)

## 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 Profiles 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 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 sign on through PeopleSoft Pure Internet Architecture or three-tier Microsoft Windows clients take advantage of signon PeopleCode.

---

## Single Signon

PeopleSoft Pure Internet Architecture 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 10, "Working with SSL and Digital Certificates," page 213](#)

---

## 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. You can assign roles to users in two ways: the static approach and the dynamic approach.

### ***Static***

Using the static approach, 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 approach 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***

Using the dynamic approach, 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. Synchronization 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 needs a list of managers for a particular transaction. Because the manager information resides in PeopleSoft Human Resources, PeopleSoft Human Resources publishes any changed information to PeopleSoft Financials to keep the data synchronized.

PeopleSoft security also publishes a message when a user profile changes (if the corresponding Service Operation version is active), which is most useful if you are not using LDAP to store user information. If you store user information in the PeopleSoft system, 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.

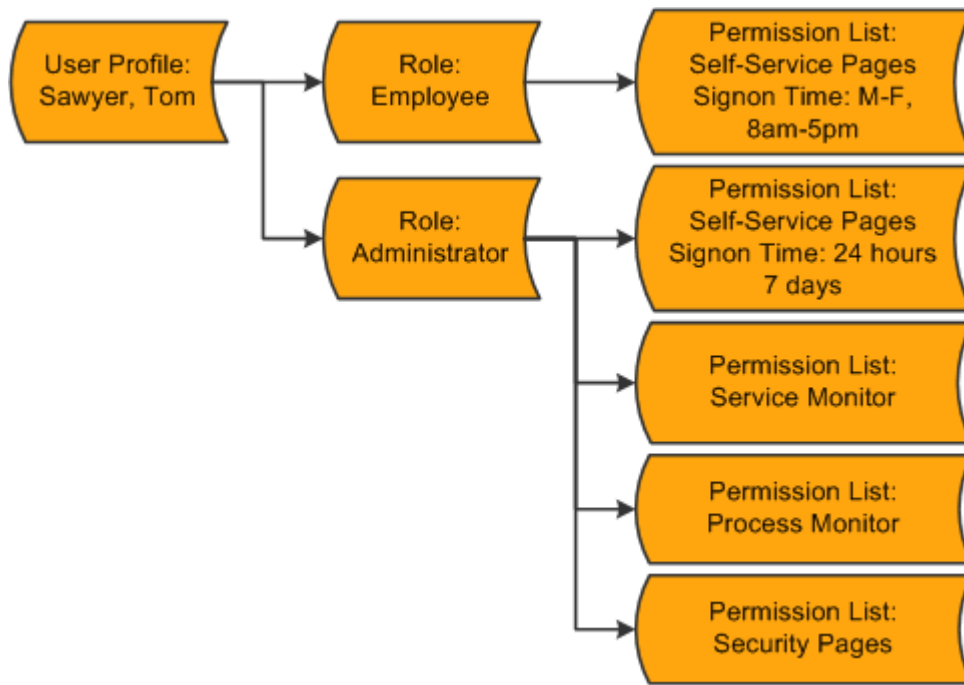
---

## 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, web services permissions, and so on. 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 definitions hierarchy showing how permissions flow to roles, which flow to user profiles

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 service 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 would 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 whereby you create numerous, generic permission lists that you can add to and remove from 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.

## 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. On the search page, locate and select the permission list that you want to copy (clone).

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 and select the permission list that you want to delete.

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 action 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, and then click the Edit Components link to access the Component Permissions page.

See [Chapter 3, "Setting Up Permission Lists," Setting Page Permissions, page 33](#).

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. A process definition of the same name also exists.

See

## Defining Permissions

This section discusses how to:

- Set general permissions.
- Set page permissions.
- Set PeopleTools permissions.
- Set process permissions.
- Set sign-on time permissions.
- Set component interface permissions.
- Set web library permissions.
- Set web services permissions.
- Set personalization permissions.
- Set query permissions.
- Set mass change permissions.
- Display additional links.
- View when a permission list was last updated.
- Run permission list queries.


## Pages Used to Define Permission Lists

<i>Page Name</i>	<i>Definition Name</i>	<i>Navigation</i>	<i>Usage</i>
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.

<b>Page Name</b>	<b>Definition Name</b>	<b>Navigation</b>	<b>Usage</b>
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.
Web Libraries	ACL_WEBLIBS	PeopleTools, Security, Permissions and Roles, Permission Lists, Web Libraries	Set web library permissions.
Web Services	ACL_WS_OPR	PeopleTools, Security, Permissions and Roles, Permission Lists, Web Services	Set web services permissions.
Personalizations	PLIST_OPTN	PeopleTools, Security, Permissions and Roles, Permission Lists, Personalizations	Specify which personalizations users can use and customize.
Query	PERMLIST_QUERY	PeopleTools, Security, Permissions and Roles, Permission Lists, Query	Control the query operations a user can perform and the data a user can access while using PeopleSoft Query.
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 General page (select PeopleTools, Security, Permissions and Roles, Permission Lists and click the General tab).

<b>General</b>	Pages	PeopleTools	Process	Sign-on Times	Component Interfaces	
----------------	-------	-------------	---------	---------------	----------------------	---

Permission List: **PTPT1100**

Description:

**Permission List General**

Navigator Homepage:  

☒ Can Start Application Server?

☐ Allow Password to be Emailed?

**Time-out Minutes**

☒ Never Time-out

☐ Specific Time-out (minutes)

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 on startup.

If this is the user profile's PeopleSoft Navigator homepage permission list, the system is passed 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 will create a user profile that is 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 Oracle 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 should not be used by an actual user who signs in to the application server and starts it by submitting the appropriate commands.

---

**Note.** Password controls do not 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; they do not apply if the user profile is used for two-tier activities like starting an application server or process scheduler.

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

---

**Allow Password to be Emailed?**

Select to enable users to receive forgotten passwords through email. At some sites, the security administrator may not want passwords appearing unencrypted in any 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 levels.

---

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. A custom time-out interval:

- Must be a positive integer.
- Cannot contain edit characters, such as commas or a \$.
- 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 set up most permission lists to time out in 20 minutes, but create a special ADA permission list for which timeout occurs after 60 minutes.

---

**Note.** Because timeout limits are also controlled at the web server level, you will need to change the web server timeout values also.

---

## Setting Page Permissions

Access the Pages page (select PeopleTools, Security, Permissions and Roles, Permission Lists and click the Pages tab).

General

Pages

PeopleTools

Process

Sign-on Times

Component Interfaces

Permission List:

ALLPAGES

Description:

All pages and weblibs

Mobile Page Permissions:

Menus

Customize | Find | View All |  First 1-24 of 24 Last

Menu Name	Menu Label	Edit Components		
APPLICATION_ENGINE	Application Engine	<a href="#">Edit Components</a>	<a href="#">+</a>	<a href="#">-</a>
APPMMSGMONITOR	Application Message Monitor	<a href="#">Edit Components</a>	<a href="#">+</a>	<a href="#">-</a>
ARCHIVING	Data Archival	<a href="#">Edit Components</a>	<a href="#">+</a>	<a href="#">-</a>
CUBE_MANAGER	Cube Manager	<a href="#">Edit Components</a>	<a href="#">+</a>	<a href="#">-</a>
EDI_MANAGER	EDI Manager	<a href="#">Edit Components</a>	<a href="#">+</a>	<a href="#">-</a>
MAINTAIN_SECURITY	Maintain Security	<a href="#">Edit Components</a>	<a href="#">+</a>	<a href="#">-</a>
MASS_CHANGE	Mass Change	<a href="#">Edit Components</a>	<a href="#">+</a>	<a href="#">-</a>

Permission Lists - Pages page

This table describes the fields on the Pages page.

<b>Mobile Page Permissions</b>	Click to grant access to mobile application pages.
	<b>Important!</b> PeopleSoft Mobile Agent is a deprecated product. These features exist for backward compatibility only.
<b>Menu Name</b>	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.
<b>Menu Label</b>	Displays the menu label associated with the PeopleSoft Application Designer menu name.
<b>Edit Components</b>	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.

When you click the Edit Components link, the Component Permissions page appears:





---

**Note.** To find the name of a menu, component, or 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 consideration. 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. Alternatively, you could grant access to only a few of the Use menu items or make some items display only.

You grant access permission to two categories of components:

- 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 do not allow you to grant item-by-item access; you can either access all the menus and menu items or you cannot. 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.

The Components page appears.

3. Locate the component to which you want to grant access.

By default, when adding a new permission list, no components are authorized.

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

The Page Permissions page appears. You specify the actions that a user can complete on this page. You can select from these 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.

Specify how users can alter information on a page, such as Add, Update/Display, and Correction. The available options 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.

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

Repeat each step for each menu name.

---

**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 in the menu.

---

### ***Granting Access to Mobile Pages***

To add access to mobile pages:

---

**Important!** PeopleSoft Mobile Agent is a deprecated product. These features exist for backward compatibility only.

---

- Select PeopleTools, Security, Permissions & Roles, Permission Lists, and select the Pages page.
- Click the Mobile Page Permissions link.  
The Mobile Page Permissions page appears.
- To add a new mobile page to the permission list, click the plus sign.
- For the Mobile Page Name edit box, click the search button.
- Search for and select the mobile page for which you need to grant access.
- Click OK.
- Save the permission list.

## Setting PeopleTools Permissions

Access the PeopleTools page (select PeopleTools, Security, Permissions and Roles, Permission Lists and click the PeopleTools tab).

The screenshot shows the 'PeopleTools' tab selected in a navigation bar. Below the tabs, the 'Permission List' is set to 'ALLPAGES' and the 'Description' is 'All pages and weblibs'. The main content area is divided into three sections: 'PeopleTools Permissions', 'Realtime Event Notification', and 'Data Archival'. The 'PeopleTools Permissions' section contains five items with checkboxes: 'Application Designer Access' (checked), 'Data Mover Access' (checked), 'Definition Security Access' (checked), 'Query Access' (checked), and 'Performance Monitor PPMI Access' (unchecked). There are also links for 'Definition Permissions', 'Tools Permissions', and 'Miscellaneous Permissions'. The 'Realtime Event Notification' section has a link for 'Realtime Event Notification Permissions'. The 'Data Archival' section contains four items with checkboxes: 'Generate SQL' (unchecked), 'Run SQL' (unchecked), 'Edit SQL' (unchecked), and 'Purge Audit' (unchecked).

### Permission Lists - PeopleTools page

The PeopleTools Permissions section of this page applies to standalone PeopleTools applications. They are not Pure Internet Architecture-based, but are Microsoft Windows programs that were not developed using PeopleSoft Application Designer. They include:

- PeopleSoft Application Designer.
- PeopleSoft Data Mover.
- PeopleSoft Definition Security.
- PeopleSoft Query (Microsoft Windows interface, not the browser interface).

The Performance Monitor PPMI Access check box does not 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 8.50 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 Definition Permissions, Tools Permissions, and Miscellaneous Permissions links enable you to provide more detail to PeopleSoft Application Designer access permissions.

### ***Definition Permissions***

Access the Definition Permissions page (click the Definition Permissions link on the PeopleTools page).

## Definition Permissions

Permission List: PTPT1100

Description: Security Administrator

Customize   Find    First 1-28 of 28 Last	
Object	*Access
Activity	Full access
Analytic Model	No access
App Engine Program	Full access
Application Package	Full access
Approval Rule Set	Full access
Business Interlink	Full access
Business Process	Full access
Component	Full access
Component Interface	Full access
Field	Full access
File Layout	Full access
File Reference	Full access
HTML	Full access
Image	Full access
Menu	Full access
Merge	No Access
Message	Full access
Message Channel	Full access
Message Node	Full access
Mobile Pages	Full access
Page	Full access
PeopleCode Work-In-Progress	No Access
Problem Type	Full access
Project	Full access
Record	Full access
Style Sheet	Full access
Type Code	Full access
Visual Merge Page	No Access

Full Access (All)

Read Only (All)

No Access (All)

## Definition Permissions page

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

---

**Note.** On this page, you add permissions to a definition type, such as Application Engine programs. You grant access to *specific* definitions, 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 setting 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 definition 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 8.50 PeopleBook: PeopleSoft Application Designer Developer's Guide*, "Using PeopleSoft Application Designer," Building and Maintaining Data and [Chapter 15, "Implementing Definition Security," page 267](#).

## Tools Permissions

Access the Definition Permissions page (click the Tools Permissions link on the PeopleTools page).

## Tools Permission

Permission List: PTPT1100

Description: Security Administrator

Customize   Find         First 1-6 of 6 Last			
Tool	*Access Code		
Build / Data Admin.	Full data adm ▼	Full Access (All)	
Change Control	Supervisor ac ▼	Read Only (All)	
Language Translations	Full access ▼	No Access (All)	
Peoplecode Debugger	Full access ▼		
SQL Editor	Full access ▼		
Upgrade	No access ▼		

### Tools Permission page

In addition to securing 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:

- 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 tool includes Copy Project, Compare and Report, and so on.

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



**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:

<b>Source DB</b>	<b>Target DB</b>	<b>Compare?</b>	<b>Copy?</b>	<b>Export?</b>	<b>Import?</b>
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**

Access the Miscellaneous Permissions page (select the Miscellaneous Permissions link on the PeopleTools page).

## Miscellaneous Permissions

Permission List: PTPT1100

Description: Security Administrator

Customize   Find       First 1-5 of 5 Last	
Feature	*Access
Access Profiles	Full access ▼
Color	Full access ▼
Field Format	Full access ▼
Style	Full access ▼
Tool Bar	Full access ▼

Full Access (All)

Read Only (All)

No Access (All)

### Miscellaneous Permissions page

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 access*, or *Full access*. You can select the (ALL) buttons to grant the same permissions to each item.

### Real-time Event Notification Permissions

Access the REN Permissions page (click the Realtime Event Notification Permissions link on the PeopleTools page).





## Process Profile Permission

Permission List: PTPT1100

Description: Security Administrator

Server Destinations	Allow Requestor To
File: <input type="text"/>	<input type="checkbox"/> Override Output Destination
Printer: <input type="text"/>	<input type="checkbox"/> Override Server Parameters
<b>OS/390 Job Controls</b>	<input type="checkbox"/> View Server Status
Name: <input type="text"/>	<input type="checkbox"/> Update Server Status
Acct: <input type="text"/>	<input type="checkbox"/> Enable Recurrence Selection
<b>Allow Process Request</b>	
*View By: <input type="text" value="None"/>	
*Update By: <input type="text" value="None"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

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 specified in PSADMIN (or PSPRCS.CFG) for the Process Scheduler Server Agent.

- Printer:

Specify the network or local printer to which the hard-copy output should be sent. You must explicitly specify the printer; no meta-variables are available for this value.

**OS/390 Job Controls**

---

**Note.** This group of options applies only to DB2 UDB for 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 z/OS, 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 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 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, especially when 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.

<b>Override Output Destination</b>	Select to allow a user to change the value in the Output Destination column on the Process Scheduler Request page.
<b>Override Server Parameters</b>	Select to enable users to select the server name and modify the run date/time group on the Process Scheduler Request page.
<b>View Server Status</b>	Select to enable users to access the Server List page in PeopleSoft Process Monitor.
<b>Update Server Status</b>	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.
<b>Enable Recurrence Selection</b>	Select to enable a run recurrence value for processes and jobs scheduled to run on the server.

### **See Also**

*Enterprise PeopleTools 8.50 PeopleBook: PeopleSoft Process Scheduler*, "Setting Up PeopleSoft Process Scheduler Security," Setting Up PeopleSoft Process Scheduler Privileges and Profiles

*Enterprise PeopleTools 8.50 PeopleBook: PeopleSoft Process Scheduler*, "Defining PeopleSoft Process Scheduler Support Information," Setting Process Definition Options

## **Setting Sign-on Time Permissions**

Access the Sign-on Times page (select PeopleTools, Security, Permissions and Roles, Permission Lists and click the Sign-on Times tab).











Web Services




- Service**
- Displays the name of the web service defined in the PeopleSoft system.
- Edit**
- Click to launch the Web Service Permissions page.
- Full Access (All)**
- Click to grant full access to all services listed on the page.
- No Access (All)**
- Click to set all services listed on the page to *No Access*.

Web Service Permissions

Access the Web Service Permissions page (click the Edit link on the Web Services page).

Web Service Permissions

Service: PT\_WORKLIST

Permission		Customize   Find      First 1-2 of 2 Last	Full Access (All)
Service Operation	Access		No Access (All)
CREATE_WORKLIST_ITEM	No Access 		
GETWLINSTANCE	No Access 		
	<div>Full Access</div> <div>No Access</div>		

Web Service Permissions page

- Service Operation**
- Each operation performed by the web service appears in the Service Operation list.
- Access**
- Grant access to the operation by selecting *Full Access*. Deny access by selecting *No Access*.

**Note.** By default, the system sets the value to *No Access*. Make sure to modify the access values to reflect the desired level.

See Also

*Enterprise PeopleTools 8.50 PeopleBook: PeopleSoft Integration Broker, "Managing Service Operations," Setting Permissions to Service Operations*

*Enterprise PeopleTools 8.50 PeopleBook: PeopleTools Portal Technologies, "Configuring WS-Security For WSRP Consumption and Production"*

## Setting Personalization Permissions

Access the Personalizations page (select PeopleTools, Security, Permissions and Roles, Permission Lists and click the Personalizations tab).

Permission List: PTPT1100

Description: Security Administrator

Personalization Options		
Option Category Level	Option Category Group	Edit Options
Tools	App Designer Preferences	<a href="#">Edit Options</a> + -

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 category group.

### ***Personalization Permissions***

When you click the Edit Options link, the Personalization Permissions page appears.





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 build 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) Deselect 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 deselect 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, do not deselect 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 will 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, do not group a large number of record components into a single access group.

---

## ***Defining Query Profiles***

Access the Query Profile page (click the Query Profile link on the Query page).

Permission List: ALLPAGES

Description: All pages and weblibs

PeopleSoft Query Use	Advanced SQL Options
<input type="checkbox"/> Only Allowed to run Queries <input type="checkbox"/> Allow creation of Public Queries <input type="checkbox"/> Allow creation of Role, Process and Archive Queries Maximum Rows Fetched: <input type="text"/> (0 = Unlimited) Maximum Run Time in Minutes: <input type="text"/> (0 = Unlimited)	<input type="checkbox"/> Allow use of Distinct <input type="checkbox"/> Allow use of 'Any Join' <input type="checkbox"/> Allow use of Subquery/Exists <input type="checkbox"/> Allow use of Union <input type="checkbox"/> Allow use of Expressions Maximum Joins Allowed: <input type="text"/> (9 = Unlimited) Maximum 'In Tree' Criteria: <input type="text"/> (9 = Unlimited)
PeopleSoft Query Output	
<input type="checkbox"/> Run <input type="checkbox"/> Run to Excel	

### Query Profile page

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, and 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.

---

**Note.** The first level of security is access to PeopleSoft Query itself. Not every user needs to create queries. You grant access to the Windows client of PeopleSoft Query by selecting the Query Access check box on the PeopleTools page of a permission list. You grant access to Query Manager by including the QUERY\_MANAGER menu and its related components on the Pages page of a permission list.

---

You select at least one of the options in the PeopleSoft Query Use section of this page to give users query access.





[Web Libraries](#)
[Web Services](#)
[Personalizations](#)
[Query](#)
[Mass Change](#)
[Links](#)
[Audit](#)

Permission List: ALLPAGES

Description: All pages and weblibs

Use the links below to navigate to other security settings for this object.

Links	
Description	Edit
Data Archive Security	<a href="#">Edit</a>
Business Objects Security	<a href="#">Edit</a>

#### Permission List - Links page

Use this page to access links to other pages within your PeopleSoft system. For example, perhaps a PeopleSoft application requires a specific security setting to be associated with a permission list. If this application-specific setting appears on a page not in PeopleTools Security, add a link to the application page so that anyone updating the permission list can easily navigate to it.

**Note.** The Links page is read-only. You create the inventory of links to pages that exist outside of PeopleTools Security by using the Security Links (PeopleTools, Security, Security Objects, Security Links) component.

#### See Also

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

## Viewing When a Permission List Was Last Updated

Access the Audit page (select PeopleTools, Security, Permissions & Roles, Permission Lists and click the Audit tab).

[Web Libraries](#)
[Web Services](#)
[Personalizations](#)
[Query](#)
[Mass Change](#)
[Links](#)
[Audit](#)

Permission List: ALLPAGES

Description: All pages and weblibs

Audit Information	
Last Update User ID:	QEDMO
Last Update Date/Time:	05/05/2009 8:13:48AM

#### Permission List - 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 8.50 PeopleBook: Data Management*, "Employing Database Level Auditing," Understanding Database Level Auditing

## Running Permission List Queries

Access the Permission List Queries page (select PeopleTools, Security, Permissions & Roles, Permission Lists and click the Permission List Queries tab).

Permission List: ALLPAGES

Description: All pages and weblibs

**Permission List Queries**

- [Permission List's User IDs](#)  
(Which User ID's are assigned to this Permission List?)
- [Permission List's Roles](#)  
(Which Roles are assigned to this Permission List?)
- [Permission List's Page Access](#)  
(Which pages can this Permission List access?)
- [Permission List's Signon Times](#)  
(What are the valid signon times for this Permission List?)
- [Permission List's Application Designer Object Access](#)  
(Which Application Designer objects can this Permission List access?)
- [Permission List's Misc. PeopleTool Access](#)  
(Can this Permission List access Application Designer, Client Process, Data Mover, Import Manager, Object Security or Query?)
- [Permission List's Content Reference Access](#)  
(Which Content References can this Permission List access?)
- [Permission List's Content Reference \(includes Portal\) Access](#)  
(Which Content References (includes Portal) can this Permission List access?)
- [Permission List's Content Reference \(includes Menu, Component and Market\) Access](#)  
(Which Content References (includes Menu, Component and Market) can this Permission List access?)
- [Permission List's Content Reference \(includes Portal, Menu, Component and Market\) Access](#)  
(Which Content References (includes Portal, Menu, Component and Market) can this Permission List access?)
- [Permission List's Web Service Operation Access](#)  
(Which Web Service Operations can this Permission List access?)

Permission List - Permission List Queries page

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

To run permission list queries:

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

A new browser window opens.

2. View the information the query returns or click a download results link.

---

**Note.** The size of the file appears in parentheses beside the download options.

---

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.

- XML file.

Downloads the query results as a xml (.xml) file.

## 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.
- Using the PeopleSoft Administrator 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.

---

**Note.** In previous releases, roles were associated with PeopleSoft Workflow. PeopleTools has expanded role definitions so that they are also a part of the security architecture. There is only one type of role definition, and you maintain it within Security.

---

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 static role members.

Other users may obtain membership in a role programmatically. You can run a batch process that uses predefined role rules and assigns roles to user profiles according to these rules. Users who become members of a particular role programmatically are dynamic role members.

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. If you implement dynamic roles, you reduce administrative tasks.

---

## Managing Roles

This section discusses how to:

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

### Copying Roles

To copy a role:

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

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 and select the role that to delete.

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 who are assigned dynamically, 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 73

---

## 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

<i>Page Name</i>	<i>Definition Name</i>	<i>Navigation</i>	<i>Usage</i>
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 aren't using the dynamic roles, this list isn't populated.
Workflow	ROLEWRKFLOW	PeopleTools, Security, Permissions & Roles, Roles, Workflow	Set user routing options.

<b>Page Name</b>	<b>Definition Name</b>	<b>Navigation</b>	<b>Usage</b>
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.
Audit	ROLE_AUDIT	PeopleTools, Security, Permissions & Roles, Roles, Audit	View when a permission list was last updated.

## Assigning Permissions to Roles

Access the Permission Lists page (select PeopleTools, Security, Permissions and Roles, Roles and click the Permission Lists tab).


**Permission Lists**
Members
Dynamic Members
Workflow
Role Grant
Links
Role Queries
Audit

Role Name: Employee  
Description: Employee

Permission Lists			
Permission List	Description	View Definition	
PTPT1000	PeopleSoft User	<a href="#">View Definition</a>	+ -
PSWDEXPR	Password Expired	<a href="#">View Definition</a>	+ -

Roles - 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 before adding it to a role.

### View Definition

Click to open the permission list definition, where you can view the options in the permission to ascertain whether it is suitable for a particular role.



General

Permission Lists

Members

Dynamic Members

Workflow

Role Grant

Links

Role Queries

Audit

Role Name:

Employee

Description:

Employee

Rules

☐ Query Rule Enabled

☐ PeopleCode Rule Enabled

☐ Directory Rule Enabled

Assign Directory Rule

Delete Members

Test Rule(s)

Execute on Server:

Execute Rule(s)

Refresh

Process Monitor

Service Monitor

User ID:

Search

Dynamic Members

Customize | Find | View All |

First 1 of 1 Last

User ID	Description	View Definition
		View Definition

Roles - Dynamic Members page

Use this page to set the rule to invoke to assign roles. A dynamic role rule is defined or coded in PeopleSoft Query, 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. The navigation buttons enable you to 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 for which to search.
- 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 group 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.

<b>Directory Rule Enabled</b>	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 the DynRoleMembers PeopleCode program. This 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, if your LDAP server is grouped by geographic region, then 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.
<b>Execute on Server</b>	Select the appropriate PeopleSoft Process Scheduler server to run the rule.
<b>Refresh</b>	After you run a rule, click to repopulate the grid with updated information.
<b>Process Monitor</b>	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.
<b>Service Monitor</b>	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.
	<hr/> <b>Note.</b> The successful completion of the dynamic roles program does not ensure that your roles were updated; the associated message must also be delivered successfully. <hr/>

---

**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.** This example assumes a working knowledge of PeopleSoft Query.

---

In this example, you need to find all users who 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.



The SQL is:

Records	Query	Expressions	Prompts	Fields	Criteria	Having	View SQL	Run
Query Name: PSOPRALIAS_QRY		Description:						
Query SQL:								
<pre>SELECT A.OPRID, A.EMPLID FROM PSOPRALIAS A WHERE A.OPRID = 'PS'</pre>								

Query view SQL

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

## Query Access Manager

Effective Date: 01/01/1900    Status: Active    Valid Tree

Tree Name: QUERY\_TREE\_HR    Human Resources Access Group

[Save Draft](#) | [Save](#) | [Save As](#) | [Close](#)    [Tree Definition](#) | [Display Options](#) | [Print Format](#)

### HR ACCESS GROUP > SECURITY VIEWS

[Collapse All](#) | [Expand All](#)    [Find](#)    [First Page](#) | [35 of 1929](#) | [Last Page](#)

- HR ACCESS GROUP - Human Resources Access Group
  - SECURITY VIEWS - Security Views**
    - OPRID\_JOB\_VW - User/Job View
    - EMPLMT\_SRCH\_GBL - Employee Search - Global
    - PERS\_SRCH\_GBL - Search - All Pers w/ an ERN
  - HR\_EMPLOYEE\_BRA -
  - EMPLOYEE REGISTRY BR -
  - TEMPLATE DATA -
  - MILITARY PROCESSING - Military Rank Processing
  - MASS UPDATE - Mass Update Archive Tables
  - I9\_DATA -
  - WAGE PROGRESSION GRP -
  - SUCCESSN ACCESS GRP - Succession Plan Access Group

Adding the view to a query tree

After you create the view, you create a query. In this example, the properties assigned to the query enable it to assign a role to users who currently have the job code K03002, Human Resource Analyst. This example shows the query properties:





General	Permission Lists	Members	Dynamic Members	<b>Workflow</b>	Role Grant
---------	------------------	---------	-----------------	-----------------	------------

Role Name: Employee

Description: Employee

**Workflow Routing Options**

☐ Allow notification

☐ Allow Recipient Lookup

☐ Use Query to Route Workflow

### Roles - 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, such as vendors, customers, employees, sales leads, and so on. This check box is available only if the Allow notification check box is selected.
- Use Query to Route Workflow** Select to determine workflow routings by a workflow query. This value depends on your workflow scheme.

## Decentralizing Role Administration

You use the Role Grant page to assign limited security administration capability to specified users. You designate them as *remote security administrators* by defining roles that they can grant to other users. Because the settings on this page are part of the implementation of *distributed user profiles*, the page is documented along with the Distributed User Profiles component.

See [Chapter 5, "Administering User Profiles," Implementing Distributed User Profiles, page 113.](#)

## Displaying Additional Links

Access the Links page (select PeopleTools, Security, Permissions & Roles, Roles and click the Links tab).



Roles - Links page

Use this page to access links to other pages within your PeopleSoft system. For example, perhaps a PeopleSoft application requires a specific security setting to be associated with a role. If this application-specific setting appears on a page not in PeopleTools Security, add a link to the application page so that anyone updating the role can easily navigate to the page.

**Note.** The Links page is read-only. You create the inventory of links to pages that exist outside of PeopleTools Security by using the Security Links component.

If you have added any links for roles 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

Access the Links page (select PeopleTools, Security, Permissions & Roles, Roles and click the Role Queries tab).

General	Permission Lists	Members	Dynamic Members	Workflow	Role Grant	Links	Role Queries
---------	------------------	---------	-----------------	----------	------------	-------	--------------

Role Name: Employee

Description: Employee

**Role Specific Queries**

[Role's User IDs](#)  
(Which User IDs are assigned to this Role - including both static and dynamic?)

[Role's Permission Lists](#)  
(To which Permission Lists does this Role belong?)

[Role's Page Access](#)  
(Which pages can this Role access?)

[Role's Content Reference Access](#)  
(Which access to Content References has been granted for this Role?)

[Role's Content Reference \(includes Portal\) Access](#)  
(Which access to Content References (includes Portal) has been granted for this Role?)

[Role's Content Reference \(includes Menu, Component and Market\) Access](#)  
(Which access to Content References (includes Menu, Component and Market) has been granted for this Role?)

[Role's Content Reference \(includes Portal, Menu, Component and Market\) Access](#)  
(Which access to Content References (includes Portal, Menu, Component and Market) has been granted for this Role?)

[Role's Web Service Operation Access](#)  
(Which access to Web Service Operations has been granted for this Role?)

### Roles - Role Queries page

Use role queries to provide detailed information about 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 action invokes a new browser window.
2. View the information the query returns or click a download results link.

---

**Note.** The size of the file appears in parentheses next to the download options.

---

The download options are:

- 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 (select PeopleTools, Security, Permissions & Roles, Roles and click the Audit tab).

Role Name: Employee

Description: Employee

Audit Information	
Last Update User ID:	QEDMO
Last Update Date/Time:	05/05/2009 8:39:22AM

Roles - 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 8.50 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. When you enter a new user into the system, the user has access only to the public pages you authorize for the NEWUSER role. When the dynamic role rules execute, the new user becomes a member of the roles that apply based on the user's employee position.

---

**Note.** The NEWUSER role is not a PeopleSoft-delivered role. You can name the role to suit your requirements.

---

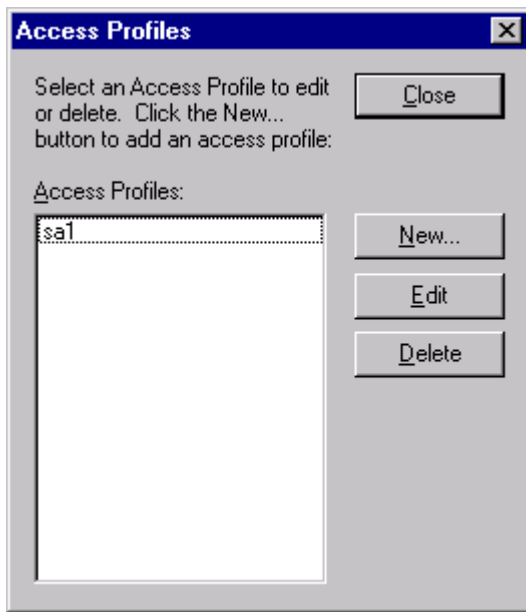
To implement a NEWUSER role:

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.









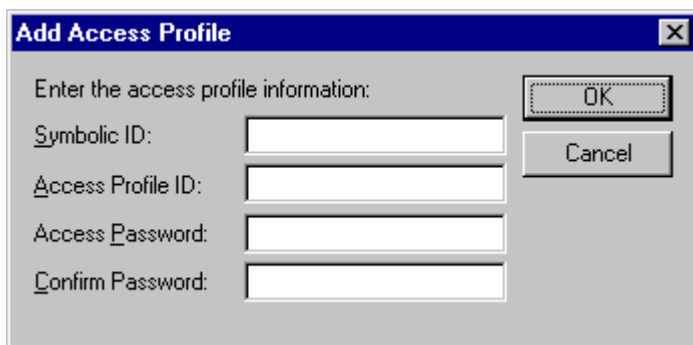
Access Profiles dialog box

<b>Close</b>	Click to exit this dialog box.
<b>New</b>	Click to create a new access profile definition.
<b>Edit</b>	Click to edit an access profile definition.
<b>Delete</b>	Click to delete an access profile definition.

## Setting Access Profile Properties

When you create or modify an Access Profile using the Access Profiles dialog, you need to understand the properties that comprise an access profile. After reading this section, you will be familiar with these properties.

Access the Add Access Profile dialog box (click the New button in the Access Profiles dialog box).



Add Access Profile dialog box





User profile types also provide a way to link user profiles with data stored in application-specific records. PeopleSoft applications primarily need this link for self-service transactions. For example, you want employees to see only their own benefits, or you want customers to view and pay only 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 correct ID based on the user profile. The system needs the value because personal data and vendor contact data may have the same key field. Because personal data and vendor contact data resides in different records, no edit exists that will prevent the two records from having the same key.

This table lists the profile types that PeopleSoft delivers:

<i><b>ID Type</b></i>	<i><b>Description</b></i>
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

## Page Used to Set Up User Profile Types

<i><b>Page Name</b></i>	<i><b>Definition Name</b></i>	<i><b>Navigation</b></i>	<i><b>Usage</b></i>
User Profile Types	PSOPRALIASTYPE	PeopleTools, Security, Security Objects, User Profile Types	Define user profile types.









## Pages Used to Specify User Profile Attributes

<i>Page Name</i>	<i>Definition Name</i>	<i>Navigation</i>	<i>Usage</i>
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 task defines user 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	Determine when and who last updated a profile.
Links	USER_OTHER	PeopleTools, Security, User Profiles, User Profiles, Links	Display 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 (select PeopleTools, Security, User Profiles, User Profiles and click the General tab).





<b>Currency Code</b>	If the user works with international currencies, select a currency code to reflect the native or base currency. Values will appear in the currency with which the user is familiar.
<b>Default Mobile Page</b>	Select the mobile homepage that should appear after users sign on to their mobile device. <hr/> <b>Important!</b> PeopleSoft Mobile Agent is a deprecated product. These features exist for backward compatibility only. <hr/>
<b>Enable Expert Entry</b>	Select to specify that some users, such as expert or power users, can defer all processing of the data that they enter. This selection enables users to reduce the number 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. Deselect this check box to prevent a user from specifying deferred processing.
<b>Allow Switch User</b>	Select this option to designate users who can change identities in a PeopleSoft system. This feature applies only when accessing PeopleSoft applications using a browser; it has no effect on two-tier or three-tier connections.  The default for this feature is hidden. You display this check box by changing the Enable Switch User options on the PeopleTools Options page.  <i>See Enterprise PeopleTools 8.50 PeopleBook: System and Server Administration, "Using PeopleTools Utilities," General Options.</i>
<b>Permission Lists</b>	
<b>Navigator Homepage</b>	Enter a value associated with PeopleSoft Workflow.
<b>Process Profile</b>	Displays a value that 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. <hr/> <b>Note.</b> Only the process profile comes from this permission list, not the list process groups. <hr/>
<b>Primary and Row Security</b>	Displays 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 details.  The system also determines mass change (if needed), and definition security permissions from the primary permission list.





**Route Control** Specify a route control profile for each role assigned to a user. For example, suppose that you have a role named EXPENSE\_REP. If you want a particular expense representative to handle all of the expense reports submitted by people whose last names begin with A, you could assign the user a specific route control profile to send the user reports submitted by individuals with last names beginning with A.

**View Definition** Click to view the role definition associated with this user profile.

See *Enterprise PeopleTools 8.50 PeopleBook: Workflow Technology*, "Using Additional Routing Options," Understanding Route Control Development.

See Chapter 4, "Setting Up Roles," Using the PeopleSoft Administrator Role, page 84.

### **Dynamic Role Rule**

Use these options to test and manually carry out business rules for dynamically updating roles and assigning them to user profiles. You design your role rules using Query Manager, PeopleCode, or LDAP directory rules.

**Execute on Server** Select the Process Scheduler server that should run your role rule.

**Test Rule(s)** Click to test the rules and verify if they will produce the desired results for a particular user. 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)** Click to run the rules and manually assign the appropriate roles to a particular user. Typically, you implement role rules on a regular schedule through PeopleSoft Process Scheduler.

**Process Monitor and Service Monitor** Click to view the status of the process carrying out the role rule and the messages that the process invoked.

## **Specifying Workflow Settings**

Access the Workflow page (select PeopleTools, Security, User Profiles, User Profiles and click the Workflow tab).



<b>From Date and To Date</b>	Enter the date on which the current role user is going to begin and return from a temporary vacancy. This field specifies the time period that the alternate user ID is used.
<b>Supervising User ID</b>	<p>Select the user ID of the user's supervisor from this drop-down list box. The system uses this value when it needs to forward information to the user's supervisor.</p> <p>The system uses the PERSONAL_DATA record to determine the user's supervisor.</p> <hr/> <p><b>Note.</b> If you are using PeopleSoft Human Capital Management (PeopleSoft HCM) applications, this field should not appear. If it does, you must set your workflow system defaults.</p> <hr/>
<b>Routing Preferences</b>	Specify the routing types that 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 the user does not have access to one or both of these places, deselect the check box. For example, if this person is not a PeopleSoft user, deselect Worklist User.
<b>Reassign Work</b>	
<b>Reassign Work To</b>	<p>Use to reassign pending work for this role user if positions change or a user is temporarily out, such as on leave or on vacation.</p> <p>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.</p> <hr/> <p><b>Note.</b> If you don't reassign pending work items, they remain unprocessed.</p> <hr/>
<b>Total Pending Worklist Entries</b>	Displays worklist items that require a user's attention.

### See Also

*Enterprise PeopleTools 8.50 PeopleBook: Workflow Technology*, "Defining Roles and Users"

## Viewing When a User Profile Was Last Updated

Access the Audit page (select PeopleTools, Security, User Profiles, User Profiles and click the Audit tab).





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): Downloads the query results as a CSV (.csv) file.

---

## 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

Access the Password Controls page (PeopleTools, Security, Password Configuration, Password Controls).





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

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

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

---

**Note.** The maximum password length is 32 characters.

---

**Purge Inactive User Profiles** This setting enables you to purge the system of user profiles that have not been used in a specified amount of time. If you maintain user profiles in a directory server, a row is added to the PSOPRDEFN table for the system to access while the user interacts with the system. However, when the user is deleted from the directory server, you must manually delete the row in PSOPRDEFN associated with the deleted user profile.

After you set the time value and save the page, click the Schedule button to access the PURGEOLDUSRS Application Engine program that performs the delete process.

**Password History** This control enables you to define the number of user passwords to retain in the password history table. If the user attempts to reuse a password that is stored in the password history table, the application issues an error and prompts the user to enter a different password.

When the user reaches the maximum number of passwords indicated in the Number of Passwords to Retain field, the system deletes the oldest password and then stores the current password.

---

**Note.** If the password history table contains values and you change the Number of Passwords to Retain field value to 0, the system deletes the password history for all users.

---

## Changing Passwords

Access the Change My Password page (from the homepage, click Change My Password). The PeopleSoft system enables users to change their passwords as needed.

## Change Password

User ID: QEDMO

Description: QE User

\*Current Password:

\*New Password:

\*Confirm Password:

**Change Password**

Change Password page

To change a PeopleSoft password:

1. From the homepage, click Change My Password.
2. On the Change Password page, enter the current password in the Current Password field.
3. In the New Password field, enter a new password.
4. Confirm the new password by entering it again in the Confirm Password field.
5. Click Change Password.

## Creating Email Text for Forgotten Passwords

Before the system emails a new, randomly generated password to a 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.

Access the Forgot My Password Email Text page (PeopleTools, Security, Password Configuration, Forgot My Password Email Text).













---

## Transferring Users Between Databases

You occasionally need to copy security information from one database to another. Typically, you do this as part of an upgrade or to transfer security information from your production environment to your development or testing environment. PeopleTools provides a set of Data Mover (DMS) scripts designed to export and import user profile security information. The provided scripts transfer user profile data from a source to a target database using these tables:

- PSOPRDEFN
- PSOPRALIAS
- PSROLEUSER
- PSUSERATTR
- PSUSEREMAIL
- PSUSERPRSNLOPTN
- ROLEXLATOPR
- PS\_RTE\_CNTL\_RUSER

---

**Note.** Use Application Designer upgrade feature to upgrade both roles and permission lists.

---

One script exports 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 are:

- USEREXPORT.DMS.

This script 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.

This script 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 the *<PS\_HOME>/scripts* folder.

### Considerations

Before running scripts to export and import your security information, you should consider these topics:

- Duplicate Rows

If the target database already contains a row of data with identical keys to a row transferred by the import script, then the duplicate row will not be transferred to the target. The scripts make no attempt to merge the duplicate row; the row is not transferred.

To ensure that you do not have data rows with duplicate keys, ensure that a User Profile in the source database does not exist in the target database with the same name.

You should not have data rows with duplicate keys in your source and target databases when you begin the copy, as unexpected results may occur that will 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 cannot transfer users between databases that run different versions of PeopleTools. Before starting the migration process, upgrade your source and target databases so the release levels match.

### ***Running the Scripts***

Complete the following procedure to run the user transfer 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, run the PeopleTools audits, including DDDAUDIT and SYSAUDIT, to check the consistency of your database.

---

## **Tracking User Sign-in and Sign-out Activity**

Access the Access Log Queries page (select PeopleTools, Security, Common Queries and click the Access Log Queries link on the Review Security Information page).





---

**Important!** Remember that deleting and purging user profile data deletes *every* row of data associated with a particular user profile from *every* table in which the OPRID field is a key field, including archived tables if they remain in your production database.

---

To preserve user profile information in a table for which the OPRID field is a key field, use the Bypass Tables page .

See [Chapter 5, "Administering User Profiles," Bypassing Tables During the Delete User Profile Process, page 94.](#)



## Chapter 6

# Working with User Profiles Across Multiple PeopleSoft Databases

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

- Implement standard user profile synchronization.
- Implement configurable user profile synchronization.
- Transfer users between databases.

---

## Understanding User Profile Synchronization

For implementations that use multiple PeopleSoft databases, you commonly have the same user in more than one database. Typically in production environments, you want the user profile information of the same user to be synchronized among databases. For example, if a user modifies her password or other user profile information in one database, you prefer that the system automatically synchronize the changes across the enterprise rather than have the user or an administrator manually replicate changes in multiple databases.

User profile synchronization involves setting up each PeopleSoft database in the enterprise to send and receive user profile updates through the Integration Broker. When you enter new profiles or modify and delete existing profiles on any publishing database and save, PeopleCode publishes a user profile service operation—which contains a user profile message—and routes the message to all subscribing nodes according to your specifications. The subscribing databases then update the user profile data with data from the publishing database.

---

**Note.** User profiles contain sensitive information. Design and implement user profile synchronization across different nodes with special care. As delivered, user synchronization behavior may not be acceptable in all cases.

---

### ***Components Used to Update User Profiles***

You can use these online components to make changes to user profile data:

- User Profiles (USERMAINT)
- Distributed User Profiles (USERMAINT\_DIST)
- My System Profile (USERMAINT\_SELF)
- Change My Password (CHANGE\_PASSWORD)

- Expired Password (EXPIRE\_CHANGE\_PSWD)
- Forgot My Password (EMAIL\_PSWD)

Administrators use the first two online components. The My System Profile component is a self-service component, which can be used to modify a limited set of data about a user. The Change My Password, Expired Password, and Forgot My Password components are used to change only the user password. Generally, the Forgot My Password component is configured as a public site that is separate from the PeopleSoft application. You can also modify user profile data through batch processes.

### ***Types of User Profile Synchronization***

PeopleSoft applications have two types of user profile synchronization:

- Default user profile synchronization.
- Configurable user profile synchronization.

The publishing processes for default and configurable user profile synchronization use different PeopleCode. PeopleSoft applications are delivered with the PeopleCode for both types of user profile synchronization. You select the appropriate PeopleCode by using the Security PeopleCode Options page. This page eliminates the need to access Application Designer to select the PeopleCode for the corresponding type of user profile synchronization.

---

**Note.** You should select the user profile synchronization type at the time of your implementation, after which you should restrict access to the Security PeopleCode Options page.

---

---

## **Implementing Standard User Profile Synchronization**

This section provides an overview of standard user profile synchronization and discusses how to set up a standard user profile synchronization.

When you implement standard user profile synchronization among databases, other than the standard user profile synchronization exceptions mentioned below, the subscribing databases have no control over the data that they receive and process.

All participating databases use the USER\_PROFILE service operation and the USER\_PROFILE.VERSION\_84 message during the publish and the subscribe processes.

This diagram shows the service operations and messages, and the way in which user profile data is published by and subscribed to by three PeopleSoft systems that are using standard user profile synchronization:

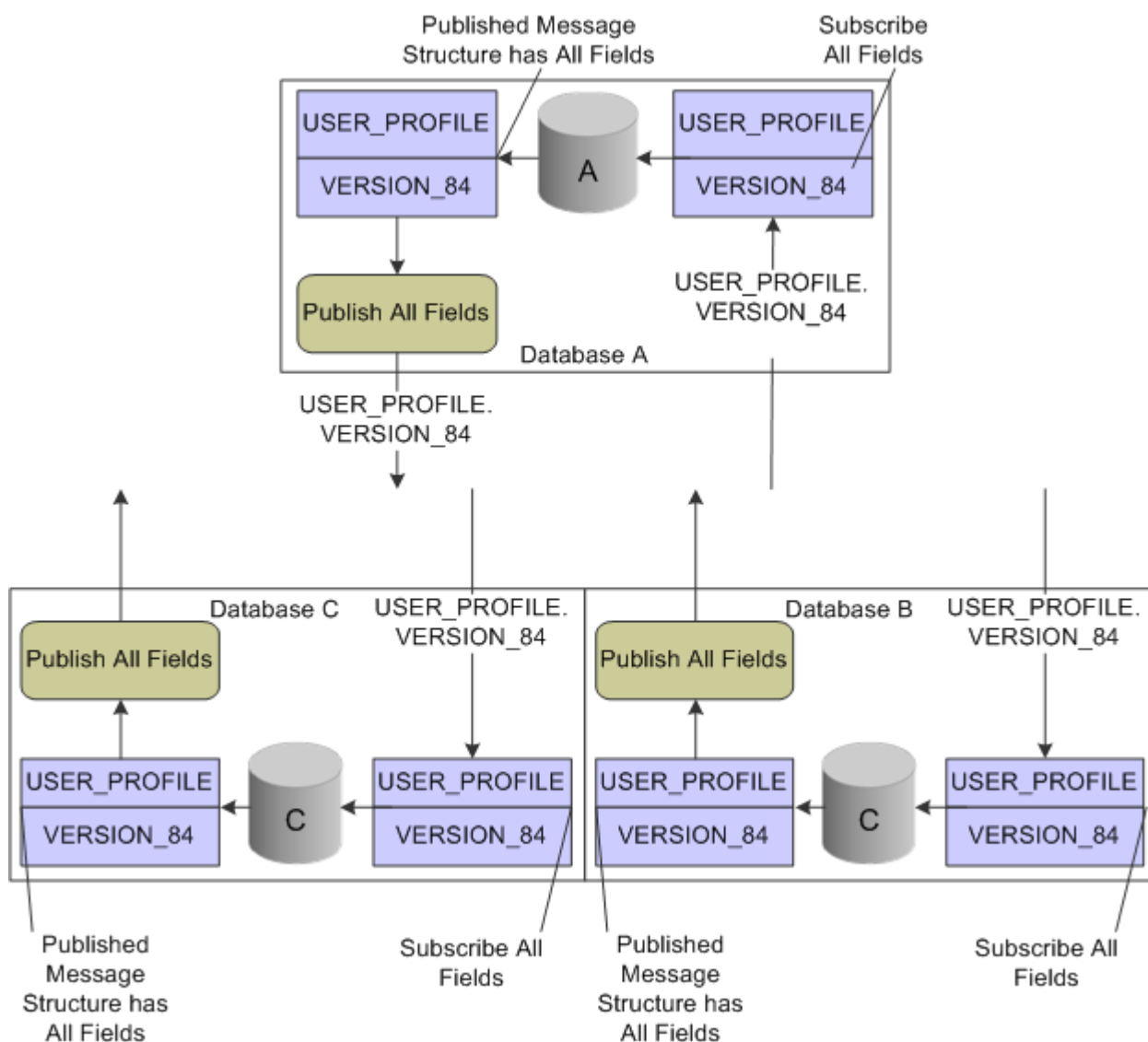


Diagram of the flow of user profile information as it uses standard synchronization among three PeopleSoft databases

### **Standard User Profile Synchronization Designed Exclusions**

Adding and deleting user profiles on the publishing node cause corresponding changes on the subscribing nodes. Modifying user profiles on the publishing node causes corresponding changes on the subscribing nodes with these exceptions:

- Changes to the primary email account are ignored if a primary email exists in the subscribing node.
- Changes to a user ID type are ignored if the user ID type is not valid on the subscribing node. Instead, the subscribing node inserts an ID type of *None* if the subscribing node does not have a row for *None* already.
- In general, changes that produce invalid field values in the subscribing node are ignored by the subscribing node.















- Release Levels

Because the PeopleTools table structures change between major releases (6.X to 7.X or 7.X to 8.X), you cannot transfer users between databases that run different versions of PeopleTools. Before starting the migration process, upgrade your source and target databases so the release levels match.

### ***Running the Scripts***

Complete the following procedure to run the user transfer 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, run the PeopleTools audits, including DDDAUDIT and SYSAUDIT, to check the consistency of your database.



## Chapter 7

# 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 authentication maps.
- Create user profile maps.
- Create role membership rules.
- Delete directory configurations.
- Enable signon PeopleCode for LDAP authentication.
- Use LDAP over SSL (LDAPS).
- View SSL for LDAP transaction setup examples.

---

**Note.** PeopleTools uses JNDI libraries only. JNDI requires no added installation as it is part of the standard PeopleTools installation.

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

---

---

## Understanding the PeopleSoft LDAP Solution

Three PeopleSoft-delivered technologies 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, which 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, which exposes the User Profiles component to PeopleCode.

The system uses it to programmatically manage a local cache of user profiles.

- Signon PeopleCode, which runs 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 topics in this chapter describe setting up the LDAP integration technology on your site. The tasks assume that an LDAP V3 compliant directory service is already installed, and that you intend 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. Directory-level users are not authenticated against the PSOPRDEFN table; they are authenticated by signon PeopleCode. Because signon PeopleCode only runs on the application server, LDAP authentication requires an application server. That is, LDAP authentication does not work for a 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 connectivity.

## Understanding LDAP Directory Configuration

The Configure Directory component (PSDSSETUP) 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 information 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	Definition 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 DN's 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 (PeopleTools, Security, Directory, Configure Directory. Click the Directory Setup tab).

Directory Setup
Additional Connect DN's
Schema Management
Test Connectivity

Directory ID: DOC\_SERVER

Description: Main Directory

Directory Product: Oracle Internet Directory

Default Connect DN: cn=admin,o=config

Password:

Server Name
Find | View All
First 1 of 1 Last

LDAP Server: 207.132.22.04

Port: 389
SSL Port:

Configure Directory - Directory Setup page





---

**Note.** The Schema Management page enables you to add PeopleSoft-delivered object classes and attribute types to your directory. If you add attributes and object classes using the Schema Management page, you must also delete them using this page.

---

<b>Apply</b>	Select this check box to apply the selected schema extension type to your directory.
<b>Type</b>	Displays the type of schema extension, either <i>Object Class</i> or <i>Attribute Type</i> .
<b>Name</b>	Displays the schema extension name.
<b>Object Identifier</b>	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.
<b>Revision</b>	Displays the number of times the schema extension was revised.
<b>Details</b>	Click to display details about the selected schema extension in the Details region at the bottom of the page.
<b>Select All</b>	Click to select all the schema extensions to apply to your directory.
<b>Deselect All</b>	Click to deselect every schema extension.
<b>Apply</b>	Click to apply the selected schema extensions to your directory.

### **Details**

When you click a schema extension 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, if any, are above this one in the hierarchy. 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 Connectivity**


Access the Test Connectivity page (select PeopleTools, Security, Directory, Configure Directory and click the Test Connectivity tab).



**Cache Schema**

---

\*Directory ID:  

Server Name:   Cache Schema Now [Process Monitor](#)

Cache Schema page

<b>Directory ID</b>	Select the directory ID to identify the directory that the system should connect to and retrieve schema information from.
<b>Server Name</b>	Search for the Process Scheduler server on which the Cache Schema process should run.
<b>Cache Schema Now</b>	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.
<b>Process Monitor</b>	After invoking the process, you can monitor the progress by clicking this link.

---

## Creating Authentication Maps

Use the Authentication page only if you are 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.

Authentication maps are used to specify the following information for LDAP authentication:

- The identity of all the LDAP servers to be searched and their credentials.
- The locations where the search has to be performed inside the LDAP.
- The attribute of the entries that must be matched with the signon user ID.

This section discusses how to:

- Defining an authentication map.
- Use the Search Attribute field in authentication maps.



<b>Anonymous Bind</b>	If all directory data required for authentication and user profile maintenance is visible to an anonymous connection, select this check box.
<b>Use Secure Socket Layer</b>	Select this option if you are implementing an SSL connection between PeopleSoft and the directory.  If you did not specify a port number for the directory, the system uses the default LDAPS port.
<b>Connect DN</b>	This value is the default connect DN that you specified on the Directory Setup page. To select one of the DN's specified on the Additional Connect DN's page, click the search button. <hr/> <b>Note.</b> If Anonymous Bind is selected, the Connect DN is ignored. <hr/>

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

<b>Search Base</b>	Enter the root of the directory information tree under which the system should search for user information.
<b>Search Scope</b>	Select the search scope for this search. Values are:  <i>Base:</i> Not applicable. You should not use <i>Base</i> on the authentication map.  <i>One:</i> The query searches only the entries one level down from the entry in the Search Base field.  <i>Sub:</i> The query searches the entire sub tree beneath the search base entry.







<b>Authentication Map</b>	Select the authentication map to associate with this user profile mapping. The server and connection information are taken from the authentication map.
<b>Status</b>	Displays the status of the selected user profile map. <hr/> <b>Note.</b> Only one user profile map should be active at any time. <hr/>
<b>Directory ID</b>	Displays the directory ID associated with the authentication mapping.
<b>User ID Attribute</b>	Specify the LDAP attribute used to populate the OPRID (user ID) field on PSOPRDEFN. <hr/> <b>Important!</b> If you specify a different value here than the Search Attribute value that you specified on the Authentication page, then users will not be able to switch to another application from the Go menu in PeopleSoft Windows clients such as Application Designer.  The second application expects to automatically authenticate a user with the value of %SignonUserId, the system variable that contains the user ID that was used to sign in. However, because the value of OPRID is different from the value of %SignonUserId, the authentication fails with an error message.  Users can still access any PeopleSoft Windows client by launching it directly and signing in using the same Search Attribute value for the user ID. <hr/>
<b>ID Type</b>	
<b>ID Type</b>	Enter the default ID type for new users, such as Employee ID, Customer ID, and so on. This field is similar to Symbolic ID.
<b>ID Type Attribute</b>	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.
<b>Default Role</b>	
<b>Use Default Role</b>	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 field 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.
<b>Role Name</b>	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.



<b>Attribute Name</b>	Add the name of the attribute as it is represented in your LDAP schema.
<b>Constant Value</b>	Appears only if you selected Use Constant Value.
<b>Always Update</b>	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.

Click the User Profile Property search button to select one of the following optional user profile properties:

<b>CurrencyCode</b>	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.
<b>EmailAddress</b>	Select if a user is part of your workflow system or you have other systems that generate emails for users.
<b>MultiLanguageEnabled</b>	Select if the user is set up to use PeopleSoft with multiple languages.
<b>NavigatorHomePagePermissionList</b>	Displays the homepage permission list that is associated with PeopleSoft Workflow (Navigator Homepage).
<b>PrimaryPermissionList</b>	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 details. PeopleSoft also determines mass change and definition security permissions from the primary permission list.
<b>ProcessProfilePermissionList</b>	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.
<b>RowSecurityPermissionList</b>	See explanation for the Primary Permission List field.
<b>SymbolicID</b>	If the symbolic ID is required for the user, select this option.
<b>UserDescription</b>	Typically, displays the name of the user, such as an employee name or a vendor name.
<b>UserIDAlias</b>	In some cases, the user ID is an alias in the form of an email address. If so, select this option.



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.

---

**Important!** You must keep the data within PeopleSoft consistent with any changes made to the structure or content of the external directory server, especially when you are 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

<i>Page Name</i>	<i>Definition Name</i>	<i>Navigation</i>	<i>Usage</i>
Role Policy	DSSECRULERULE	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 (PeopleTools, Security, Directory, Role Membership Rules).

Role Policy

Role Policy

Rule Name:PTNTLDAP-ALL-USERS

Description:

User Profile Map:QE\_TEST\_NOVELL

Directory ID:QE\_TEST\_NOVELL

Assign to Role

Directory Search Parameters

Search Base:dc=com

Search Scope:Sub

Build Filter

CustomizeFind

First1 of 1Last

	{	Attribute	Operation	Value	}	And/Or	
1	<input type="checkbox"/>	groupMembership	=	QETOOLS	<input type="checkbox"/>		<div>+ -</div>

Refresh Search FilterClear Search Filter

Search Filter:objectclass=person

Search Attributes

FindFirst1 of 1Last

Directory Attribute:

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.
-------------	--

Copyright © 1988, 2009, Oracle and/or its affiliates. All Rights Reserved.

153



## Search Attributes

**Directory Attribute** Select attributes that identify the user to add to this membership. The system searches only for members within the group that is 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

<i>Page Name</i>	<i>Definition Name</i>	<i>Navigation</i>	<i>Usage</i>
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 (PeopleTools, Security, Directory, Delete Directory Configuration).

**Delete Directory**Directory ID: `DOC_SERVER`

- ☐ Delete Associated Maps
- ☐ Delete Associated Searches
- ☐ Delete Associated Role Rules
- ☐ Delete Associated Entry Rules

**Delete Directory Configuration**

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** 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

Access the Address Book page (PeopleTools, Security, Directory, Workflow Address Book).





















1. 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 &EXEC_RSLT;
&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 principle applies to any transaction.

---

2. Change the SSL setting to indicate that SSL should be used. For example: `&LDAP_SEARCH_1.SSL = "YES";`

Note these points:

- The SSL setting in PeopleCode takes priority over the setting in Application Designer. For example, setting *YES* in Application Designer and *NO* in PeopleCode will result in a non-SSL transaction.
- 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.
- Whenever you enable or disable sign-on PeopleCode, reboot the application server domain.
- Whenever you install or uninstall a certificate, reboot the application server.



## Chapter 8

# 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:

<b>Function</b>	<b>Exec Auth Fail</b>	<b>Description</b>
WWW_Authentication	Not Required	<p>Applies when you want the browser to pass the client certificate to the web server for authentication by mutual authentication Secure Sockets Layer (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.</p> <p>The function performs the following:</p> <ol style="list-style-type: none"> <li>1. Extracts the user's distinguished name (DN) from the client certificate passed to the application server by the HTTP server.</li> <li>2. Sets a global variable to the DN for a subsequent call to the LDAP_ProfileSynch function.</li> <li>3. Converts the DN to a PeopleSoft user ID and sets the current user context.</li> </ol>
LDAP_Authentication	Required	<p>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.</p> <p>This function performs the following:</p> <ol style="list-style-type: none"> <li>1. Searches the directory for all entries that match the entered user name.</li> <li>2. Attempts to bind to the directory for each found DN using the entered password.</li> <li>3. Sets a global variable to the bound DN for a subsequent call to LDAP_ProfileSynch.</li> <li>4. Converts the DN to the appropriate PeopleSoft Username and sets the current user context.</li> </ol>
SSO_Authentication	Not Required	<p>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).</p> <p>This function performs the following:</p> <ol style="list-style-type: none"> <li>1. Converts the PeopleSoft User ID to a DN.</li> <li>2. Sets a global variable for a subsequent call to LDAP_ProfileSynch.</li> </ol>

<i>Function</i>	<i>Exec Auth Fail</i>	<i>Description</i>
LDAP_ProfileSynch	Not Required	<p>Applies in 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 &amp;global_DN has been initialized by one of the previous authentication functions.</p> <p>Remember that regardless of how a user is authenticated, each user populates a row in PSOPRDEFN to which applications can refer during transactions (if necessary). The LDAP_ProfileSynch updates that row in PSOPRDEFN (or user profile cache) with the most current information.</p> <p>As delivered, this function performs the following:</p> <ol style="list-style-type: none"> <li>1. Retrieves the LDAP entry specified by &amp;global_DN.</li> <li>2. Either creates or updates the corresponding PeopleSoft user profile.</li> </ol> <p><b>Note.</b> One of the XXX_Authentication functions needs to be carried out prior to running LDAP_ProfileSynch.</p> <p>PeopleSoft provides 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.</p> <p>See <a href="#">Chapter 8, "Employing Signon PeopleCode and User Exits," LDAP_ProfileSynch Considerations, page 173.</a></p>

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 web site than users of the other authentication methods.





- 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 Pure Internet Architecture, 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 that the user types on 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.

---



<b>PeopleCode Function</b>	<b>Description</b>
See <i>Enterprise PeopleTools 8.50 PeopleBook: PeopleCode Language Reference</i> , "System Variables," %PSAuthResult.	Returns the result (boolean) of PeopleSoft authentication.
See <i>Enterprise PeopleTools 8.50 PeopleBook: PeopleCode Language Reference</i> , "PeopleCode Built-in Functions," SetAuthenticationResult.	Verifies customers who log on to the system even if the PeopleSoft authentication fails.
See <i>Enterprise PeopleTools 8.50 PeopleBook: PeopleCode Language Reference</i> , "System Variables," %SignonUserId.	User ID value entered by the user on the Signon page. This applies to Pure Internet Architecture and Windows signon.
See <i>Enterprise PeopleTools 8.50 PeopleBook: PeopleCode Language Reference</i> , "System Variables," %SignOnUserPswd.	User password value the user entered at the Signon page. This value is encrypted. This applies to Pure Internet Architecture and Windows signon.
See <i>Enterprise PeopleTools 8.50 PeopleBook: PeopleCode Language Reference</i> , "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 Pure Internet Architecture.

---

**Note.** Do not use %SwitchUser in Signon PeopleCode.

---

## Enabling Signon PeopleCode

Access the Signon PeopleCode page (PeopleTools, Security, Security Objects, Signon PeopleCode).











- 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.

---

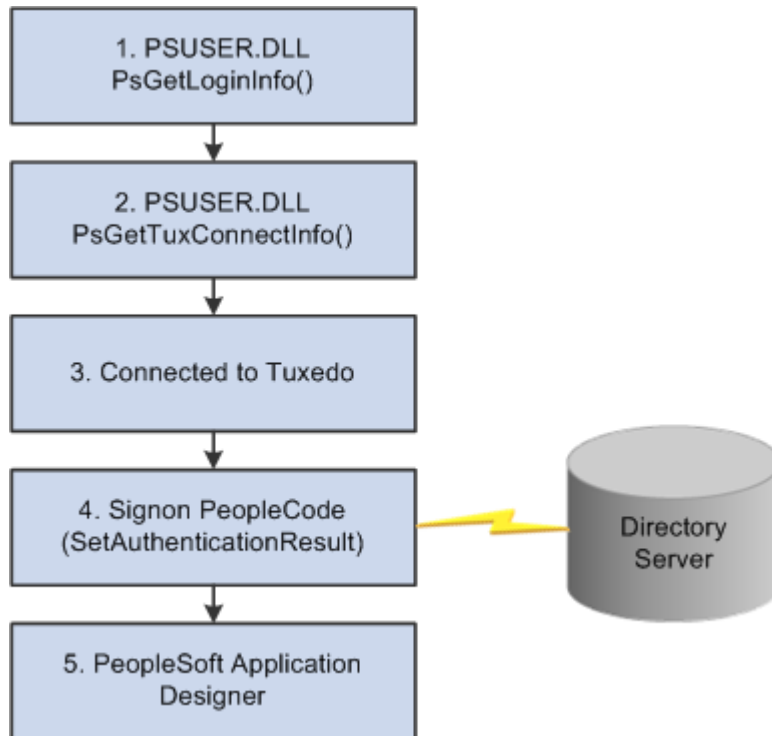
## Signing In Through the Web Server

This section provides a step-by-step example of the steps that occur within the system after you have it configured to trust authentication performed at the web server level:

<b>Step</b>	<b>Component</b>	<b>Description</b>
1	Browser	The user clicks a link to the PeopleSoft application, for example <a href="http://serverXYZ/servlets/psportal/peoplesoft8/?cmd=start">http://serverXYZ/servlets/psportal/peoplesoft8/?cmd=start</a> .
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.  The method the system uses to authenticate the user and the method the web server uses to add 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.
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.  <b>Note.</b> The password verification prevents a sophisticated hacker from connecting to the application server directly and carrying out service requests.



With the three-tier Microsoft 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:



Microsoft 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:





All parameters except bSubsequentSignon, which is Boolean, are of the data type CHAR and are defined as follows:

<b>Parameter Name</b>	<b>Description and Values</b>
BSubsequentSignon	An initial or subsequent signon. Values are: FALSE: Initial signon. User just started the PeopleSoft system. TRUE: Subsequent signon. User probably selected an item from the Go menu in the Development Environment (PSIDE.EXE).
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 change to either.
szDBType	Database type. Values are: DB2: DB2 z/OS through Centura Gateway. DB2ODBC: DB2 z/OS 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:



## Chapter 9

# Implementing Single Signon

This chapter provides an overview of single signon and discusses how to:

- Implement PeopleSoft-only single signon.
- Implement Oracle Access Manager as the PeopleSoft single signon solution.

---

## Understanding Single Signon

This section discusses:

- Single signon options.
- PS\_TOKEN.

## Understanding Single Signon Options

Single signon refers to the ability of users to navigate freely within a system of multiple applications after only being authenticated once. There are two different ways to configure single signon, depending on the participating applications that you have installed. The following table displays the single signon options.

<i>Single Signon Option</i>	<i>Description</i>
PeopleSoft-only	<p>This option enables single signon only between multiple PeopleSoft applications, such as PeopleSoft Human Capital Management and PeopleSoft Customer Relationship Management. After a user is authenticated by one PeopleSoft application, an in-memory value gets set in the browser (PS_TOKEN cookie) that the next PeopleSoft application uses for a user credential.</p> <p>If you have only PeopleSoft applications, use this option.</p> <p><b>Note.</b> This option is the same single signon feature offered in previous PeopleSoft releases.</p> <p>See <a href="#">Chapter 9, "Implementing Single Signon," Implementing PeopleSoft-Only Single Signon, page 191.</a></p>





- Single signon configuration considerations.
- Single signon configuration examples.
- Making the PeopleSoft single signon token secure.
- Using the single signon API.
- Configuring single signoff.

---

**Note.** In this configuration, you must create PeopleSoft node definitions for each of the participating applications. You can run any of the participating applications on Oracle WebLogic or IBM WebSphere. You can use passwords or digital certificates for single signon authentication.

---

## Understanding PeopleSoft-Only Single Signon

PeopleSoft software 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.

---

**Note.** The PeopleSoft-only single signon solution applies only to PeopleSoft applications.

---

After the first application server/node authenticates a user, the system delivers a web browser cookie containing an authentication token (PS\_TOKEN). PeopleSoft 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 users automatically so they don't have to complete the signon process repeatedly.

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 to prevent tampering.

---

## Working with the Single Signon Page

Access the Single Signon page (PeopleTools, Security, Security Objects, Single Signon).



**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.

Node Definitions

Connectors

Portal

WS Security

Routings

Node Name:

QE\_LOCAL

Copy Node

\*Description:

QE\_LOCAL

Rename Node

Node Type:

PIA

☒ Default Local Node

\*Authentication Option:

Password

☒ Local Node

☒ Active Node

☐ Non-Repudiation

☐ Segment Aware

Node Password:

\*Default User ID:

QEMGR

Hub Node:

Master Node:

Company ID:

IB Throttle Threshold:

Image Name:

Codeset Group Name:

Save

Contact/Notes

Properties

Node Definitions page

The two options related to single signon are:



1. Log on to the portal master.
2. Navigate to PeopleTools, Portal, Node Definitions.
3. Select the QE\_LOCAL default local Node.
4. For Authentication Option, choose *Certificate* from the drop-down list.
5. Make sure PTNTAS05 is defined as Remote Node.

### **Step 2: Define the Content-side (slave) to recognize Portal to establish the trust**

To Define the Content-side (slave) to recognize Portal to establish the trust:

1. Log on to the Content-side Portal (slave).
2. Select PeopleTools, Portal, Node Definition.
3. Make sure that the QE\_LOCAL node is defined as a remote Node, and click the QE\_LOCAL remote Node.
4. For Authentication Option, choose *Certificate* from the drop-down list.
5. Select PeopleTools, Security, Security Objects, Single Signon and confirm that the QE\_LOCAL message node appears in list of trusted nodes in the Trust Authentication Tokens issued by these Nodes group box.

### **Step 3: Create Private Key and Install Digital Certificate for Local Node**

To Create Private Key and Install Digital Certificate for Local Node:

1. Login to the Portal.
2. Select PeopleTools, Security, Security Objects, Digital Certificates.

---

**Note.** Make sure that Root CA with Issuer Alias = PeopleTools is available.

---

3. Click the Add a new row button (+).
4. In the Type field, select *Local Node*.
5. Enter *QE\_LOCAL* in the Alias field.
6. In the Issuer Alias Field, select *PeopleTools*.
7. Click the Request link.
8. Fill in the form.

---

**Note.** Use Key Size=512 bits for UNIX Application Server Common Name = QE\_LOCAL

---

9. Click the OK button.
10. Select all of the text and copy the request.
11. Go to the certificate provider and select Request a certificate.

12. Select "Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file."
13. Paste the request, and click submit and download.
14. Open the certificate with a text editor, such as c:\temp\newcert.
15. Select All and copy the certificate.
16. Return to Portal - Digital Certificate page.
17. Click Import.
18. Paste the certificate into the text box.

---

**Note.** Make sure no space after END CERTIFICATE, otherwise, you are not allowed to save. Click the OK button .

---

#### ***Step 4: Install Digital Certificate for Remote Node on Content-Side.***

To Install Digital Certificate for Remote Node on Content-Side:

1. Log onto Content-side (Slave) Portal.
2. Navigate to PeopleTools, Security, Security Objects, Digital Certificates.
3. Click Add a new row button (+).
4. Select Remote Node, Type QE\_LOCAL, and select Issuer Alias = *PeopleTools*.
5. Click Import.
6. Open c:\temp\newcert with a text editor and copy and paste the digital certificate into the empty text box.
7. Click OK.

## **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-only single signon, this section presents an example of how the PeopleSoft—only 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***

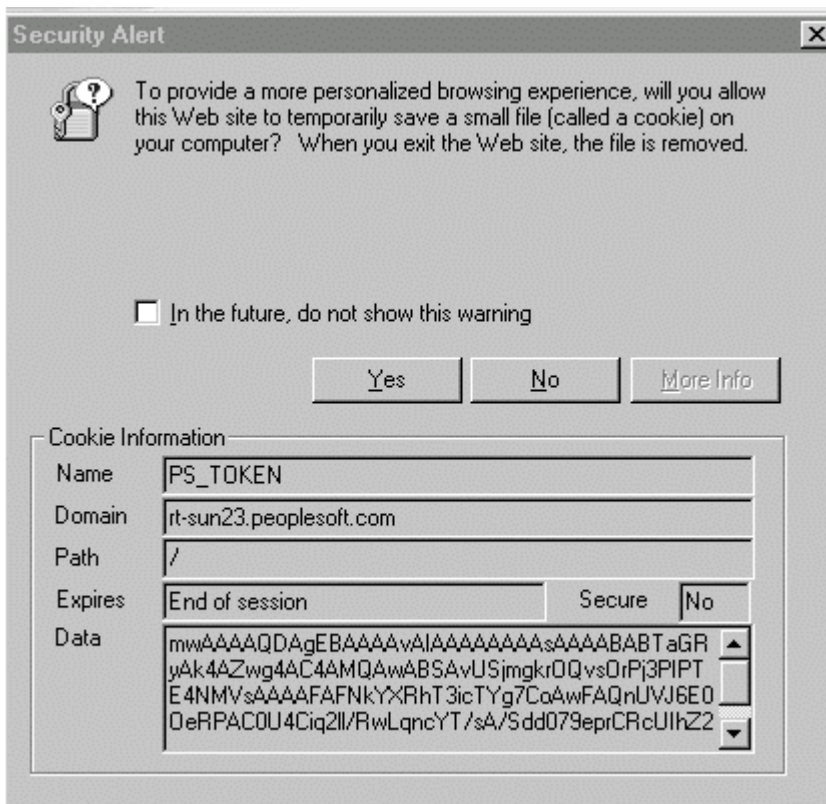
The following occurs:

- If the signon attempt to the HCM application server is successful, the application server generates a single signon token.
- 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 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 because 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:

- Is this a 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 timeout 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.** You should use digital certificate authentication when implementing single signon.

---

## **PeopleSoft-Only 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 Pure Internet Architecture 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 Pure Internet Architecture 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 Pure Internet Architecture 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 Pure Internet Architecture 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 Pure Internet Architecture, 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 8.50 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 example, 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`.

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 software, 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 Pure Internet Architecture-to-Pure Internet Architecture (iClient-to-iClient) single signon.

---

## PeopleSoft-Only 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 timeout 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.

You should use 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 10, "Working with SSL and Digital Certificates," page 213](#) and [Chapter 7, "Employing LDAP Directory Services," page 135](#).

### ***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-Only 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 SSL site, and assume that web server Y is not. In these situations, many organizations 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 identify 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 provides a component interface named PRTL\_SS\_CI that enables external applications to seamlessly integrate a single signon solution with the PeopleSoft portal applications. This ensures that users who have already signed in to the portal don't have to sign in 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 software.

---

**Note.** Due to constraints imposed by the PeopleCode **SwitchUser** built-in function, PRTL\_SS\_CI does not work properly when called from PeopleCode. Only external applications, such as Java, Visual Basic, and C/C++ programs, can access PRTL\_SS\_CI.

---

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.

<b>Step</b>	<b>Description</b>
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.
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 the PeopleSoft system 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.

---

**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 PeopleSoft-Only Single Signoff

In addition to single signon, the PeopleSoft system 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`.





9. WebLogic users must disable basic authentication.

Access <PIA\_HOME>\web\serv\peoplesoft\config> and modify the config.xml file by adding this tag:  
<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>

For Example:

```
<security-configuration xmlns:xacml="http://www.bea.com/ns/weblogic/90/security/xacml">
  <name>peoplesoft</name>
  <realm>myrealm</realm>

  .....

  <credential-encrypted>{3DES}d0a1fqoTbX1GUq7RQPhDNDgkWkIZhzWVlEXkmSMbt9Uuf1FfVZIrJC</credential-encrypted>
  <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>

  </security-configuration>
```

10. Stop and restart the application server, web server, and HTTP server.

## Chapter 10

# Working with SSL and Digital Certificates

This chapter provides an overview and discusses how to configure digital certificates.

---

## Understanding SSL and Digital Certificates

The PeopleSoft system 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 software 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.

## 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. PeopleTools use the inherently supported SSL implementation provided with JRE.<sup>TM</sup>

The PeopleSoft system 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.

<b><i>Technology</i></b>	<b><i>How HTTPS/SSL is Implemented</i></b>
PeopleSoft Portal Solutions	Secure page transport — Uses web server platform to provide server side SSL.  Secure access to remote content providers — Application server uses JRE to provide the client side of SSL connection to gateway. Uses web server platform to provide server side SSL.

<i>Technology</i>	<i>How HTTPS/SSL is Implemented</i>
PeopleSoft Integration Broker (application messaging)	Secure message transport to remote nodes — Application server uses JRE 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 JRE 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. You should save the certificate to a Microsoft Windows workstation, right click on it using Microsoft 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 that you have in place.

---



---

**Note.** Currently, root CA key size is limited to 1024 bits.

---

To view details regarding a particular certificate, click Details.

<b>Type</b>	<p>Select the type of certificate.</p> <p><i>Local Node.</i> Select this option when you are setting up a local node for the PeopleSoft messaging system (PeopleSoft Integration Broker).</p> <p><i>Root CA.</i> Select this when you are adding a new Root CA to your key store.</p> <p><i>Remote.</i> Select this option when you are setting up a remote node for the PeopleSoft messaging system (PeopleSoft Integration Broker).</p>
<b>Alias</b>	Enables you to add a custom alias for identification purposes.
<b>Issuer Alias</b>	Contains the alias of the authority that issued the certificate.
<b>Valid To</b>	Shows how long the certificate is valid for use.
<b>Detail</b>	<p>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.</p> <hr/> <p><b>Note.</b> Depending on the type of certificate you're adding, this link might be displayed as Add Root, Import, or Request.</p> <hr/>

---

**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).

---



## Chapter 11

# Working with Web Service Security (WS-Security)

This chapter contains an overview of WS-Security and discusses how to:

- Implementing WS-Security for WSRP.
- Implementing WS-Security for PeopleSoft Integration Broker.

---

## Understanding WS-Security

By implementing the WS-Security standard, PeopleSoft provides the ability to leverage emerging XML security technologies to address web services security requirements. WS-Security provides:

- A way for applications to construct secure SOAP message exchanges.
- A general-purpose mechanism for associating security tokens with SOAP messages.
- XML message integrity and confidentiality.

By providing WS-Security capabilities, you can leverage the standard set of SOAP extensions, that you use when building secure web services, to implement message content integrity and confidentiality. WS-Security provides a way to insert and convey security tokens in SOAP messages. The ability to leverage WS-Security standards provides for better interoperability and improved usability, enabling the implementation of robust security within a WSRP-capable environment. The solutions being provided through the PeopleSoft WS-Security implementation include:

- Enable web service security between WSRP consumer and producer.

The web services consumer passes the appropriate identification to a producer as part of the SOAP message, so that producer can verify the identity in order to execute requested web services on behalf of the user without requiring a user to log in. Integration between web services consumer and producer feature is currently supported in PeopleSoft WSRP Portal, PeopleSoft Integration Broker, and BPEL product.

- SOAP message integrity. Ensuring that messages have not been tampered with
- SOAP message confidentiality. Guaranteeing that messages are protected against eavesdroppers.

The WS-Security Username Token Profile defines a standard way to associate user ID and password information in the SOAP messaging for web services interoperability.

The Security Assertion Markup Language (SAML) token uses assertions to define a standard way to associate common information such as issuer ID, NotBefore and NotOnOrAfter conditions, assertion ID, subject, and so on.

The OASIS WS-Security specification is the open standard for web services security. Its goal is to let applications secure SOAP message exchanges by providing encryption, integrity, and authentication support. It provides authentication support for SOAP messaging. WS-Security offers these general-purpose mechanisms for associating security tokens with message content:

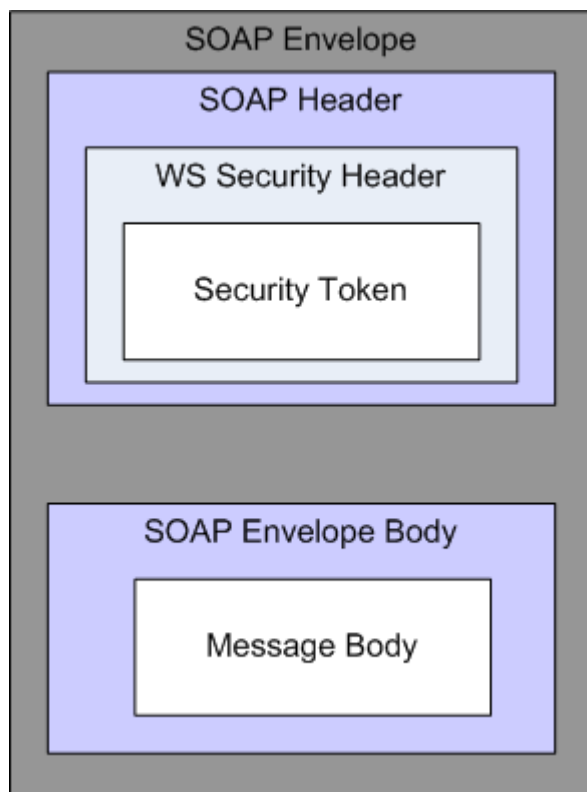
- Username token.
- SAML token.

---

**Note.** PeopleSoft provides multiple levels of security for WSRP. These levels, or options, are discussed in the following chapter. PeopleSoft recommends that you determine the level that is appropriate for your needs before implementing WS-Security. Using SSL connections to secure transmissions may be sufficient.

---

This figure shows how WS-Security inserts and conveys security tokens in SOAP messages:



WS-Security SOAP Message Structure

---

## Implementing WS-Security for WSRP

If using the web services for remote portals technology, you implement WS-Security.

See *Enterprise PeopleTools 8.50 PeopleBook: PeopleTools Portal Technologies*, "Configuring WS-Security For WSRP Consumption and Production."

---

## Implementing WS-Security for PeopleSoft Integration Broker

If using PeopleSoft Integration Broker, you configure WS-Security to ensure secure transmissions.

See *Enterprise PeopleTools 8.50 PeopleBook: PeopleSoft Integration Broker Administration*, "Setting Up Secure Integration Environments."



## Chapter 12

# Encrypting Text With PSCipher

This chapter contains an overview and discusses how to:

- Use the PSCipher utility.
- Generate a unique encryption key.
- Update the encryption key on Oracle WebLogic.
- Update the encryption key on IBM WebSphere.
- Secure the external key file.

---

## Understanding the Triple Data Encryption Standard (DES) Encryption Implementation

The PSCipher utility provides Triple DES encryption (also 3DES) for increased data security. When you install Enterprise PeopleTools on your application servers and web servers, a default, Triple DES encryption key is provided. If your site decides to use the default key, no further configuration of your system is required to implement Triple DES encryption. However, if your site requires or desires a unique encryption key, you can generate a unique key using the PSCipher command line utility as described in this chapter.

The version of the default encryption key is version 1.1, or {V1.1}. If you generate a unique key, the current version used by the system would be {V1.2}. Each time you generate a new key, the system increments the current version number.

---

## Using the PSCipher Utility

The PSCipher feature encrypts and decrypts text used in your PeopleSoft system. System administrators interact with PSCipher through a Java, command line utility located on the web server, which enables you to encrypt text, such as user IDs and passwords, stored in configuration files. PSCipher also involves a runtime element, running on the application server, that decrypts the encrypted text. The runtime element requires no user interaction.

In previous releases, PSCipher was used, for example, to secure the node IDs and node passwords used in conjunction with PeopleSoft Integration Broker configurations. You can now use the PSCipher command line utility to encrypt (with Triple DES) a variety of text values stored in various configuration files throughout your system. In addition, PSCipher also provides:

- Key generation: You can generate unique encryption keys if you do not want to use the default key.

- Version maintenance: The key file maintains a version history of all previous versions of the key file, which enables text encrypted with a previous version to be decrypted.

---

**Note.** PSCipher decrypts text encrypted in previous releases. For example, PSCipher in Enterprise PeopleTools 8.49 supports text encrypted with PSCipher in Enterprise PeopleTools 8.46.

---

To encrypt text, you submit text values in the form of arguments that PSCipher encrypts and then displays in its encrypted form. Suppose you needed to encrypt a user ID of "HRDMO" and a password of "DMOPSWD". You would submit these values to PSCipher as follows:

```
...\pscipher HRDMO
```

and

```
...\pscipher DMOPSWD
```

PSCipher returns the encrypted form of these submitted text values, which you can then copy to a configuration file to assign to a configuration parameter.

---

**Note.** This same procedure will need to be applied whenever you intend to encrypt text using PSCipher. Note that in the following sections of this document it is assumed that you understand how to encrypt the text value.

---

---

## Generating a Unique Encryption Key

You use the PSCipher Java utility's `buildkey` command to build new Triple DES encryption keys. The `buildkey` command adds a new Triple DES encryption key stored in the `psvault` file (the key file). If you generate new versions of the key file, the system appends the new version of the key to the end of the key file.

To invoke the command on a Windows server, change to the directory where PSCipher resides and enter:

```
...\pscipher -buildkey
```

To invoke the command on UNIX, change to the directory where PSCipher resides and enter:

```
.../PSCipher.sh -buildkey
```

Select one web server in your system to generate the new version of the key file. The `pscipher.bat` and `PSCipher.sh` utilities only run in the Java environment of the web server. After you have created the new key file, you then copy the new version of `psvault` from the initial server to the appropriate directories on all the appropriate servers in your system. The `psvault` file is stored in different directories depending on your web server vendor (as described in the following sections). On the application server the `psvault` file resides in `<PS_HOME>\secvault`.

---

**Note.** If you are not using the default encryption key and you have generated a unique encryption key, note that each time you add a new server to your system, you will need to copy the key file to the appropriate location on that server. For example, if you are using the default key version (`{V1.1}`), any server you add to the system and install PeopleTools 8.50 on will also have the default key version (`{V1.1}`). As such, no further steps are required. However, if you have generated a new key, giving the version number a value of `{V1.2}` or greater, then you need to make sure to copy that key file to the added server(s). Also, each time you update the key, you need to ensure that the new version of the key file is copied to the additional servers in your system.

---

---

**Warning!** When you upgrade to new PeopleTools releases, as in PeopleTools 8.48 to PeopleTools 8.50, you will need to backup any modifications you have made to the key file using PSCipher in the previous release and reapply that same key file to the appropriate servers onto which you have installed the new PeopleTools release.

---

## Updating the Encryption Key on IBM WebSphere

On IBM WebSphere, PSCipher.bat and psvault key file are stored in the following location:

<PIA\_HOME>\webserve\<Node\_Server>\<APPLICATION>.ear

## Generating the Encryption Key on IBM WebSphere

To update the encryption key:

1. Run <PIA\_HOME>\webserve\<Node\_Server>\<APPLICATION>.ear PSCipher -buildkey to create a new key in the key file.

For example,

```
c:\>cd ptinstall\webserve\DS9Node_DS9Node_server1\peoplesoft.ear
c:\ptinstall\webserve\DS9Node_DS9Node_server1\peoplesoft.ear>PSCipher.bat -buildkey
Your environment has been set.
A new key of version {V1.2} is generated successfully
```

2. Copy <PIA\_HOME>\webserve\<Node\_Server>\<APPLICATION>.ear\psvault to the equivalent location on all other web server hosts and to <PS\_HOME>\secvault\psvault on all application servers in your system.
3. Modify the encrypted text fields as described in the following sections.

## Updating the Web Profile

The configuration.properties file is located in the following directory:

<PIA\_HOME>\webserve\<Node\_Server>\<APPLICATION>.ear\PORTAL\WEB-INF\psftdocs\ps\

The following encrypted text values in the configuration.properties file need to be updated:

```
WebUserId={V1.1}et5LM5/C2fQPWt5cztag==
WebPassword={V1.1}et5LM5/C2fQPWt5cztag==
```

Submit the values for these properties to PSCipher, and copy the generated encrypted text to the WebUserID and WebPassword properties in the configuration.properties file, overwriting any previous value assigned to the property.

## Updating the Integration Gateway

On the Integration Gateway, you need to modify the following files:

- gatewayUserProfile.xml
- integrationGateway.properties

The gatewayUserProfile.xml file is located in the following directory:

```
<PIA_HOME>\webserv\<Node_Server>\<APPLICATION>.ear\PSIGW\WEB-INF\
```

In the gatewayUserProfile.xml file, update the following text value:

```
<password>{V1.1}GD9k1UFw8760HVaqeT4pkg==</password>
```

---

**Note.** There can be more than one password field in this file. There could be different `<password></password>` entries for different users. You should use PSCipher to encrypt all `<password></password>` entries.

---

Submit the values for these properties to PSCipher, and copy the generated encrypted text to the `<password></password>` entry in the gatewayUserProfile.xml file, overwriting any previous value.

The integrationGateway.properties file is located in the following directory:

```
<PIA_HOME>\webserv\<Node_Server>\<APPLICATION>.ear\PSIGW\WEB-INF\
```

Update the following text values stored in the integrationGateway.properties file.

---

**Note.** If you are not currently assigning a value to one of the following properties, you don't need to supply a value.

---

- ig.isc.password=
- ig.isc.\$NODENAME.password=
- #ig.certificatePasswd=
- secureFileKeystorePasswd=
- #ig.jms.JMSTargetConnector.JMSProvider.Password=
- # ig.jms.Queue1.Password=
- # ig.jms.Topic1.Password=
- #ig.jms.Topic1.NodePassword=

Submit the values for these properties to PSCipher, and copy the generated encrypted text to the corresponding entries in the integrationGateway.properties file, overwriting any previous value.

## Updating WSRP/WSS

You need to update the wss.properties file used for Web Services Remote Portal (WSRP) and Web Services Security (WSS).

The wss.properties file needs to be updated in the following locations:

- ...applications/peoplesoft/PSIGW.war\WEB-INF\classes (for Weblogic)

- `<PIA_HOME>\webserve\<Node_Server>\<APPLICATION>.ear\PSIGW.war\WEB-INF\classes` (for Websphere)

Update the following text entry in the `wss.properties` file in both locations:

```
org.apache.ws.security.crypto.merlin.keystore.password=
```

Submit each password value to PSCipher, and copy the generated encrypted text to the corresponding entries in the `wss.properties` file, overwriting any previous value.

---

## Updating the Encryption Key on Oracle WebLogic

On Oracle WebLogic, PSCipher.bat and psvault are stored in the following location:

```
<PIA_HOME>\webserve\<DOMAIN>.
```

## Generating the Encryption Key on Oracle WebLogic

To update the encryption key:

1. Run `<PIA_HOME>\webserve\<DOMAIN>\PSCipher -buildkey` to create a new key in the key file.

For example,

```
c:\cd PIA_HOME\webserve\peoplesoft
c:\PIA_HOME\webserve\peoplesoft>PSCipher.bat -buildkey
Your environment has been set.
A new key of version {V1.2} is generated successfully
```

2. Copy `<PIA_HOME>\webserve\<DOMAIN>\psvault` to the equivalent location on all other web server hosts and to `<PS_HOME>\secvault\psvault` on all application servers in your system.
3. Modify the encrypted text fields as described in the following sections.

## Updating the Web Profile

The `configuration.properties` file is located in the following directory:

```
<PIA_HOME>\webserve\<DOMAIN>\applications\peoplesoft\PORTAL\WEB-INF\psftdocs
```

The following encrypted text values in the `configuration.properties` file need to be updated:

```
WebUserId={V1.1}et5LM5/C2fQPWt5cztagg==
WebPassword={V1.1}et5LM5/C2fQPWt5cztagg==
```

Submit the values for these properties to PSCipher, and copy the generated encrypted text to the `WebUserID` and `WebPassword` properties in the `configuration.properties` file, overwriting any previous value assigned to the property.

## Updating the Integration Gateway

On the Integration Gateway, you need to modify the following files:

- gatewayUserProfile.xml
- integrationGateway.properties

The gatewayUserProfile.xml file is located in the following directory:

<PIA\_HOME>\websrv\<DOMAIN>\applications\peoplesoft\PSIGW\WEB-INF\

In the gatewayUserProfile.xml file, update the following text value:

```
<password>{v1.1}GD9klUFw8760HVaqeT4pkg==</password>
```

---

**Note.** There can be more than one password field in this file. There could be different <password></password> entries for different users. You should use PSCipher to encrypt all <password></password> entries.

---

Submit the values for these properties to PSCipher, and copy the generated encrypted text to the <password></password> entry in the gatewayUserProfile.xml file, overwriting any previous value.

The integrationGateway.properties file is located in the following directory:

<PIA\_HOME>\websrv\<DOMAIN>\applications\peoplesoft\PSIGW\WEB-INF

Update the following text values stored in the integrationGateway.properties file.

---

**Note.** If you are not currently assigning a value to one of the following properties, you don't need to supply a value.

---

- ig.isc.password=
- ig.isc.\$NODENAME.password=
- #ig.certificatePasswd=
- secureFileKeystorePasswd=
- #ig.jms.JMSTargetConnector.JMSProvider.Password=
- # ig.jms.Queue1.Password=
- # ig.jms.Topic1.Password=
- #ig.jms.Topic1.NodePassword=

Submit the values for these properties to PSCipher, and copy the generated encrypted text to the corresponding entries in the integrationGateway.properties file, overwriting any previous value.

## Updating WSRP/WSS

You need to update the `wss.properties` file used for Web Services Remote Portal (WSRP) and Web Services Security (WSS).

The `wss.properties` file needs to be updated in the following locations:

- `<PIA_HOME>\webserv\<DOMAIN>\applications\peoplesoft\PORTAL\WEB-INF\classes\`
- `<PIA_HOME>\webserv\<DOMAIN>\applications\peoplesoft\pspc\WEB-INF\classes\`

Update the following text entry in the `wss.properties` file in both locations:

`org.apache.ws.security.crypto.merlin.keystore.password=`

Submit each password value to PSCipher, and copy the generated encrypted text to the corresponding entries in the `wss.properties` file, overwriting any previous value.

---

## Securing the External Key File

The encryption key used by PSCipher is stored in a key file named `psvault`. This file is critical to your system security. It is very important to protect this file using *at least* the concepts discussed in this section.

## Setting up Operating System File Security

The key file should be secured and protected by your operating system with the appropriate file access permissions on all platforms. The recommended file access permissions are:

- File 'read' access for only the administrators that need to run the PSCipher command-line utility to encrypt text.
- File 'read' access for the only the administrators that need to start the application servers and web servers.
- File 'write' access for only the administrators that need to run PSCipher `–buildkey` to create a new PSCipher key.

## Backing Up the Key File

It will be a time-consuming task to recover your system if you accidentally damage or delete the key file. Therefore, it is important to save a backup of your key file. It is recommended that every time you build a new key that you backup your latest key file to a safe location.

---

**Note.** You only need to keep the latest version of your key file for your backup. The latest version contains a version history of previous keys.

---



## Chapter 13

# Securing Data with PeopleSoft Encryption Technology

This chapter provides overviews of data security, PeopleSoft Encryption Technology (PET), 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 PeopleSoft Encryption Technology, 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.

Privacy is normally implemented with some type of encryption.

- Integrity – keeping transmitted data intact.

Integrity can be accomplished with simple checksums, or better, with more complex cryptographic checksums known as one-way hashes. Many times, checksums are combined with a type of asymmetric cryptography to produce digital signatures. These signatures, when verified, assure you that the data has not changed.

- Authentication – verifying the identity of an entity that is transferring data.

Authentication can also be accomplished using 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 Encryption Technology.

### **Symmetric Encryption**

Symmetric encryption involves both encrypting and decrypting a piece of data using the same key, which is stored on the sending and receiving entities. 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 possess 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 possibility 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 PeopleSoft Encryption Technology

*PeopleSoft Encryption Technology* 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 application data, giving you strong cryptography with the flexibility to change and grow, by incrementally acquiring stronger and more diverse algorithms for encrypting data.

### PeopleSoft Encryption Technology 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 PeopleSoft Encryption Technology 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.

### PeopleSoft Encryption Technology Development

The functional elements of PeopleSoft Encryption Technology 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*.

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.

---

## 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 8.50 PeopleBook: System and Server Administration*, "Setting Application Server Domain Parameters."

- In the Oracle 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 8.50 PeopleBook: PeopleSoft Process Scheduler*, "Using the PSADMIN Utility."

---

**Note.** The path added must be the directory which contains the .dll and .lib files. There can be no intermediate subdirectory between the path setting and these files.

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 comprises 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 are 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 13, "Securing Data with PeopleSoft Encryption Technology," Defining Encryption Profiles, page 251

*Enterprise PeopleTools 8.50 PeopleBook: PeopleCode API Reference*, "Crypt Class"

## Internal Algorithms

Support for the following algorithms is provided by the PeopleCode crypt class. They are automatically available for inclusion in your algorithm chains.

<b>Algorithm</b>	<b>Description</b>
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).
PSUnicodeToAscii_Generic_ENC	Convert Unicode text to ASCII  <b>Note.</b> Use when encrypting data across multiple platforms where one platform is OS390. This algorithm functions the same as PSUnicodeToAscii on all platforms other than OS390.
PSAsciiToUnicode_Generic_DEC	Convert ASCII text to Unicode  <b>Note.</b> Use when performing cross-platform decryption where one platform is OS390. This algorithm functions the same as PSAsciiToUnicode on all platforms other than OS390.

## 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. These algorithms are available when you load the OpenSSL encryption library into the PET database.

### Encoding Algorithms

Following are the supported OpenSSL encoding algorithms.

<b>Algorithm</b>	<b>Description</b>
base64_encode	Encode data in base64 format.
base64_decode	Decode data from base64 format.

### Hashing Algorithms

Following are the supported OpenSSL hashing algorithms.

<b>Algorithm</b>	<b>Description</b>
md2_generate	Generate an MD2 hash value from the input data.
md4_generate	Generate an MD4 hash value.

<b>Algorithm</b>	<b>Description</b>
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 Algorithms**

This table describes the supported OpenSSL symmetric encryption algorithms, which implement triple Data Encryption Standard (DES) encryption with various key sizes and modes.

<b>Algorithm Name</b>	<b>Description</b>
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.

<b>Algorithm Name</b>	<b>Description</b>
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 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.

---

**Note.**

All algorithm chains that use 3 DES *encryption* algorithms must include either the base64\_encode or PSHexEncode algorithm as a step in the encryption algorithm chain. All algorithm chains that use 3 DES *decryption* algorithms must include the corresponding base64\_decode or PSHexDecode algorithm as a step in the decryption algorithm chain.

---

### **Digital Signature Handling Algorithms**

Following are the supported OpenSSL algorithms for generating signatures.

<b>Algorithm Name</b>	<b>Description</b>
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 pass phrase used to decrypt and unlock the signer's private key. This parameter's value is the actual pass phrase.

---

**Note.** The output of these algorithms must be a hex encoded signature if it is going to be used as the SIGNATURE parameter value for the Verify routine. To generate a Hex value a PSHexEncode algorithm must be the second to the last step in the chain.

---

Following are the supported OpenSSL algorithms for verifying signatures.

<i>Algorithm Name</i>	<i>Description</i>
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:

- *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-----".

---

**Note.** The API implementation of the rsa\_sha1\_verify algorithm requires that the Public Key be certified.

---

- *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.

---

**Note.** The system expects all hex encoded values to begin with 0x. If the hex encoded signature value does not begin with these two characters, you must manually prepend 0x to it or the signature will be invalid.

---

### **Secure Messaging — pkcs7\_signed\_sign**

The pkcs7\_signed\_sign algorithm generates a signed PKCS7 message. The parameters are:

- *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 pass phrase used to decrypt and unlock the signer's private key. This parameter's value is the actual pass phrase.

### **Secure Messaging — *pkcs7\_signed\_verify***

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\_encrypt***

The *pkcs7\_signed\_verify* algorithm verifies a signed PKCS7 message. The parameters are:

- *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.

See [Chapter 13, "Securing Data with PeopleSoft Encryption Technology," Symmetric Encryption Algorithms, page 236.](#)

### **Secure Messaging — *pkcs7\_encrypted\_decrypt***

The *pkcs7\_encrypted\_decrypt* algorithm decrypts an encrypted PKCS7 message. The parameters are:

- *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 pass phrase used to decrypt and unlock the recipient's private key. This parameter's value is the actual pass phrase.

### **Secure Messaging — *pkcs7\_signandencrypt\_signandencrypt***

The *pkcs7\_signandencrypt\_signandencrypt* algorithm generates a signed and encrypted PKCS7 message. The parameters are:

- *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 pass phrase used to decrypt and unlock the signer's private key. This parameter's value is the actual pass phrase.

- *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.

See [Chapter 13, "Securing Data with PeopleSoft Encryption Technology," Symmetric Encryption Algorithms, page 236.](#)

### **Secure Messaging — *pkcs7\_signandencrypt\_decryptandverify***

The *pkcs7\_signandencrypt\_decryptandverify* algorithm decrypts and verifies an encrypted PKCS7 message. The parameters are:

- *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 pass phrase used to decrypt and unlock the recipient's private key. This parameter's value is the actual pass phrase.

## PGP Algorithms

This section describes the secure messaging algorithms supported by the delivered PGP glue code. The messaging algorithms are 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:

- *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 pass phrase used to decrypt the signer's private key. This parameter's value is the actual pass phrase.

- *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. The parameters are:

- *SIGNERPUBLICKEY*

Specify 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-----".

- *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.

This algorithm has one parameter: , which is

### ***pgp\_encrypted\_encrypt***

The *pgp\_encrypted\_encrypt* algorithm generates an encrypted PGP message. The parameters are:

- *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:

- *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 pass phrase used to decrypt the recipient's private key. This parameter's value is the actual pass phrase.

- *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:

- *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 pass phrase used to decrypt the signer's private key. This parameter's value is the actual pass phrase.

- *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 pass phrase used to decrypt the recipient's private key. This parameter's value is the actual pass phrase.

- *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 13, "Securing Data with PeopleSoft Encryption Technology," Loading Encryption Libraries, page 244

## 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 or PSUnicodeToAscii\_Generic\_ENC, and the last algorithm must be PSAsciiToUnicode or PSAsciiToUnicode\_Generic\_DEC.

## Cross Platform Algorithm Chain Considerations

When encrypting and decrypting data across multiple platforms where OS390 is one of two or more platforms, the PSUnicodeToAscii\_Generic\_ENC algorithm must be the first algorithm in the encrypting algorithm chain. Conversely, PSAsciiToUnicode\_Generic\_DEC must be the last algorithm in the decrypting algorithm chain.

---

**Note.** If all participating encrypting and decrypting systems are on the OS390 platform, it is not necessary to use the generic algorithms. If none of the encrypting and decrypting systems in a cross platforms scenario are on the OS390 platform, the PSUnicodeToAscii\_Generic\_ENC algorithm functions exactly like the PSUnicodeToAscii algorithm and the PSAsciiToUnicode\_Generic\_DEC algorithm functions exactly like the PSAsciiToUnicode algorithm.

---

---

**Important!** If you modify current algorithm chains by replacing the PSUnicodeToAscii or the PSAsciiToUnicode algorithms with the PSUnicodeToAscii\_Generic\_ENC or the PSAsciiToUnicode\_Generic\_DEC algorithms, respectively, currently stored encrypted data on the OS390 DB must be unencrypted using the original decryption chain and reencrypted with the new encryption chain.

---

---

## Loading Encryption Libraries

Access the Load Encryption Libraries page (PeopleTools, Security, Encryption, Load Encryption Libraries).

# Load Encryption Libraries

Library ID:

PSPETPGP

Description:

Library File:

PSPETPGP.DLL

Load Library

Loaded Algorithms

FindFirst1-6 of 6Last

Algorithm ID:

pgp\_encrypted\_decrypt

Description:

Algorithm Parameters

FindFirst1-4 of 4Last

Parameter Name:

RECIPIENTKID

☐ From Keyset

Parameter Value:

Parameter Name:

RECIPIENTPKPASSPHRASE

☐ From Keyset

Parameter Value:

Parameter Name:

RECIPIENTPRIVATEKEY

☒ From Keyset

Parameter Value:

Parameter Name:

RECIPIENTPUBLICKEY

☒ From Keyset

Parameter Value:

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*
- Sun Solaris  
OpenSSL: *libpspetssl.so*
- HP Tru64 Unix  
OpenSSL: *libpspetssl.so*
- HP-UX  
OpenSSL: *libpspetssl.sl*
- IBM AIX  
OpenSSL: *libpspetssl.a*

**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 PeopleSoft Encryption Technology facility uses the parameter's value to access the encryption key from the PET keystore.

---

**Important!** If the library you specify fails to load, you must sign out of your application, then shut down and restart the application server before signing back in.

---

---

**Note.** You must create a valid openssl.cnf file *before* you load the PSPETSSL encryption libraries or the system removes the pkcs7 routines from the list of loaded encryption libraries.

---

---

**Note.** When running multiple PS\_HOME application server directories against the same database, each PS\_HOME OpenSSL and PGP libraries and settings must be configured identically.

---







## Defining Algorithm Chains

Access the Algorithm Chain page (PeopleTools, Security, Encryption, Algorithm Chain).

### Algorithm Chain

Algorithm Chain ID: 3DES CBC HEX DECRYPT

Algorithm Chain Description: 3 Des CBC Decrypt Hex Decode

Algorithm Chain				
Customize   Find    		First	1-4 of 4	Last
Algorithm ID		Sequence		
PSUnicodeToAscii		1	+	-
PSHexDecode		2	+	-
3des_ks168_cbc_decrypt		3	+	-
PSAsciiToUnicode		4	+	-

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.

See [Chapter 13, "Securing Data with PeopleSoft Encryption Technology," Cross Platform Algorithm Chain Considerations, page 244.](#)

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 Encryption Technology includes the following predefined algorithm chains:

<b><i>Algorithm Chain</i></b>	<b><i>Algorithms</i></b>
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
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

<b>Algorithm Chain</b>	<b>Algorithms</b>
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
SMIME_DECRYPTED	PSUnicodeToAscii smime_encrypted_decrypt PSAsciiToUnicode
SMIME_DECRYPTED_VERIFY	PSUnicodeToAscii smime_signandencrypt_decryptandverify PSAsciiToUnicode
SMIME_ENCRYPTED	PSUnicodeToAscii smime_encrypted_encrypt PSAsciiToUnicode
SMIME_ENCRYPTED_SIGNED	PSUnicodeToAscii smime_signandencrypt_signandencrypt PSAsciiToUnicode

---

## Defining Algorithm Keysets

Access the Algorithm Keyset page (PeopleTools, Security, Encryption, Algorithm Keyset).

## Algorithm Keyset

Algorithm ID:   rsa\_md5\_sign

Keysets

Find | View All

First 1 of 1 Last

Keyset ID: MYMD5KEY

Use Certificate Store Value

Certificate Alias

Verisign Class 4

Certificate

Private Key

Use Entered Value

Key Value:

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 or a private key.

Important!

The certificate must be a local node certificate.

See

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.

---

**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**

<http://www.openssl.org/>

---

## Defining Encryption Profiles

Access the Encryption Profile page (PeopleTools, Security, Encryption, Encryption Profile).

## Encryption Profile

Encryption Profile ID: TRIPLE DES ENC B64

Algorithm Chain ID: 3DES CBC B64 ENCRYPT

Description: Triple DES encryption

Parameters		Find	First	1-4 of 4	Last
Algorithm ID: PSUnicodeToAscii	Chain Sequence: 1				
Algorithm ID: 3des_ks168_cbc_encrypt	Chain Sequence: 2				
<div> <div>▼ Parameter Values</div> <div>Find First 1-2 of 2 Last</div> <div> <div>Parameter Name: IV</div> <div> <input type="checkbox"/> From Keyset </div> <div> <div>Parameter Value: 0x0102030405060708</div> </div> </div> <div> <div>Parameter Name: SYMMETRICKEY</div> <div> <input checked="" type="checkbox"/> From Keyset </div> <div> <div>Parameter Value: 3DESFinancials</div> <div>🔍</div> </div> </div> </div>					
Algorithm ID: base64_encode	Chain Sequence: 3				
Algorithm ID: PSAsciiToUnicode	Chain Sequence: 4				

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

Access the Delete Encryption Profile page (PeopleTools, Security, Encryption, Delete Encryption Profile.).

To delete an encryption profile:

1. Select the profile you want to delete
2. Click the Delete button.

---

## Testing Encryption Profiles

Access the Encryption Demo page (PeopleTools, Security, Encryption, Test Encryption Profile).

### Encryption Demo

Encryption Profile ID:

TRIPLE DES ENC B64



Run Encryption Profile

Text to be Encrypted:

Hello, world.

Encrypted Text:

cA5YK2ByV5X+WqxATbsog==

Encryption Demo page

Use the Encryption Demo page to :

- Ensure that the encryption profiles produce the expected results.
- Determine the character length of the encrypted value.

---

**Important!** When planning to store encrypted data in fields on a table, you must consider that the length of the encrypted value is often *longer* than the unencrypted value.

---

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.

This is an example of PeopleCode that invokes an encryption profile:

```

&cry = CreateObject("Crypt");
&bar = CRYPT_WRK.CRYPT_PRFL_ID;
&cry.Open(&bar);
&cry.UpdateData(CRYPT_WRK.DESCRLONG);
DERIVED_CRYPT.DESCRLONG = &cry.Result;

/*If there is no Result, then maybe we are running a veriy routine.*/

If None(DERIVED_CRYPT.DESCRLONG) Then
    DERIVED_CRYPT.DESCRLONG = &cry.Verified;
End-If;

```

**See Also**

*Enterprise PeopleTools 8.50 PeopleBook: PeopleCode API Reference, "Crypt Class"*

---

## Using PeopleCode Encryption Methods

Two PeopleCode methods are provided by PET as part of PCI compliance which requires keys to be stored in encrypted format:

- `EncryptPETKey( )`
- `DecryptPETKey( )`

These methods are called and applied to keys wherever applicable when using PeopleSoft encryption technology. These functions are generally transparent to the application developer when using the PeopleTools PET pages. However, if you create applications which provide their own pages to display keys, you must use these functions to encrypt and decrypt keys to show them on application pages.

The two affected record.fields are:

- `PSCRYPTKEYSET.CRYPT_KEY.`
- `PSCRYPTPRFLPRM.CRYPT_PARAM_VAL.`

**See Also**


---

## Using Application Engine Programs to Encrypt and Decrypt Tables

There are two Application Engine programs that do full table encryption and decryption:

- `PTENCRYPTPET`

If you use Data Mover to export data from a PeopleTools version that pre-dates PET to the current tools version, run `PTENCRYPTPET` on the target database after the import to encrypt the table data.

- PTDECRYPTPET

If you use Data Mover to export PET table data from the current version into a version of PeopleTools that predates the introduction of the encrypt and decrypt field object methods, run PTDECRYPTPET on the source data prior to exporting to decrypt the table data.

Run PTDECRYPTPET on encrypted tables before running any process that does *not* have the ability to execute PeopleCode—Crystal Reports, nVision, SQR, and so on.

---

**Note.** It is recommended that you run PTENCRYPTPET after the system completes such processing.

---

---

**Note.** PET encryption and decryption works regardless of whether the keys are encrypted.

---

**See Also**

*Enterprise PeopleTools 8.50 PeopleBook: Application Engine*, "Managing Application Engine Programs," Running Application Engine Programs



## Chapter 14

# 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 Manager helps you build SQL queries to retrieve information from your application tables. For each Query Manager or Query Viewer 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 the 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 the 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 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 the 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 the 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. and Canadian record components to grant users in each region security access to only the record components they should use.

---

**Note.** You should consider adding record definitions to the 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 the 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 the Query tree.
- View and modify definitions.

## **Understanding Query Access Group Trees**

If you have worked with Tree Manager or trees, 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 points:

- 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, similar to folders in Microsoft Windows.
- Records represent a PeopleSoft record definition.

## ***Structure***

Regarding structure, consider the following points:

- Always use the ACCESS\_GROUP Tree Structure.
- Do not use SetID or UKV/BU.
- Do not have Details.
- Do not use Levels.
- Do not use Branches.

## ***Requirements***

Regarding requirements, consider the following points:


- 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**


Access the Query Access Manager page (PeopleTools, Security, Query Security, Query Access Manager.).

**Basic Search**

\*Search By:  

Tree Name:

[Create a New Tree](#)

Query Access Manager <span>Customize   Find   View All    First 1-7 of 7 Last</span>					
Tree Name	Category	Effective Date	Description	Delete	Copy
<a href="#">QE_QAS_QRY</a>	DEFAULT	10/30/2008	Tree for QAS security Testing	<a href="#">Delete</a>	<a href="#">Copy</a>
<a href="#">QE_QRY_RPTG_TREE</a>	DEFAULT	01/01/1900	Records for Query Automation	<a href="#">Delete</a>	<a href="#">Copy</a>
<a href="#">QE_QRY_TREE</a>	TOOLS	01/01/1900	Used in Query Manager security	<a href="#">Delete</a>	<a href="#">Copy</a>
<a href="#">QE_QUERY_TREE</a>	QEDMO	01/01/1900	Query Access Tree	<a href="#">Delete</a>	<a href="#">Copy</a>
<a href="#">QUERY_TREE_OLAP</a>	TOOLS	01/01/1900	Cube Manager generated records	<a href="#">Delete</a>	<a href="#">Copy</a>
<a href="#">QUERY_TREE_PT</a>	TOOLS	01/01/1900	PeopleTools Query Tree	<a href="#">Delete</a>	<a href="#">Copy</a>
<a href="#">QUERY_TREE_WF</a>	TOOLS	01/01/1990	Workflow Query Tree	<a href="#">Delete</a>	<a href="#">Copy</a>

### Query Access Manager - Search page

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. On the Basic Search page select your search criteria.

You can search by Tree Name, Tree Category, Tree Description, Group Name used in a Tree, or Record Name used in a Tree.

2. Click Search.

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

3. Click the tree name link.

The search page also enables you to delete or copy a tree. Click the Delete or Copy link to perform the desired task. 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 enter the name for the copied tree.

Some of the trees in the grid may appear with no Copy and Delete buttons visible. In this situation, Definition Security settings are such that you have only read-only access to these trees.

## Defining the Query Tree

Access the Tree Definition and Properties page (Click the Create a New Tree link on the Basic Search page).

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

Tree Definition and Properties

\*Tree Name:

\*Structure ID:

ACCESS\_GROUP

\*Description:

\*Effective Date:

06/04/2009

31

\*Status:

Active

\*Category:

DEFAULT

Item Counts

Node Count:

0

Tree Change Message Options

☒ Send Tree Change Message

☐ Don't send Tree Change Message

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	The description appears with the name and effective date in the list box when you select from a list of trees.
Effective Date	The status default is set to Active. Query trees are available immediately if the effective date is active; you don't need to run an SQR utility like you do for organizational security trees.
Category	If necessary add a category, which are groupings of the definitions.
Item Counts	Item Counts shows the number of nodes within the access group.

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

Viewing and Modifying Definitions

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

## Query Access Manager

Effective Date:01/01/1900Status:ActiveValid Tree

Tree Name:QUERY\_TREE\_PTPeopleTools Query Tree

Save AsCloseTree DefinitionDisplay OptionsPrint Format

PT\_ACCESS\_GROUP >PORTAL

Collapse AllExpand AllFind

First Page43 of 850Last Page

PT\_ACCESS\_GROUP - PeopleTools Access Group

XMLPUBLISHER - XML Publisher

PERFMON - Performance Monitor

OPTIMIZATION - Optimization

PORTAL - Portal

PSPRSMPerm - Portal Structure Permission

PSPRSMATTRVAL - Portal Attr Value Tbl

PSPRSMATTR - Portal Attribute Table

PSPRDMCNTPRV - Portal Content Provider Tbl

PSPRSMDEFN - Portal Structure Defn Tbl

PSPRDMDEFN - Portal Definition Table

BUSINESS\_INTERLINK - Business Interlinks

GLOBAL\_TIME - Time Definitions

CONTENT\_DEFINITION - CONTENT\_DEFINITION

Query Access Manager page

Effective Date	Shows the current effective date.
Status	Shows either Active or Inactive.
Tree Name	Shows the name of the current tree.
Save, Save As	These are the two save options. Each option appears only if it relates to the current activity. Save enables you to save your changes to the database. Save As enables you to clone tree definitions at save time.
Close	Closes the definition and returns you to the search page.
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.

<b>Print Format</b>	Displays a print preview of the tree definition.
<b>Bread Crumbs</b>	Once you have drilled down into a definition, a "bread crumb" view appears just above the Collapse/Expand All controls to provide orientation, especially within large trees.
<b>Collapse All</b>	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.
<b>Expand All</b>	Expands all nodes of the tree so that each child object is visible.
<b>Find</b>	<p>If you are looking for a specific access group or a record you can use the Find Value page rather than drilling down into the 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.</p> <p>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.</p> <p>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.</p> <p>For example, to find all occurrences of 'TBL' in the Records, you specify <i>%TBL</i> as a search condition (for Microsoft SQL Server database).</p> <p>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.</p> <hr/> <p><b>Note.</b> Always save modifications to the tree prior to using the Find feature.</p> <hr/>

### Node/Record Controls

When you have a node or record selected, the actions you perform are controlled by the icons that appear to the left and right of the definition. The descriptions of the actions are below. You can pass the mouse pointer over an icon to reveal its label.



When a node folder is open, click the Collapse Node icon to collapse the node.



When a node folder is closed, click the Expand Node icon to expand the node.



The Insert Sibling Group icon inserts an access group node at the same level as the currently selected node.



The Insert Child Group icon inserts an access group node at the next level lower than the currently selected node.



The Insert Child Record icon inserts a record definition within an access group node.



For access groups, click the Edit Data icon to edit the Description and the Definition (long description) on the Access Group Table.



Click the Delete icon to delete both access groups and records. You can't delete the root node.



You can cut and paste access groups and records to move them within the tree. Once you click the Cut icon, 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*, (also called data permission 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.

---

Typically, 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 the table or view from this record definition, you don't need to rebuild it.

### ***Row-Level (Data Permission) Security Views***

Using PeopleSoft row-level security views enables you to restrict users from seeing certain rows of data. You can restrict data by:

- User, by using the OPRID field.
- Primary permission list, by using the OPRCLASS field.
- Row security permission list, by using the ROWSECCLASS field.

To implement row-level security through a security view:

1. In Application Designer, insert one of the three row-level security fields (OPRID, OPRCLASS, ROWSECCLASS) into the record definition.
2. Configure the field as a Key, but not a List Box Item.
3. Save the record and build the view.
4. Use the record as the search record or query security record.

Now, when the user searches, the system dynamically adds a **WHERE** clause — that incorporates the security field — to the search **SELECT** statement. The value of the security field is based on the current user.

## Chapter 15

# 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.

<i><b>Definition Type</b></i>	<i><b>Associated Designer Tool</b></i>
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
Messages	PeopleSoft Application Designer
Mobile Pages <b>Important!</b> PeopleSoft Mobile Agent is a deprecated product. These features exist for backward compatibility only.	PeopleSoft Application Designer
Pages	PeopleSoft Application Designer
Analytic Types	PeopleSoft Application Designer

<b>Definition Type</b>	<b>Associated Designer Tool</b>
Projects	PeopleSoft Application Designer
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. Consider these types of questions:

- 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?

## 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, you've created a permission list for analysts who support the PeopleSoft Payroll module, and you call it PAYROLL\_DEV. The analysts are allowed to update only payroll definitions. Using Definition Security, you create a definition group containing only payroll definitions, and give it a name, such as PAYROLL\_OBJ. Finally, 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:

<i>Rule</i>	<i>Description</i>
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 <i>primary permission list</i> ? If not, the system denies access and displays a message, such as " <i>definition_name</i> 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 " <i>definition_name</i> is not a definition that you are authorized to update."  The definition type appears 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.

---

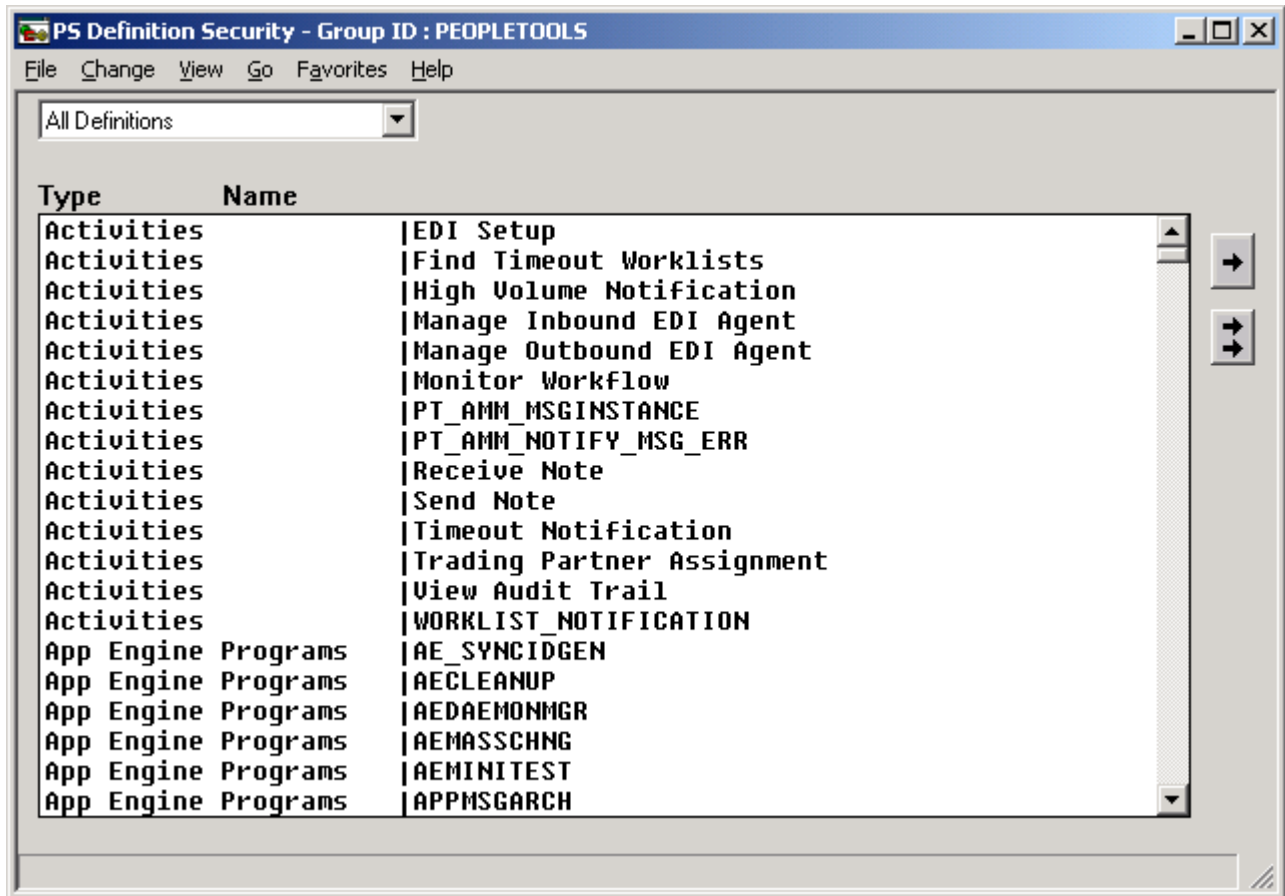
**Important!** A user gets definition security permissions through the primary permission list, not through roles.

---

## Working With Definition Groups

PeopleSoft Definition Security is a Microsoft Windows-based application that you can access from PeopleSoft Application Designer.

Access the PS Definition Security (Go, Definition Security).



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.

A confirmation prompt appears.

---

## 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 reports that detail *specific secured definitions* by user or by permission list, access the Common Queries - Definition Security Queries page (PeopleTools, Security, Common Queries-click the Definition Security Queries link).

You can also view reports that detail access to *definition types* by user or by permission list from the User Profiles and Permission Lists components.

See [Chapter 3, "Setting Up Permission Lists," Running Permission List Queries, page 67.](#)

See [Chapter 5, "Administering User Profiles," Running User ID Queries, page 105.](#)



## Chapter 16

# 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 software 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 pages.

To access the Personalization pages, select PeopleTools, Personalization.

Personalizations are grouped in three levels of categories to aid in development, organization, and deployment:

- 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, using the Personalizations page of the permission lists component in PeopleTools Security. The Personalizations page enables the security administrator to assign role-based personalizations and enable user control for selected personalization options, if needed.

End users can view and modify their available personalization options from the My Personalization component (USER\_SELF\_PERSONAL).

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 need to be familiar with the personalization option categories delivered with PeopleSoft software, and the pages used to view and modify them. This section discusses:

- Navigation personalizations.
- Regional settings.
- General options.
- System messages.
- Internally controlled options.
- Pages used to define and modify personalizations.

---

**Note.** PeopleSoft Mobile applications use the standard personalizations.

PeopleSoft Mobile Agent is a deprecated product. Mobile personalization features exist for backward compatibility only.

---

## Understanding Navigation Personalizations

The following table presents the delivered navigation personalization 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 set the option.

---

<i>Option Code</i>	<i>Description</i>	<i>Default Value</i>	<i>PTPT1000</i>
ACEGRDCOLS (Max columns for Show all Columns)	Specify the maximum number of columns that are displayed in an analytic grid when the user selects Show All Columns. You can specify up to 100.	40	No
ACEGRDROWS (Max rows for View All)	Specify the maximum number of rows that are displayed in an analytic grid when the user selects View All.	100	No
ADBTN (Tab over Add/Del Buttons (+/-))	Enable tabbing over the Add (+) and Delete (-) buttons within grids and scrolls.	No	No
ANAVSORT	Enable top navigation sort.	Yes	No
AUTOMENU (Automatic menu collapse)	Enable the menu to automatically collapse when a transaction is selected. The user can expand the menu either by pressing Ctrl-Y or clicking the Show Menu icon.	No	Yes
BADDRESSBAR (Show browser address location)	Enable the display of the browser's address bar.  <b>Note.</b> This option takes effect only after a new browser instance is launched.	Yes	No
BBUTTONS (Show browser navigation bar)	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.  <b>Note.</b> This option takes effect only after a new browser instance is launched.	Yes	No
BLINKS (Show browser links)	Enable the display of the browser's personal links toolbar.  <b>Note.</b> This option takes effect only after a new browser instance is launched.	Yes	No

<i><b>Option Code</b></i>	<i><b>Description</b></i>	<i><b>Default Value</b></i>	<i><b>PTPT1000</b></i>
BMENU (Show browser menu)	Enable the display of the browser's menu bar.  <b>Note.</b> This option takes effect only after a new browser instance is launched.	Yes	No
BMOPOPUP	Enable mouse over pop up pages, which display a page over the main page when you hover over certain text fields.	Yes	No
CALBTN (Tab over Calendar Button)	Enable tabbing over the calendar controls, which appear as buttons on the page.	No	Yes
EXPERT	Enable expert entry.	Yes	Yes
GRDRWS (Max rows for View All)	Specify the maximum number of rows that are displayed in a grid or scroll area when the user selects View All.	100	No
GRDTAB (Tab over Grid Tabs)	Enable tabbing over the tabs or headings within grids.	No	Yes
HDRICN (Tab over Header Icons)	Enable tabbing over header icons, which appear at the top of each page and include Home, Add To Favorites, and Sign Out.	No	Yes
LKPBTN (Tab over Lookup Button)	Enable tabbing over the lookup buttons to the right of edit boxes that have an associated list of valid values.	No	Yes
NBAR (Tab over Navigation Bar)	Enable tabbing over navigation bars, which appear at the top of grids and scroll areas to control the appearance of rows and columns.	No	Yes
NONPS (Tab over Browser Elements)	Restrict tabbing to include only the PeopleSoft elements of the page, and tab over non-PeopleSoft elements.	No	Yes

<i>Option Code</i>	<i>Description</i>	<i>Default Value</i>	<i>PTPT1000</i>
PGLNK (Tab over Page Links)	Enable tabbing over links to other pages in the same component.	No	Yes
POPUP (Tab over Related Page Links)	Enable tabbing over the pop-up menu icon that opens a page of associated menu items.	No	Yes
TBAR (Tab over Toolbar)	Enable tabbing over the toolbar at the bottom of a page. Toolbar items include buttons that control standard operations on the page, such as Save and Return to Search.	No	Yes
TYPEAHD	Enable auto suggest type ahead on prompt edit boxes. The system performs a prompt lookup as you type, suggesting appropriate values.	Yes	Yes

## Understanding Regional Settings

The following table presents the delivered regional settings.

**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.

<i>Option Code</i>	<i>Description</i>	<i>Default Value</i>	<i>PTPT1000</i>
ADES (Afternoon designator (PM, pm))	(Locale-based) Specify the afternoon designator string to use to indicate PM on a 12 hour display, such as <i>PM</i> or <i>pm</i> . This value has a 5-character limit.	PM	Yes
AUTOGREGCAL	Specify whether the system automatically recognizes and converts date values to Gregorian calendar dates.	Yes	Yes

<b>Option Code</b>	<b>Description</b>	<b>Default Value</b>	<b>PTPT1000</b>
CALENDAR	<p>(Locale-based) Specify the calendar type to use. Select from these values:</p> <ul style="list-style-type: none"> <li>• <i>Gregorian</i></li> <li>• <i>Hijri (UmmA l-Qura)</i></li> <li>• <i>Thai</i></li> </ul> <p><b>Note.</b> If auto-recognize Gregorian dates is set to <i>Yes</i> and the calendar is set to non-Gregorian, any dates entered in date fields that fall in the range of the Gregorian calendar will be assumed to be Gregorian and will be converted to specified calendar dates.</p>	Gregorian	Yes
DCSP (Decimal Separator)	(Locale-based) Specify the decimal separator character for values with decimals, such as <i>1.00</i> or <i>1,00</i> . You can enter any single character.	.	No
DFRMT (Date Format)	<p>(Locale-based) Specify the format for displaying the date. Select from the following values:</p> <ul style="list-style-type: none"> <li>• <i>DDMMYY</i> (day first)</li> <li>• <i>MMDDYY</i> (month first)</li> <li>• <i>YYMMDD</i> (year first)</li> </ul>	MMDDYY	Yes
DTSP (Date Separator)	(Locale-based) Specify a date separator character used to separate the month, day, and year in a date. For example, if you specify a hyphen (-), the date appears as 01-01-2001. If you specify a slash (/), the date appears as 01/01/2001. You can enter any single character.	/	No
LTZONE (Local Time Zone)	<p>Select the local time zone, such as <i>Moscow Time</i>, <i>Greenwich Mean Time</i>, or <i>Japan Standard Time</i>.</p> <p><b>Note.</b> This setting alters the <i>display</i> of the time for the end user, but does not affect the Base Time Zone setting on the PeopleTools Options page.</p>	Pacific Time (US), Tijuana	Yes

<b>Option Code</b>	<b>Description</b>	<b>Default Value</b>	<b>PTPT1000</b>
MDES (Morning designator (AM, am))	(Locale-based) Specify the morning designator string to use to indicate AM on a 12 hour display, such as <i>AM</i> or <i>am</i> . This value has a 5-character limit.	AM	Yes
TFRMT (Time Format)	(Locale-based) Specify the time format for display. Select from the following values: <ul style="list-style-type: none"> <li>12 hour clock (01:05:00 PM)</li> <li>24 hour clock (13:05:00)</li> </ul> <b>Note.</b> Whether microseconds appear is not a personalization option.	12 hour clock	Yes
TMSP (Time Separator)	Specify the time separator character to separate hours, minutes, and seconds, such as (:) or (.). You can enter any single character.	:	No
TSEP (Digit Group Separator)	(Locale-based) Specify the digit group separator character for displaying numerical values over 999 — such as a comma (1,000) or a period (1.000). To specify a space, enter the space between single quotes (' '). You can enter any single character.	,	No
TZONE (Use Local Timezone)	Indicate that transactions are to use the local time zone of the client machine.  If you select <i>No</i> , transactions use the local time zone of the server, where the server may in turn be set to a corporate time zone.	No	Yes
WEEKFIRSTDAY	(Locale-based) Specify which day begins the week.	Sunday	Yes

### ***Locale-Based Regional Settings***

Some of the regional settings, as noted in the table, are locale-based. Their values can be determined based on the locale setting of the user's browser. Because this is one of three sources that can determine which value applies, it's important to understand which source takes precedence:

- In the Define Personalizations component (PSUSEROPTNDEFINE), you can specify default values for locale-based settings, which apply in the absence of any overriding setting.
- The user's browser locale setting is used by the PeopleSoft system to invoke the default values of regional settings for that locale, which you can configure on the Locale Defaults page. Each setting for which you configure a value overrides any default value that's specified for that setting in the Define Personalizations component.
- If a user specifies a value for a locale-based setting in the My Personalizations component, that value overrides any value configured for that setting for the user's browser locale on the Locale Defaults page. That value also overrides any default value that's specified for that setting in the Define Personalizations component.

### See Also

Chapter 16, "Managing PeopleSoft Personalizations," Working with Locale-Based Personalizations, page 295

## 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.

<i>Option Code</i>	<i>Description</i>	<i>Default Value</i>	<i>PTPT1000</i>
ACCESS (Accessibility Features)	<p>Specify accessibility features. This option provides better support for assistive technologies. Select from the following values:</p> <ul style="list-style-type: none"> <li>• <i>Use accessible layout mode</i> — For use with screen readers. Page elements (fields, links, buttons, and so on) are presented in linear fashion to assistive software.</li> <li>• <i>Use standard layout mode</i> — Supports assistive technologies without altering the page design.</li> <li>• <i>Accessibility features off</i> — This disables accessibility features.</li> </ul>	Accessibility features off	Yes

<i>Option Code</i>	<i>Description</i>	<i>Default Value</i>	<i>PTPT1000</i>
EXCEL97 (Excel 97 grid download)	<p>Indicate that you want to use the character set defined in the user language instead of the default UTF-8 character set when you download a page grid to Microsoft Excel 97.</p> <p>Enter <i>Y</i> to enable, or <i>N</i> to disable this option.</p> <p><b>Note.</b> This option is recommended only for non-English speaking users who use Microsoft Excel 97. It isn't recommended for Excel in Microsoft Office 2000 and later.</p>	N	Yes
CUSTOMPGSET (Customize Page Settings)	<p>Indicate that the Customize Page pagebar link should appear at the top of pages at runtime. Users can use this control to define, share, and copy page personalizations.</p> <p><b>Warning!</b> When this option is disabled, all existing page personalizations for the user are deleted. Grid personalizations aren't affected.</p> <p><b>Note.</b> You can prevent the Customize Page pagebar link from appearing in a given component, regardless of whether users have access to this option, by clearing the Customize Page Link check box in the Internet properties of the component definition.</p> <p>See PeopleTools 8.50 PeopleBook, PeopleSoft Application Designer, "Creating Component Definitions," Setting Component Properties.</p>	Yes	No
METAXP (Time page held in cache)	<p>Enable browser caching for the navigation pages that remain relatively static. This option specifies the time, in minutes, that portal homepage and navigation pages are held in the cache.</p> <p>You can specify a value between 0 (no caching) and 525600 minutes (one year).</p>	900	Yes

<b>Option Code</b>	<b>Description</b>	<b>Default Value</b>	<b>PTPT1000</b>
MLTLNG (Multi Language Entry)	<p>Enable data entry in multiple languages.</p> <p>On a page where the Data Language drop-down list box is available, users can select a preferred language for data entry on that page.</p> <p>When this option is disabled, the Data Language drop-down list box has no effect.</p>	No	Yes
SCLANG (Spell Check Dictionary)	Specify the language to use for the spell check dictionary. Users can select from a wide range of supported languages, or use their session language.	Use session language	Yes

### See Also

*Enterprise PeopleTools 8.50 PeopleBook: PeopleTools Portal Technologies, "Using Portal Caching Features"*

## Understanding System 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. The following table presents the options for system messages.

**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.

<b>Option Code</b>	<b>Description</b>	<b>Default Setting</b>	<b>PTPT1000</b>
SCNFRM (Save Confirmation)	Display a brief message confirming each save action.	Yes	No
SWARN (Save Warning)	Display a warning when the user makes a change and attempts to leave the transaction without saving.	Yes	Yes

## Understanding Internally Controlled Options

Internally controlled personalization options are different from the other personalization option categories. Although they're defined in the Define Personalizations component (PSUSEROPTNDEFINE), they never appear in My Personalizations, even if you assign them to a permission list.

Instead of accessing these options in My Personalizations, users access and configure them at other locations; the location depends on the individual option. These options are always enabled and can't be disabled, but you can specify their default settings in the Define Personalizations component.

### **Query Preferences**

You specify the default values of the Query preference options in the Define Personalizations component, and individual users can modify those values in Query preferences. The following personalization options are used by PeopleSoft Query:

<b>AUTOJOIN</b>	This option appears as the Enable Auto Join check box on the Query Preferences page. It's selected by default.
<b>NAMESTYLE</b>	This option appears as the Name Style setting on the Query Preferences page. Its default value is <i>Name and Description</i> .
<b>DICTIONARY</b>	This option is not used in the current release.
<b>SORTBY</b>	This option is not used in the current release.

See Enterprise PeopleTools 8.50 PeopleBook: PeopleSoft Query, "Creating and Running Simple Queries," Creating New Queries, Specifying Query Preferences.

### **Portal Preference**

The following personalization option is used by PeopleSoft internet technology:

<b>PAGEHDRCACHE</b>	<hr/> <p><b>Note.</b> This option is not available to end users. The default value that you set for it in the Define Personalizations component is the only value used, and it applies globally to all users.</p> <hr/> <p>Use PAGEHDRCACHE to configure caching for the PeopleSoft portal navigation header. This option specifies the time, in minutes, that portal headers are held in the cache. The delivered initial value of this option is 480 minutes.</p>
---------------------	---

### **Tree Manager Preference**

The following personalization option is used by PeopleSoft Tree Manager:

<b>TMLINES</b>	<p>This option appears as the Display Lines Per Page setting on the Configure User Options page of PeopleSoft Tree Manager. Its default value is 60 lines.</p> <p>See Enterprise PeopleTools 8.50 PeopleBook: PeopleSoft Tree Manager, "Using PeopleSoft Tree Manager," Saving and Configuring Trees, Setting Display Options.</p>
----------------	--

## Pages Used to Define and Modify Personalizations

<i>Page Name</i>	<i>Definition Name</i>	<i>Navigation</i>	<i>Usage</i>
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 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 component, 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 example, 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 example, for CRM personalizations, select the CRM category.

---

**Note.** Whether you have installed all of the applications listed in the Option Category Level options, the same category levels appear. Ignore any category levels that do not apply to your site.

---

You add and modify the delivered personalization options using the Define Personalizations component.

Access the Define Personalization page (PeopleTools, Personalization, Personalization Options). This grid contains the following 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

Click the Definition tab.

### Define Personalizations

Option Category Level: PeopleTools

Define Personalizations							
Customize   Find   View All   [Grid Icon]   [List Icon]   First 1-25 of 48 Last							
Definition   Format   Explanation   [Filter Icon]							
*User Option	Description	*Option Category Group	Option Category	User Option Type	Locale Based		
ACCESS	Accessibility Features	PS Internet Architecture	General Options	System	<input type="checkbox"/>	+	-
ACEGRDCOLS	Max Col/View All-Analytic Grid	PS Internet Architecture	Navigation Personalizations	System	<input type="checkbox"/>	+	-
ACEGRDROWS	Max Row/View All-Analytic Grid	PS Internet Architecture	Navigation Personalizations	System	<input type="checkbox"/>	+	-
ADBTN	Tab over Add/Del Buttons (+/-)	PS Internet Architecture	Navigation Personalizations	System	<input type="checkbox"/>	+	-
ADES	Afternoon designator (PM, pm)	PS Internet Architecture	Regional Settings	System	<input checked="" type="checkbox"/>	+	-
ANAVSORT	Drop down Menu Sort Order	PS Internet Architecture	Navigation Personalizations	System	<input type="checkbox"/>	+	-
AUTOGREGCAL	Auto-recognize Gregorian dates	PS Internet Architecture	Regional Settings	System	<input type="checkbox"/>	+	-
AUTOJOIN	Enable Auto Join	Query Preferences	Internally Controlled	Functional	<input type="checkbox"/>	+	-
AUTOMENU	Automatic Menu Collapse	PS Internet Architecture	Navigation Personalizations	System	<input type="checkbox"/>	+	-

Define Personalizations - Definition tab

#### 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*: Options that users set within an application or tool, 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 them 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 see only options that posses the following attributes: the User Option Type is set to System, *and* permission to override that option is granted by one of the users' assigned permission lists.

Using the Format Tab

Click the Format tab.

Define Personalizations

Option Category Level: PeopleTools

Define Personalizations

Customize | Find | View All | First 1-25 of 48

Definition

Format

Explanation

*User Option▼	Field Format	Format Length	Record (Table) Name	Field Name	Option Default Value
WEEKFIRSTDAY	<div></div>		PSXLATITEM	DAY_OFWEEK	Sunday
TZONE	<div></div>		PSXLATITEM	PSYESNO	No
TYPEAHD	<div></div>		PSXLATITEM	PSYESNO	Yes
TSEP	Mixedcase <div></div>	3			,
TMSP	Mixedcase <div></div>	1			:
TMLINES	Numbers <div></div>	2			60
TFRMT	<div></div>		PSXLATITEM	PT_TIME_FORMA	12 hour clock
TBAR	<div></div>		PSXLATITEM	PSYESNO	No
SWARN	<div></div>		PSXLATITEM	PSYESNO	Yes
SORTBY	Uppercas <div></div>	1			C

Define Personalizations - Format tab

- User Option**

Shows the code associated with the option.
- Field Format and Field Format Length**

Specify the field characteristic of the option. Used for the Option Default Value for options that are not validated against the database.
- Record (Table) Name**

Specifies the lookup table that holds the personalization options values.

<b>Field Name</b>	Specifies the field on the lookup table containing the valid option values.
<b>Option Default Value</b>	Shows the current default for the option. This value is set through the Set Option Default Value.
<b>Set Option Default Value</b>	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:

<b>Option Category Level</b>	Shows the high-level category to which the option belongs, such as PeopleTools or HCM.
<b>User Option</b>	Shows the code associated with the option.
<b>Description</b>	Shows the description of the option.
<b>Current Default Value</b>	Displays the current default value
<b>Option Default Value</b>	Select the appropriate value from the drop down list, or add the appropriate option manually. For options that derive default values from a prompt table, the system displays a drop down list. Otherwise, the system displays an edit box.

## **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).

Click the Explanation tab.

Define Personalizations

Option Category Level: PeopleTools

Define Personalizations				
Customize   Find   View All     First 1-25 of 48 Last				
Definition	Format	Explanation		
*User Option	Message Set Number	Message Number	Image Name	
WEEKFIRSTDAY	141	212		
TZONE	141	43		
TYPEAHD	141	98		
TSEP	141	42		
TMSP	141	41		
TMLINES				
TFRMT	141	40		
TBAR	141	39	PT_EX_TOOLBAR	
SWARN	141	38		
SORTBY				

Define Personalizations - 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 presents 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.** By default, all options created within the category level of Custom appear in the Custom category group.

Access the Category Group page (PeopleTools, Personalization, Category Groups).

Category Group

Category Group			
		Customize   Find    	First 1-6 of 6 Last
*Option Category Group	*Object owner identifier	*Description	
APP DESIGNER	PeopleTool	App Designer Preferences	 
CUSTOM	PeopleTool	Custom Personalizations	 
PIA	PeopleTool	PS Internet Architecture	 
PORTAL	PeopleTool	Portal Personalizations	 
QUERY	PeopleTool	Query Preferences	 
TREE MANAGER	PeopleTool	Tree Manager Preferences	 

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. 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.

Access the Category page (PeopleTools, Personalization, Categories).

## Category

Personalization Categories			Customize   Find     First 1-5 of 5 Last	
*Option Category	*Object owner identifier	*Description		
GENERAL	PeopleTool	General Options	+	-
INTERNAL	PeopleTool	Internally Controlled	+	-
LOCALE	PeopleTool	Regional Settings	+	-
MESSAGES	PeopleTool	System & Application Messages	+	-
NAVIGATION	PeopleTool	Navigation Personalizations	+	-

Category page

<b>Option Category</b>	Shows the name of the category in which options are displayed on the My Personalizations page.
<b>Object owner identifier</b>	Displays the name of the group responsible for the maintenance of the category group.
<b>Description</b>	Provides a description of the category for identification purposes. This field has a 30-character limit.
<b>Important!</b> 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 software provides 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 8.50 PeopleBook: Global Technology*, "Controlling International Preferences," Setting Up Locale-Based Formatting for the PeopleSoft Pure Internet Architecture

---

## 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 59

---

## Creating Custom Personalization Options

Creating custom personalization options involve the following steps:

1. Define the option using the Define Personalization interface.

See Chapter 16, "Managing PeopleSoft Personalizations," Defining Personalization Options, page 288.

2. Implement the behavior using PeopleCode personalization options (discussed in the following section).

See Chapter 16, "Managing PeopleSoft Personalizations," Working with the My Personalizations Interface, page 297.

3. To enable users 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 8.50 PeopleBook: PeopleCode Language Reference, "PeopleCode Built-in Functions"*

# Working with the My Personalizations Interface

This section discusses how to:

- Use the Personalizations page.
- Set personalize options.
- Use the Personalization Explanation page.
- Modify a personalization option.

## Using the Personalizations Page

Select My Personalizations to access the Personalizations page.

### Personalizations

QE User

Standard settings are in effect.

Changes to Personalization settings require you to log off and log back on in order to take effect.

Personalization Categories	
Description	Personalize Option
General Options	Personalize Option
Regional Settings	Personalize Option
System & Application Messages	Personalize Option
Navigation Personalizations	Personalize Option

Restore Defaults

Personalizations page

- Description**

The description column contains a brief description for identifying a particular category of personalization options.
- Personalize Options**

Click this button to view and modify the options within a category.

**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 (From the homepage, click My Personalizations, then click the Personalize Options button in the General Options row).

Option Category: General Options

Personalizations

FindFirst1-4 of 4Last

Personalization Option	Default Value	Override Value	
Accessibility Features	Accessibility features off	<div></div>	<a href="#">Explain</a>
Time page held in cache	900	<div></div>	<a href="#">Explain</a>
Multi Language Entry	No	<div></div>	<a href="#">Explain</a>
Spell Check Dictionary	Use session language	<div></div>	<a href="#">Explain</a>

Restore Category Defaults

My Personalizations - Personalize Options page

- 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 the new value 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 Personalization Explanation page (click the Explain link on the Option Category page).

Personalization Explanation

Multi Language Entry

Default Value

No

Override Value

Restore Option to Default

Explanation

When Multi Language Entry is enabled, you will be able to enter data in the language you specified in the Data Language: dropdown in pages where multiple language entry is available.

Image:

Data Language:

English

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.
Override Value	Overrides the default value. For example, 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	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.

<b>Image</b>	<p>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.</p> <p>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.</p>
<b>OK/Cancel</b>	<p>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, use either button.</p>

## 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 enter an override value.

5. Click OK.

This saves the change to the system.

6. Sign out and then sign in again to view your changes.

# Index

## Numerics/Symbols

&authMethod global variable 172  
%PSAuthResult function 176  
%Request function 176  
%SignonUserId function 176  
%SignOnUserPswd function 176

## A

access groups  
    defining 61  
    query trees *See Also* query access group trees  
access IDs  
    access profiles access profiles  
    application servers 96  
    encrypting 19  
    LDAP servers 96  
    understanding 18, 86  
access profiles  
    access IDs *See Also* access IDs  
    creating, changing passwords, deleting 88  
    customizing for administrators 19  
    managing 86  
    setting properties 87  
    setting up 86  
Access Profiles dialog box 86  
Active Directory  
    assigning roles dynamically 173  
ADA compliance 33  
Add Access Profile dialog box 87  
Additional Connect DN's page 138  
Address Book page 156  
administrators  
    customizing definitions 19  
    understanding signon PeopleCode  
        permissions 174  
AIX encryption library filenames 246  
Algorithm Chain page 247  
Algorithm Keyset page 249  
algorithms  
    chains, defining 244  
    chains, delivered 248  
    defining chains 247  
    defining encryption profiles 251  
    defining keysets 249  
    developing encryption profiles 232  
    internal 234  
    OpenSSL *See Also* OpenSSL algorithms  
    PGP PGP algorithms  
    understanding 234  
    understanding encryption 230  
    understanding hashing 231  
aliases  
    adding for digital certificates 215  
    defining nodes for single signon 195  
    selecting for algorithm keysets 250  
    using email IDs as user ID aliases 97, 150  
Americans with Disabilities Act (ADA)

    compliance 33  
Application Designer  
    applying permissions 40  
    definition security rules 270  
    designing definitions 267  
    restricting menu access 37  
    setting tools permissions 42  
    upgrading roles/permission lists 117, 132  
Application Engine programs  
    DYNROLE 7  
    DYNROLE\_PUBL 7  
    LDAPMAP 7  
    LDAPSHEMA 7  
    PORTAL\_CSS 28  
    PURGEOLDUSERS 109  
    PURGEOLDUSRS 7  
    security integration 7  
    USR\_PRFL\_XFR 7  
application servers  
    authenticating web server connections 182  
    connecting to LDAP servers 136  
    enabling users to start 32  
    managing user IDs 96  
    securing connections with LDAP servers 159  
    signing on 20  
    single signon transaction (sample) 197  
    understanding connect IDs 18  
    understanding single signon 192  
    using encryption 16  
archiving 47  
asymmetric encryption 231  
auditing  
    displaying profile update information 103  
    running user transfer scripts 118, 133  
    tracking login/logout activities 118  
    viewing role update information 83  
Authenticate function 207, 208  
authentication  
    accessing X.509 certificates 178  
    directory authentication program 175  
    directory-based 23  
    enabling for LDAP 136  
    enabling signon PeopleCode for LDAP 158  
    maps *See Also* authentication maps  
    PeopleSoft-based 23  
    PS\_TOKEN cookie  
        *See Also* PS\_TOKEN cookie  
    running signon PeopleCode after  
        authentication failure 178, 181  
    setting for nodes 195  
    single signon transaction (sample) 197  
    single signon with third-party (sample) 205  
    tokens *See Also* authentication tokens  
    understanding 22  
    understanding client 171  
    understanding delivered solutions 169  
    using digital signatures 231  
    using LDAP 173  
    using LDAP over SSL 159  
    using signon PeopleCode 21  
    using the External\_Authentication function  
        181  
    using the LDAP\_Authentication function

- 170, 172
- using the LDAP authentication program 181
- using the PsGetTuxConnectInfo() function 187
- using the SetAuthenticationResult function
  - 176, 183
- using the SSO\_Authentication function
  - 170, 172
- using the WWW\_Authentication function
  - 170, 171
- web server-level considerations 171
- web server security exit
  - See Also* web server security exit
- authentication maps
  - associating with user profile maps 148
  - creating 143
  - deleting from LDAP directory configurations
    - 156
  - selecting LDAP servers 145
  - setting directory information 143
  - setting user search information 144
  - understanding 142
- Authentication page 143
- authentication tokens
  - PS\_TOKEN cookie
    - See Also* PS\_TOKEN cookie
  - understanding 16
- authorization
  - authentication *See Also* authentication
  - authorization IDs 17
  - bypassing signon 183
  - certificate authorities (CAs) *See Also* CAs
  - permission lists
    - permission lists, permission lists
  - roles roles
  - understanding security 11, 16

## B

- base64\_decode algorithm 235
- base64\_encode algorithm 235
- batch processes *See* Process Scheduler
- bind variables 76
- Blackberry 97
- browsers
  - enabling navigation page caching 284
  - setting navigation options 278
  - using encryption 16
- business interlinks
  - implementing SSL 214
  - using Directory Business Interlinks for LDAP
    - 135
  - using LDAP over SSL 159

## C

- caches
  - adding user profile properties 149
  - caching directory schema 141
  - enabling navigation page caching 284
  - invoking/monitoring schema cache processes
    - 140
  - maintaining for user profiles 135
  - understanding user profile options 146
  - updating upon signon 150

- Cache Schema page 141
- CAs
  - understanding 16, 214
  - understanding SSL 213
  - using LDAP over SSL 159
- categories
  - searching personalizations by option category
    - level 289
  - understanding 294
  - understanding personalization 277
  - working with category groups 293
- Category Group Page 293
- category groups
  - understanding 277
  - working with 293
- Category Page 294
- CBC 230
- cert7.db
  - using LDAP over SSL 159
- certificates
  - certificate authorities (CAs) *See Also* CAs
  - certificate database 159
  - digital *See Also* digital certificates
  - PeopleSoft keystore 250
  - public key *See Also* public key certificates
  - root root certificates
  - X.509 X.509 certificates
- CFB 230
- change control
  - overriding object types settings 42
  - setting access levels 44
- Cipher Block Chaining (CBC) 230
- Cipher Feed Back (CFB) 230
- client authentication 171
- component interfaces
  - DELETE\_ROLE 5
  - DELETE\_USER\_PROFILE 5
  - PRTL\_SS\_CI 207
  - ROLE\_MAINT 5
  - security integration 4
  - setting permissions 53
  - USER\_PROFILE 5
  - USERMAINT\_SELF 5
  - User Profile 135
- components
  - granting access 37
  - interfaces *See Also* component interfaces
  - setting page permissions 33
- connect IDs 18
- content references 27, 28
  - synchronizing/viewing related 28
- cookies
  - PS\_TOKEN *See Also* PS\_TOKEN cookie
  - single domain limitation 200
- crypt class
  - invoking encryption profiles 253
  - supported algorithms 234
  - understanding algorithms 234
- cryptographic hash *See* hashing
- cryptography PeopleSoft Encryption Technology
- currency
  - setting for user profile maps 150
  - setting for user profiles 97
- cut function 264

## D

- Data Archive Manager 47
- databases
  - creating database-level IDs 19
  - single signon configurations (sample) 203
  - synchronizing users 123
  - transferring user profiles 117, 131
  - understanding connect IDs 18
  - using cert7.db 159
- Data encryption 221
- Data Encryption Standard (DES) *See* DES
- Data Mover scripts (DMS)
  - migrating security links setup data 9
  - transferring users between databases 117, 118, 131, 133
- data permission security
  - for queries 264
- DB2
  - access ID terminology 88
  - setting job controls 50
- debugging *See* PeopleCode Debugger
- default mobile page
  - setting for user profiles 98
- Define Personalizations component
  - accessing/understanding 289
  - Definition tab 290
  - Explanation tab 292
  - Format tab 291
  - Set Option Default Value page 292
- Define Personalizations page 288
- definition groups
  - adding/removing definitions 273
  - assigning to permission lists 274
  - definition security rules 270
  - enabling/disabling display-only mode 275
  - understanding 269
  - viewing 272
  - working with 271
- definitions
  - access profile *See Also* access profiles
  - adding/removing 273
  - administrator 19
  - groups *See Also* definition groups
  - LDAP schema 7
  - mass change 65
  - node *See Also* nodes
  - process groups process groups
  - query access group tree
    - query access group trees
  - query security record 264
  - record 257, 258, 264
  - role *See Also* roles
  - security security definitions
  - security rules 270
  - setting permissions 40
  - types and design tools 267
  - understanding 12
  - understanding field-level security 269
  - understanding security 267
  - viewing user/permission list access 275
- DELETE\_ROLE component interface 5
- DELETE\_ROLE service operation 6
- DELETE\_USER\_PROFILE component interface 5
- DELETE\_USER\_PROFILE service operation 6
- Delete Directory page 155
- Delete Encryption Profile page 252
- DES
  - algorithm chains 248
  - algorithms 236
- dialog box security 14
- digital certificates
  - authenticating nodes 195
  - authentication 200
  - certificate authorities (CAs) *See Also* CAs
  - configuring 214
  - importing 214
  - single signon 200
  - understanding 213
  - understanding SSL 213
- Digital Certificates page 214
- digital signatures
  - authentication 231
  - generating via OpenSSL algorithms 237
  - setting in the PS\_TOKEN cookie 191
  - verifying via OpenSSL algorithms 238
- directory authentication program 175
- directory servers
  - authentication 21, 23
  - configuring the LDAP directory 136
  - implementing SSL 144, 157
  - integrating 21
  - specifying 141
  - understanding user profile options 146
- Directory Setup page 137
- distinguished names (DNs) *See* DNs
- DMS
  - Data Mover scripts (DMS), Data Mover scripts (DMS)
- DNs
  - connecting to LDAP servers 136, 138
  - setting additional connect DNs 138
  - setting for authentication maps 144
  - setting up cross-domain single signon 202
  - using the LDAP\_Authentication function 170, 172
  - using the SSO\_Authentication function 170, 172
  - using the WWW\_Authentication function 170
- domains
  - qualifying names 202
  - setting up cross-domain single signon 202
  - single domain limitations 200
- Dynamic Members page 73
- dynamic roles
  - assigning 101
  - assigning membership (example) 75
  - change notifications 24
  - creating NEWUSER roles 83
  - displaying members 73
  - understanding 23, 69
- DYNROLE\_PUBL program 7
- DynRoleMembers program 74
- DYNROLE program 7

## E

- ECB 230, 237
- Electronic Code Book (ECB) 230, 237
- email
  - enabling recipient lookup 80

- entering addresses for user profile maps 150
- entering addresses for user profiles 97
- receiving forgotten passwords 32, 110
- encryption
  - access IDs *See Also* access IDs
  - asymmetric 231
  - Data Encryption Standard (DES) 236
  - library filenames 246
  - loading libraries 244
  - OS390 considerations 235, 244
  - passwords 185
  - PGP *See Also* PGP
  - profiles encryption profiles
  - PS\_TOKEN cookie PS\_TOKEN cookie
  - symmetric 230
  - understanding 230
  - using SSL *See Also* SSL
- Encryption Profile page 251
- encryption profiles
  - defining 251
  - deleting 252
  - developing/using 232
  - invoking from PeopleCode 253
  - opening 234
  - testing 253
- Entrust 213
- errors
  - authenticating nodes (single signon) 195
  - emailing forgotten passwords 32
  - importing digital certificates 214
  - specifying authentication domains 200
  - using bind variables as dynamic role rules 76
- events
  - adding signon PeopleCode triggers 178
  - realtime event notification (REN) 46
- exporting
  - security information 117, 131
  - source/target database permissions 45
- External\_Authentication function 181, 182

## F

- fields
  - containing signon PeopleCode 178
  - understanding field-level security 16, 269
- Forgot My Password Email Text page 110
- Forgot My Password Hint page 111
- functions
  - %PSAuthResult 176
  - %Request 176
  - %SignonUserId 176
  - %SignOnUserPswd 176
  - adding to signon PeopleCode 178
  - Authenticate 207, 208
  - authentication 169
  - cut 264
  - External\_Authentication 181, 182
  - GetUserID 207
  - GetUserOption 296
  - iScripts 55
  - LDAP\_Authentication 172
  - LDAP\_profilesynch 202
  - LDAP\_ProfileSynch 173
  - paste 264
  - PsGetLogonInfo() 183, 185
  - PsGetTuxConnectInfo() 183, 187

- SetAuthenticationResult 176, 183
- SetUserDescr() 92
- Set User Description 92
- SetUserOption 296
- SSO\_Authentication 172
- WWW\_Authentication 171

## G

- GetUserID function 207
- GetUserOption function 296
- granting roles 80

## H

- hashing
  - OpenSSL algorithms 235
  - understanding 231
  - understanding digital signatures 231
- HP Tru64 Unix encryption library filenames 246
- HP-UX encryption library filenames 246
- HTTPS
  - securing the authentication token 206
  - understanding SSL 213
  - using digital certificates 213

## I

- ID page 99
- importing
  - digital certificates 214
  - enabling automatic role imports 149
  - security information 117, 131
  - source/target database permissions 45
- integration
  - directory servers 21
  - integration gateway encryption 16
  - understanding security integrations 4
  - using the single signon API 207
  - web server security exit
    - See Also* web server security exit
- Integration Broker
  - authenticating nodes 195
  - configuring user profile synchronization 123
  - implementing SSL 214
- integration gateway encryption 16
- iPlanet
  - assigning roles dynamically 173
- iScripts 55

## J

- Java Virtual Machine (JVM), rebooting 55
- Jolt 16
- JVM, rebooting 55

# K

keysets, defining algorithm 249  
key stores

- authenticating nodes 195
- PeopleSoft keystore 250

# L

languages

- enabling multi-language entry 284
- setting for spell check 284
- setting for user profile maps 149, 150
- setting for user profiles 97
- setting in the PS\_TOKEN cookie 190
- setting translation permissions 44

LDAP

- assigning roles dynamically 173
- authentication, enabling 136
- authentication, using 173
- authentication maps
  - See Also* authentication maps
- authentication over SSL, enabling 159
- authentication program 181
- directory, configuring 136
- directory configurations, deleting 155
- directory services, using 135
- enabling password controls 177
- LDAPS *See Also* LDAPS
- mapping attributes to user IDs 172
- role rules *See Also* role rules
- schema, caching 141
- schema definitions, putting into databases 7
- schema extensions, installing 139
- schema extensions, viewing 140
- servers *See Also* LDAP servers
- signon PeopleCode, enabling 158
- single signon, implementing 191
- specifying connect DN's 138
- specifying network information 137
- testing connectivity 140
- understanding 16
- user profile maps *See Also* user profile maps
- using business interlinks 159
- using the LDAP\_Authentication function
  - 170, 172
- using the LDAP\_profilesynch function
  - 202
- using the LDAP\_ProfileSynch function
  - 171, 173
- using the LDAPSHEMA program 7
- using the workflow address book 156
- web server security exit 181

LDAP\_Authentication function 170, 172

LDAP\_profilesynch function 202

LDAP\_ProfileSynch function 171, 173

LDAPMAP program 7

LDAPS

- understanding 159
- using 144, 157

LDAPSHEMA program 7

LDAP servers

- applying configuration to authentication
  - functions 169
- authentication 23
- connecting from application servers 136

- implementing SSL 138
- integrating 21
- managing user IDs 96
- securing connections with application servers
  - 159
- selecting for authentication maps 145
- setting up cross-domain single signon 202
- specifying for directory services 138
- using signon PeopleCode 21

libraries

- encryption library filenames 246
- loading encryption 244
- setting web library permissions 55
- using PGP 233

licensing PGP® encryption 241

Lightweight Directory Access Protocol (LDAP)

*See* LDAP

links

- activating/deactivating 9
- adding to application-specific pages 8
- displaying links added for user profiles 104
- enabling for browsers 278
- migrating setup data 9
- understanding 8

Linux

- encryption library filenames 246
- OpenSSL command line program 251

Load Encryption Libraries page 244

# M

Mandatory User Properties page 147

maps

- authentication *See Also* authentication maps
- user profile user profile maps

mass changes 65

Members page 73

menus

- deleting access 38
- enabling for browsers 278
- setting access 34
- understanding security 14

messages

- changing user profiles 24
- PGP 241
- PKCS7 238
- setting system message options 286
- XML 213

Microsoft Windows *See* Windows

mobile pages

- enabling access 34
- granting access 38

# N

navigation

- enabling navigation page caching 284
- Navigator homepage
  - See Also* Navigator homepage
- setting options 278
- understanding personalization 277
- understanding single signon 192

Navigator homepage

- setting for security profiles 31

- setting for user profiles 98
- Navigator homepage permission list
  - setting for user profile maps 150
- NEWUSER roles, creating 83
- Node Definitions page 194
- nodes
  - adding nodes for single signon 192
  - defining for single signon 194
  - query access group trees 259
- notifications
  - dynamic role changes 24
  - enabling for PeopleSoft Workflow 80
  - realtime event notification (REN) 46
  - using the workflow address book 156
- Novell NDS
  - assigning roles dynamically 173

## O

- Object Permissions page 40
- objects
  - accessing for signon PeopleCode 177
  - locking/unlocking 44
  - roles *See Also* roles
  - schema extensions 140
  - security definition *See Also* security definitions
  - setting permissions 40, 45
  - understanding security 12
  - user profiles *See Also* user profiles
- OFB 230
- OpenSSL
  - algorithms *See Also* OpenSSL algorithms
  - command line program 251
  - encryption library filenames 246
- OpenSSL algorithms
  - accessing 235
  - defining keysets 250
  - encoding 235
  - handling digital signatures 237
  - hashing 235
  - pkcs7\_encrypted\_decrypt 239
  - pkcs7\_encrypted\_encrypt 239
  - pkcs7\_signandencrypt\_decryptandverify 240
  - pkcs7\_signandencrypt\_signandencrypt 240
  - pkcs7\_signed\_sign 238
  - pkcs7\_signed\_verify 239
  - symmetric encryption 236
  - verifying digital signatures 238
- Optional User Properties page 149
- Oracle Internet Directory
  - assigning roles dynamically 173
- Oracle Jolt 16
- Oracle Tuxedo *See* Tuxedo
- OS/390 job controls 50
- Output Feed Back (OFB) 230

## P

- pages
  - adding links to application-specific 8
  - granting access 37
  - mobile *See Also* mobile pages
  - personalizing 284
  - setting permissions 33

- understanding security 14
- Password Controls page 106
- passwords
  - applying controls 32
  - authenticating nodes 195
  - authenticating web server connections 182
  - capturing user entries 174
  - changing 109
  - changing for access profiles 89
  - changing for administrators 19
  - creating for default users 179
  - enabling age and lockout controls 107
  - enabling controls 176
  - encrypting 185
  - entering for LDAP directories 138
  - forgotten 112
  - forgotten passwords, creating/deleting hints for 111
  - forgotten passwords, receiving emails for 32, 110
  - forgotten passwords, setting up a site for 112
  - requesting new 112
  - reusability 109
  - setting controls 106
  - setting for access IDs 88
  - setting for user profiles 96
  - setting restrictions 108
  - setting up access profiles 86
  - setting validity duration 108
  - synchronizing changes 24
  - understanding 18
  - using LDAP authentication 174
  - using the RevalidatePassword function 172
- paste function 264
- PeopleCode
  - crypt class *See Also* crypt class
  - Debugger PeopleCode Debugger
  - directory authentication program 175
  - functions *See Also* functions
  - methods for encryption 254
  - personalization 296
  - record PeopleCode
    - See Also* signon PeopleCode
    - signon PeopleCode signon PeopleCode
- PeopleCode Debugger
  - monitoring the directory authentication program 175
  - setting access permissions 44
- PeopleSoft Administrator role 84
- PeopleSoft Application Designer
  - See* Application Designer
- PeopleSoft Business Interlinks business interlinks
- PeopleSoft Data Archive Manager 47
- PeopleSoft Encryption Technology
  - developing encryption profiles 232
  - understanding 229, 232
- PeopleSoft Integration Broker
  - See* Integration Broker
- PeopleSoft Mobile personalizations 278
- PeopleSoft Navigator homepage
  - See* Navigator homepage
- PeopleSoft Password Controls program 177
- PeopleSoft Performance Monitor 39
- PeopleSoft Process Scheduler
  - See* Process Scheduler
- PeopleSoft Pure Internet Architecture security 16
- PeopleSoft Query
  - defining query profiles 62, 257

- designing definitions 267
- personalizing internal options 286
- query access group trees
  - See Also* query access group trees
- PeopleSoft Report Manager 15
- PeopleSoft security *See* security
- PeopleSoft signon signon
- PeopleSoft Signon window 183, 185
- PeopleSoft single signon *See* single signon
- PeopleSoft Tree Manager 267
- PeopleSoft Workflow
  - enabling notifications 80
  - setting Navigator homepage permission list for user profile maps 150
  - setting the Navigator homepage for user profiles 98
  - using the address book 156
- PeopleTools
  - delivered definitions 270
  - directory authentication program 175
  - editing menu items 37
  - Personalization PeopleTools 277
  - security
    - See Also* PeopleTools Security, PeopleTools Security
  - setting permissions 39
  - transferring users between databases 118, 133
- PEOPLETOOLS definition group 270
- PeopleTools Security
  - adding links to application-specific pages 8
  - adding personalizations to permission lists 296
  - administering security *See Also* security
- performance issues
  - asymmetric/symmetric encryption 231
  - enabling Performance Monitor
    - See Also* Performance Monitor
  - implementing permission lists 26
  - reducing execution intervals for dynamic rules 84
  - setting access group permissions 62
  - setting maximum rows retrieved by queries 64
- Performance Monitor
  - enabling 39
  - setting monitoring permissions 52
  - setting user access 51
- Permission List Access Groups page 61
- Permission List - Mass Change page 65
- permission lists
  - adding personalizations 296
  - assigning definition groups 269, 274
  - assigning to roles 12, 72
  - assigning to user profiles 12
  - auditing updates 66
  - complying with Americans with Disabilities Act (ADA) 33
  - creating, copying and deleting 26
  - defining 29
  - definition security rules 270
  - displaying links added for permission lists 65
  - PTPT1000
    - See Also* PTPT1000 permission list
  - running queries 67
  - setting component interface permissions 53
  - setting for user profiles 98
  - setting general permissions 30
  - setting object permissions 40
  - setting page permissions 33
  - setting PeopleTools permissions 39
  - setting permissions for user profile maps 150
  - setting personalization permissions 59
  - setting process permissions 47
  - setting query permissions 60
  - setting signon time permissions 52
  - setting web library permissions 55
  - setting web services permissions 57
  - setting WSRP permissions 57
  - synchronizing with content references 28
  - understanding 12, 25
  - upgrading 24
  - using PSWDEXPR 108
  - viewing definition access 275
- Permission Lists - Audit page 66
- Permission Lists - Audit page 66
- Permission Lists - Component Interfaces page 53
- Permission Lists - General page 30
- Permission Lists page 72
- Permission Lists - Pages page 33
- Permission Lists - PeopleTools page 39
- Permission Lists - Personalizations page 59
- Permission Lists - Query page 60, 67
- Permission Lists - Sign-on Times page 52
- Permission Lists - Web Libraries page 55
- Permission Lists - Web Services page 57
- Personalization PeopleTools 277
- Personalization Permissions page 59
- personalizations
  - adding, modifying, viewing 289
  - adding to permission lists 296
  - categories 294
  - creating custom options 296
  - defining options 288
  - managing options 278
  - modifying options 300
  - PeopleCode functions 296
  - Personalization PeopleTools 277
  - setting general options 284
  - setting internal options 286
  - setting international/regional options 281
  - setting navigation options 278
  - setting permissions 59
  - setting system message options 286
  - understanding 277
  - using locale-based 295
  - working with category groups 293
- Personalizations page 297
- Personalize Explanation page 299
- Personalize Options page 298
- PET *See* PeopleSoft encryption
- PGP
  - algorithms *See Also* PGP algorithms
  - encryption library 233
  - encryption library filenames 246
  - messages 241
  - platform support 234
  - pgp\_encrypted\_decrypt algorithm 242
  - pgp\_encrypted\_encrypt algorithm 242
  - pgp\_signed\_sign algorithm 241
  - pgp\_signed\_verify algorithm 241
  - pgp\_signedandencrypted\_decryptandverify algorithm 243
  - pgp\_signedandencrypted\_signandencrypt algorithm 242
  - PGP algorithms

- accessing 241
  - defining keysets 250
  - pgp\_encrypted\_decrypt 242
  - pgp\_encrypted\_encrypt 242
  - pgp\_signed\_sign 241
  - pgp\_signed\_verify 241
  - pgp\_signedandencrypted\_decryptandverify 243
  - pgp\_signedandencrypted\_signandencrypt 242
  - pkcs7\_encrypted\_decrypt algorithm 239
  - pkcs7\_encrypted\_encrypt algorithm 239
  - pkcs7\_signandencrypt\_decryptandverify 240
  - pkcs7\_signandencrypt\_signandencrypt algorithm 240
  - pkcs7\_signed\_sign algorithm 238
  - pkcs7\_signed\_verify algorithm 239
  - PKCS Utilities 159
  - PORTAL\_CSS program 28
  - portals
    - configuring single signoff 209
    - defining nodes 194
    - PeopleSoft Portal Solutions 213
    - securing the authentication token 206
    - setting up cross-domain single signon 202
    - single signon configuration 200
    - synchronizing permission lists with content references 28
    - understanding single signon 192
    - using the single signon API 207
  - private keys 231
  - process groups
    - setting process permissions 47
    - understanding batch process security 14
  - Process Profile Permission page 48
  - process profiles
    - setting for user profiles 98
    - setting permissions 48
    - setting permissions for user profile maps 150
    - understanding batch process security 14
  - Process Scheduler
    - servers *See Also* Process Scheduler servers
    - setting permissions 47
    - setting user permissions 98
    - understanding security 14
  - Process Scheduler servers
    - enabling users to start 32
    - running role rules 101
  - profiles
    - access *See Also* access profiles
    - encryption encryption profiles
    - process process profiles
    - query 62, 257
    - route control 100
    - users *See Also* user profiles
    - web web profiles
  - programs
    - Application Engine
      - Application Engine programs
    - batch Process Scheduler
    - PeopleTools 37
    - running at signon time 174
  - PRTL\_SS\_CI component interface 207
  - PS\_TOKEN cookie
    - fields 190
    - securing 206
    - security features 190
    - single signon transaction (sample) 197
    - understanding 192
  - PSACCESSLOG table 118
  - PSACCESSPRFL table 19
  - PSAsciiToUnicode\_Generic\_DEC algorithm 235
  - PSAsciiToUnicode algorithm 235, 244
  - PSCipher
    - data encryption 221
  - PS Definition Security window 271
  - PsGetLogonInfo() function 183, 185
  - PsGetTuxConnectInfo() function 183, 187
  - PSHexDecode algorithm 235
  - PSHexEncode algorithm 235
  - PSOPRDEFN table 21, 146
  - PSUnicodeToAscii\_Generic\_ENC algorithm 235
  - PSUnicodeToAscii algorithm 235, 244
  - PSUSER.DLL
    - customizing 185
    - implementing customized 188
  - PSWDEXPR permission list 108
  - PTPT1000 permission list
    - modifying general personalization options 284
    - setting international/regional options 281
    - setting navigation options 278
    - setting system message options 286
  - public key certificates
    - understanding 16
  - public keys
    - asymmetric encryption 231
    - certificates *See Also* public key certificates
  - PURGEOLDUSERS program 109
  - PURGEOLDUSRS program 7
  - purging user profiles 119
- ## Q
- queries
    - applying row-level security 264
    - assigning dynamic role membership 75
    - defining access groups 61
    - defining profiles 62, 257
    - query access group trees
      - See Also* query access group trees
    - running permission list 67
    - running role queries 81
    - running user ID queries 105
    - setting permissions 60
    - setting up security 257
    - understanding query security records 264
    - using bind variables as dynamic role rules 76
  - query access group trees
    - building 257
    - defining 260
    - finding 263
    - modifying/viewing 261
    - opening 259
    - understanding 258
  - Query Access Manager page 259
  - Query Profile page 62
  - query profiles, defining 62, 257
- ## R
- RDBMS IDs *See Also* access IDs
  - realtime event notification (REN) 46
  - record PeopleCode *See* signon PeopleCode

- records
    - applying row-level security 264
    - recording PeopleCode exits 178
    - record PeopleCode
      - See Also* signon PeopleCode
    - understanding query security 264
  - Red Hat Linux *See* Linux
  - relational database management system (RDBMS)
    - IDs *See Also* access IDs
  - REN 46
  - Report Manager 15
  - Report Repository 15
  - reports
    - repository 15
    - understanding security 15
    - viewing definition access 275
  - RevalidatePassword function 172
  - ROLE\_MAINT component interface 5
  - ROLE\_MAINT service operation 6
  - Role Grant page 80
  - Role Policy page 152
  - role rule program 75, 101
  - role rules
    - assigning roles dynamically to users 101
    - building search filters 154
    - checking role rule program status 75, 101
    - defining 152
    - deleting from LDAP directory configurations 156
    - running manually 101
    - selecting a Process Scheduler server 101
    - selecting servers 153
    - selecting user profile maps 153
    - setting directory search parameters 153
    - testing 101
    - understanding 151
    - using bind variables 76
  - roles
    - applying automatically 149
    - assigning 23
    - assigning permissions 72
    - assigning to user profiles 12
    - creating NEWUSER 83
    - decentralizing administration 80
    - defining options 71
    - DELETE\_ROLE component interface 5
    - DELETE\_ROLE service operation 6
    - deleting 5, 6
    - displaying links added for roles 80
    - dynamic *See Also* dynamic roles
    - dynamic assignment 24
    - maintaining 5, 6
    - PeopleSoft Administrator 84
    - relationship to user profiles/permission lists 25
    - removing users, copying and deleting 70
    - reporting 15
    - ROLE\_MAINT component interface 5
    - ROLE\_MAINT service operation 6
    - ROLESYNCHEXT\_MSG service operation 6
    - rules *See Also* role rules
    - running queries 81
    - selecting alternate users 102
    - setting for user profile maps 148
    - setting for user profiles 100
    - setting user routing options 79
    - static *See Also* static roles
    - understanding 12, 69
    - understanding security 11
    - upgrading 24
    - viewing role definitions associated with users 101
    - viewing update information 83
  - Roles page 100
  - ROLESYNCHEXT\_MSG service operation 6
  - root certificates
    - authenticating nodes 195
    - understanding 16
    - using LDAP over SSL 159
  - route control profiles 100
  - routing
    - selecting alternate users for role routings 102
    - setting user options 79
    - setting user preferences 103
  - row-level security
    - for queries 264
  - rows
    - applying row-level security 264
    - setting maximum for grids 278
    - transferring duplicate 118, 132
    - understanding row-level security 264
    - understanding security 15
  - rules
    - definition security 270
    - role rules *See Also* role rules
  - runtime security 16
- ## S
- schema
    - installing schema extensions for LDAP 139
    - invoking/monitoring cache processes 140
    - viewing schema extensions for LDAP 140
  - Schema Management page 139
  - scripts
    - Data Mover
      - See Also* Data Mover scripts (DMS), Data Mover scripts (DMS)
    - iScripts 55
    - signon PeopleCode
      - See Also* signon PeopleCode
  - searches
    - deleting from LDAP directory configurations 156
    - LDAP authentication maps 144
    - personalization definition pages 289
    - query access group trees 263
    - query security records 264
    - role rules 153
  - Search page 289
  - Secure Sockets Layer (SSL) *See* SSL
  - security
    - access profiles *See Also* access profiles
    - administering from applications 8
    - application data 15
    - applying row-level 264
    - batch processes *See Also* Process Scheduler
    - definition groups definition groups
    - definitions security definitions
    - definition security rules 270
    - digital certificates
      - See Also* digital certificates
    - encryption encryption

- implementing 22
- LDAP directory services *See* LDAP
- pages, dialog boxes, menus 14
- PeopleSoft Encryption Technology
  - See Also* PeopleSoft Encryption Technology
- PeopleSoft Pure Internet Architecture 16
- PeopleTools
  - See Also* PeopleTools Security, PeopleTools Security
- permission lists permission lists
- personalization *See* personalization
- preparing to use 8
- Process Scheduler *See Also* Process Scheduler
- PS\_TOKEN cookie PS\_TOKEN cookie
- queries queries
- reports reports
- roles roles
- setting mass change permissions 65
- setting permissions for user profile maps 150
- signon and timeout 13
- synchronizing multiple systems 24
- table-level 15
- tracking login/logout activities 118
- understanding 11
- understanding column-level 16
- understanding definitions 267
- understanding field-level 16, 269
- understanding integrations 4
- understanding online 13
- understanding row-level 15, 264
- user profiles
  - See Also* user profiles, user profiles
- web server security exit
  - web server security exit
- Windows security exit Windows security exit
- security definitions
  - application data 15
  - hierarchy 25
  - understanding 12, 15
- security exits
  - web server *See Also* web server security exit
  - Windows Windows security exit
- Security Links - User page 8
- Security PeopleCode Options page 128
- servers
  - application *See Also* application servers
  - directory directory servers
  - LDAP LDAP servers
  - selecting for role rules 153
  - understanding security 16
- service monitor
  - checking role rule program status 75, 101
- service operations
  - DELETE\_ROLE 6
  - DELETE\_USER\_PROFILE 6
  - ROLE\_MAINT 6
  - ROLESYNCHEXT\_MSG 6
  - security integration 5
  - synchronization 24
  - USER\_PROFILE 6
  - USER\_PROFILE\_XFR 6
- SetAuthenticationResult function 176, 183
- Set Option Default Value page 292
- Set User Description function 92
- SetUserOption function 296
- signon
  - bypassing the PeopleSoft Signon window 183, 185
  - locking accounts 108
  - passwords *See Also* passwords
  - PeopleCode signon PeopleCode
  - setting logon information for users 96
  - setting time permissions 52
  - setting up access profiles 86
  - signing in via the web server 182
  - single *See Also* single signon
  - understanding 13, 20
  - understanding connect IDs 18
  - user IDs *See Also* user IDs
  - using the LDAP\_Authentication function 170
- signon PeopleCode
  - accessing X.509 certificates 178
  - adding event triggers and functions 178
  - assigning roles dynamically 173
  - authenticating users at the web-server level 171
  - authentication 21
  - authentication, delivered solutions 169
  - authentication, LDAP 146, 158
  - authentication failure, running PeopleCode after 178, 181
  - enabling 107, 176
  - invoke as user signing in 177
  - modifying 175
  - programs, adding 177
  - programs, enabling 177
  - programs, setting the run order for 177
  - programs, writing 181
  - signing on via web servers 183
  - specifying fields and records 178
  - understanding 173
  - understanding permissions 174
- Signon PeopleCode page 176
- single signoff, configuring 209
- single signon
  - adding nodes 192
  - authentication 200
  - configuration, implementing 200
  - configurations (sample) 203
  - configuring single signoff 209
  - defining nodes 194
  - developing external applications to support 208
  - digital certificates 200
  - implementing LDAP 191
  - PS\_TOKEN cookie
    - See Also* PS\_TOKEN cookie
  - qualifying domain names 202
  - sample transaction 197
  - securing the authentication token 206
  - setting expiration time 192
  - setting up 191
  - setting up for machines without DNS entries 201
  - setting up in cross-domain environments 202
  - single domain limitations 200
  - understanding 22, 192
  - using the API 207
  - using the SSO\_Authentication function 170, 172
- Single Signon page 192
- Solaris encryption library filenames 246
- spell check dictionary 284
- SQL
  - Editor 44
  - queries *See Also* queries

- views 15, 264
- SQL Editor 44
- SSL
  - certificate authorities (CAs) *See Also* CAs
  - digital certificates digital certificates
  - implementing between PeopleSoft and
    - directory servers 144, 157
  - LDAP, using 159
  - LDAP servers, implementing SSL for 138
  - securing the authentication token 206
  - understanding 16, 213
  - using the WWW\_Authentication function
    - 170, 171
- SSO\_Authentication function 170, 172
- static roles
  - displaying members 73
  - understanding 23, 69
- status
  - setting for authentication maps 143
  - viewing for user profile maps 148
- Structured Query Language (SQL) *See* SQL
- switch user
  - enabling 98
- symbolic IDs
  - setting for access profiles 86, 88
  - setting for user profile maps 150
  - setting for user profiles 96
  - understanding 19
- symmetric encryption 230
- synchronization
  - synchronizing permission lists and content
    - references 28
  - synchronizing user profiles 22, 24, 123

## T

- tables
  - PSACCESSLOG 118
  - PSACCESSPRFL 19
  - PSOPRDEFN 21, 146
  - understanding row-level security 264
  - understanding security 15
- templates
  - email for forgotten passwords 110
  - LDAP authentication program 181
  - mass change 65
  - portal solutions using frame-based
    - 201, 203, 209
- Test Connectivity page 140
- Test Encryption Profile page 253
- testing
  - encryption profiles 253
  - LDAP connectivity 140
  - links 9
  - role rules 101
- three-tier environments
  - applying password controls 32
  - using 20
  - using the PsGetTuxConnectInfo() function
    - 187
  - Windows security exit 183
- timeouts
  - complying with Americans with Disabilities
    - Act (ADA) 33
  - setting for PeopleSoft system users 33
  - setting for web servers 33

- setting in the PS\_TOKEN cookie 191
  - understanding security 13
- tracking user sign-in/sign-out 118
- transactions
  - single signon (sample) 197
- translations
  - setting permissions 44
  - updating Translate table values 42
- Tree Definition and Properties page 260
- Tree Manager 267
- trees
  - access groups *See Also* access groups
  - query access group trees
    - query access group trees
- triggers, signon PeopleCode 178
- Tuxedo
  - using encryption 16
  - using the Windows security exit 183
- two-tier environments
  - applying password controls 32
  - customizing administrator definitions 19
  - LDAP authentication 136
  - understanding connect IDs 18
  - using 20
  - Windows security exit 183

## U

- UNIX
  - encryption library filenames 246
  - OpenSSL command line program 251
- upgrade issues
  - query access group trees 258
  - setting upgrade permissions 45
  - source/target database permissions 45
  - synchronizing permission lists with content
    - references 28
  - transferring users between databases
    - 117, 131
  - upgrading permission lists, roles and user
    - profiles 24
- USER\_PROFILE\_XFR service operation 6
- USER\_PROFILE component interface 5
- USER\_PROFILE service operation 6
- USEREXPORT.DMS 117, 132
- user IDs
  - creating default 179
  - mapping LDAP attributes 172
  - modifying web profiles 180
  - running queries 105
  - setting in the PS\_TOKEN cookie 190
  - understanding 18
  - understanding signon 177
  - understanding types 89
- USERIMPORT.DMS 117, 132
- USERMAINT\_SELF component interface 5
- user profile maps
  - adding user profile properties to caches 149
  - deleting from LDAP directory configurations
    - 156
  - enabling automatic role application 149
  - enabling multiple languages 150
  - enabling signon PeopleCode for LDAP
    - authentication 159
  - selecting for role rules 153
  - setting currency 150

- setting default roles 148
  - setting email addresses 150
  - setting ID types 148
  - setting languages 149
  - setting mandatory properties 147
  - setting optional properties 149
  - setting permissions 150
  - setting the Navigator homepage permission list 150
  - updating caches 150
  - using constant values 149
  - using symbolic IDs 150
  - user profiles
    - component interface 135
    - creating, copying, and deleting 119
    - creating, copying and deleting 92
    - deactivating 96
    - defining types 91
    - DELETE\_USER\_PROFILE component interface 5
    - DELETE\_USER\_PROFILE service operations 6
    - deleting 5, 6, 109
    - displaying added links 104
    - displaying profile update information 103
    - distributed 113
    - enabling application server startup 32
    - enabling deferred processing 98
    - enabling Process Scheduler server startup 32
    - entering email addresses 97
    - entering symbolic IDs 96
    - locking accounts 108
    - maintaining 5
    - maps *See Also* user profile maps
    - password expiration 108
    - passwords *See Also* passwords
    - passwords, setting 96
    - passwords, setting controls 106
    - preserving historical data 120
    - purging inactive 119
    - reassigning workflow 103
    - role/permission list relationship to 25
    - roles, assigning dynamically 101
    - roles, setting 100
    - roles, viewing associated definitions 101
    - setting general attributes 97
    - setting language preferences 97
    - setting logon information 96
    - setting permission lists 98
    - setting process profiles 98
    - setting routing preferences 103
    - setting supervisor IDs 103
    - setting the currency 97
    - setting the default mobile page 98
    - setting the Navigator homepage 98
    - setting vacancy times 103
    - signon PeopleCode, understanding 173
    - signon PeopleCode, using 21
    - specifying attributes 94
    - specifying workflow settings 101
    - storing 21
    - supporting LDAP 202
    - synchronizing among databases 123
    - synchronizing changes 24
    - transferring between databases 117, 123, 131
    - understanding 12, 85
    - understanding options 146
    - understanding types 89
    - upgrading 24
    - USER\_PROFILE\_XFR service operation 6
    - USER\_PROFILE component interface 5
    - USER\_PROFILE service operation 6
    - user IDs *See Also* user IDs
    - user IDs, running queries for 105
    - user IDs, setting values 99
    - USERMAINT\_SELF component interface 5
    - users, identifying 99
    - users, selecting alternate 102
    - using the LDAP\_ProfileSynch function 171
  - User Profiles - General page 95
  - user profile synchronization 123
    - configurable 130
    - implementing configurable 127
    - implementing standard 124
    - types 124
  - User Profile Types page 91
  - users
    - access IDs *See Also* access profiles
    - deleting 7
    - enabling email recipient lookup 80
    - passwords *See Also* passwords
    - personalization personalization
    - profiles user profiles
    - removing from roles 70
    - roles *See Also* roles
    - setting PeopleSoft system timeouts 33
    - setting routing options 79
    - tracking login/logout activities 118
    - understanding connect IDs 18
    - understanding symbolic IDs 19
    - user IDs *See Also* user IDs
    - viewing definition access 275
  - USR\_PRFL\_XFR program 7
- ## V
- VeriSign 213
- ## W
- web libraries 55
  - web profiles
    - modifying 180
    - PS\_TOKEN cookie 200
  - web servers
    - authenticating users 171, 178
    - rebooting JVMs 55
    - securing the authentication token 206
    - security exit *See Also* web server security exit
    - setting timeouts 33
    - signing in 182
    - single domain limitations 200
    - single signon configurations (sample) 203
    - single signon transaction (sample) 197
    - using encryption 16
  - web server security exit
    - creating default users 179
    - modifying web profiles 180
    - signing in via the web server 182
    - understanding 179
    - writing signon PeopleCode programs 181
  - web services

- setting permissions 57
- Windows
  - encryption library filenames 246
  - OpenSSL command line program 251
  - security exit *See Also* Windows security exit
  - setting language preferences 97
  - signing in to the PeopleSoft database 20
  - understanding access/connect IDs 18
- Windows security exit
  - customizing PSUSER.DLL 185
  - implementing a customized PSUSER.DLL 188
  - understanding 183
- Workflow page 79, 101
- workflows
  - entering email addresses 97
  - PeopleSoft Workflow
    - See Also* PeopleSoft Workflow
  - reassigning to users 103
  - setting user routing options 79
  - specifying user profile settings 101
- WWW\_Authentication function 170, 171

## X

- X.509 certificates
  - accessing 178
  - defining algorithm keysets 250
- XML messaging 213

## Z

- z/OS job controls 50

