



EnterpriseOne Tools 8.94

PeopleBook: System Administration

November 2004

EnterpriseOne Tools 8.94 PeopleBook: System Administration
SKU E1_TOOLS8.94TSA-B 1104

Copyright © 2004 PeopleSoft, Inc. All rights reserved.

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

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

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

PeopleSoft, PeopleTools, PS/nVision, PeopleCode, PeopleBooks, PeopleTalk, and Vantive are registered trademarks, and Pure Internet Architecture, Intelligent Context Manager, and The Real-Time Enterprise are trademarks of PeopleSoft, Inc. All other company and product names may be trademarks of their respective owners. The information contained herein is subject to change without notice.

Open Source Disclosure

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

Apache Software Foundation

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

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

OpenSSL

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

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

SSLey

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

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

Loki Library

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

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

Contents

General Preface

About This PeopleBook	xxiii
PeopleSoft Application Prerequisites.....	xxiii
PeopleSoft Application Fundamentals.....	xxiii
Documentation Updates and Printed Documentation.....	xxiv
Obtaining Documentation Updates.....	xxiv
Ordering Printed Documentation.....	xxiv
Additional Resources.....	xxv
Typographical Conventions and Visual Cues.....	xxvi
Typographical Conventions.....	xxvi
Visual Cues.....	xxvii
Country, Region, and Industry Identifiers.....	xxvii
Currency Codes.....	xxviii
Comments and Suggestions.....	xxviii
Common Elements Used in PeopleBooks.....	xxviii

Preface

System Administration Preface.....	xxxii
PeopleSoft Products.....	xxxii
PeopleSoft EnterpriseOne System Administration.....	xxxii

Chapter 1

Getting Started with PeopleSoft Tools System Administration.....	1
PeopleSoft Tools System Administration Overview.....	1
Implementation.....	2

Chapter 2

Administering the Data Dictionary.....	3
Understanding Data Dictionary Administration.....	3
Updating Display Decimals in Data Dictionary.....	4
Updating Display Decimals.....	4

Chapter 3

Configuring Object Management Workbench.....	7
Understanding Object Management Workbench Administration.....	7
Default Projects.....	8
Project Constants.....	8
Project and Object Logging.....	8
Activity Rules.....	9
Allowed Actions.....	9
Object Save Locations.....	9
Object Action Notifications.....	9
Notification Subscriptions.....	9
The Configuration Process Flow.....	10
OMW Application and User Role Security.....	11
Securing OMW Applications.....	11
Securing User Roles.....	11
Securing Administrative Updates.....	11
Choosing a Configuration Option.....	12
Understanding Configuration Settings Indicators.....	12
Choosing a Configuration Option.....	12
Configuring OMW User Roles and Allowed Actions.....	13
Understanding OMW User Roles and Allowed Actions.....	13
Example of Allowed Actions for an OMW Role.....	15
Prerequisite.....	16
Forms Used to Configure OMW User Roles and Allowed Actions.....	16
Modifying a User Role.....	16
Deleting a User Role.....	17
Setting Up Allowed User Actions.....	17
Configuring OMW Functions.....	20
Understanding OMW Functions.....	20
Forms Used to Configure OMW Functions.....	20
Disabling SAR Integration.....	20
Controlling Logging Detail.....	21
Controlling Development in the Event of Logging Failure.....	22
Setting Up Project Constants.....	22
Configuring Activity Rules.....	23
Understanding Activity Rules.....	23
Forms Used to Configure Activity Rules.....	26
Setting Up Project Status Activity Rules.....	26
Setting Up Object Transfer Activity Rules.....	27
Configuring Object Save Locations.....	29

Understanding Object Save Locations.....	29
Forms Used to Configure Object Save Locations.....	29
Creating an Object Save Location.....	30
Modifying an Object Save Location.....	30
Deleting an Object Save Location Record.....	30
Configuring Notification Subscriptions.....	31
Understanding Notification Subscriptions.....	31
Forms Used to Configure Notification Subscriptions.....	31
Enabling or Disabling Object Action Notifications.....	31
Adding a Notification Subscription.....	32
Modifying a Notification Subscription.....	33
Deleting a Notification Subscription.....	33
Sorting Notification Subscriptions.....	34
Working with OMW Logs.....	34
Understanding OMW Logs.....	34
Forms Used to Work with OMW Logs.....	35
Viewing Project or Object Logs.....	35
Locating Object Logs.....	35
Locating Project Logs.....	38
Viewing Detail Logs.....	39
Reordering Log Record Fields.....	39
Printing Logs.....	40

Chapter 4

Setting Up EnterpriseOne Printing.....	41
Understanding EnterpriseOne Printing.....	41
Printing Reports.....	41
Running Reports on the Server.....	42
Running Reports on the Workstation.....	42
Print-Time Characteristics.....	42
Print Settings for the Workstation jde.ini.....	43
Setting Up Printers.....	43
Understanding Printer Setup.....	43
Adding a Printer.....	44
Defining a Default Printer.....	48
Modifying an Existing Printer.....	49
Copying an Existing Printer.....	49
Deleting a Printer.....	50
Deleting a Paper Type.....	50

Searching for Incorrect Printing Records.....	51
Searching for Incorrect Printer Records.....	51
Determining Which Batch Processes are Attached to Printers.....	51
Determining Which Batch Processes are Attached to Printers.....	51
Generating and Retrieving Logs for Your Report.....	52
Understanding jde.ini Settings for the Report Logs Directory.....	52
Forms Used to Create Logs for Your Report.....	53
Creating Logs for Your Report.....	53
Setting Up a Printer to Use a Barcode Font.....	54
Forms Used to Set Up a Printer to Use a Barcode Font.....	54
Setting Up Barcode Font Printing.....	54
Running Reports on Line Printers.....	54
Understanding How to Run Reports on Line Printers.....	55
Forms Used to Run Reports on Line Printers.....	55
Designing a Report to Run on a Line Printer.....	55
Setting Up a Line Printer.....	56
Printing Multiple Copies to a Remote iSeries Line Printer.....	57

Chapter 5

Working with Servers.....	59
Understanding the Work With Servers Program.....	59
Managing Server Jobs.....	59
Understanding Server Jobs.....	60
Forms Used to Manage Server Jobs.....	61
Setting Processing Options for Work with Servers (P986116).....	62
Checking the Status of Reports.....	62
Changing the Priority and the Printer for Jobs.....	62
Printing Jobs.....	63
Viewing Reports Online.....	63
Viewing the Logs for a Job.....	63
Terminating Jobs.....	64
Holding and Releasing Jobs.....	64
Managing Job Queues.....	64
Understanding Job Queues.....	65
Prerequisites.....	66
Forms Used to Manage Job Queues.....	67
Adding a Job Queue.....	67
Revising a Job Queue.....	68
Copying a Job Queue.....	68

Changing the Status of a Job Queue.....	69
Overriding a Job Queue.....	69
Managing EnterpriseOne Subsystems.....	69
Understanding EnterpriseOne Subsystems.....	70
Forms Used to Manage EnterpriseOne Subsystems.....	73
Locating Subsystems Running on a Server.....	73
Reviewing Job Records for Subsystems.....	74
Terminating Subsystems.....	74

Chapter 6

Working with User Profiles.....	77
Understanding User Profiles.....	77
Understanding How Role Profiles Make Profiling Easier.....	77
Tables Used by the User Profile Revisions Application.....	78
Adding New Users.....	78
Understanding How to Add Users.....	78
Adding an Individual User.....	79
Adding Multiple Users.....	79
Setting Up User Profiles.....	80
Understanding User Profile Setup.....	80
Prerequisites.....	81
Forms Used to Set Up User and Role Profiles.....	82
Setting Processing Options for User Profile Revisions (P0092).....	82
Creating and Modifying User Profiles.....	82
Creating and Modifying Role Profiles.....	84
Copying User and Role Profiles.....	85
Assigning or Deleting Environments to User and Role Profiles.....	85
Assigning Business Preferences to User and Role Profiles.....	86
Creating Profiles by Using a Batch Process.....	86
Reviewing User and Profile Definitions.....	87
Setting Up User Roles.....	88
Understanding User Roles.....	88
Forms Used to Set Up User Roles.....	90
Migrating Roles.....	91
Defining Roles.....	94
Revising Roles.....	95
Sequencing Roles.....	95
Adding an Environment to a Role.....	96
Setting Up a Role Relationship.....	96

Choosing Roles for Display at Sign-in.....	97
Enabling the Role Chooser.....	97
Creating Role-to-Role Relationships.....	98
Revising Role Relationships.....	98
Delegating Roles.....	99
Adding Roles to a User.....	99
Adding Users to a Role.....	100
Copying User Roles.....	101
Adding a Language Translation to a Role.....	101
Changing a Role Description.....	101

Chapter 7

Understanding PeopleSoft EnterpriseOne Security.....	103
PeopleSoft EnterpriseOne Security Overview.....	103
Understanding Users, Roles, and *PUBLIC.....	104
Understanding How PeopleSoft EnterpriseOne Checks Security.....	104
Understanding Cached Security Information.....	105
Understanding Security Types.....	105
Understanding Object-Level Security.....	106

Chapter 8

Using Security Workbench.....	109
Understanding Security Workbench.....	109
Managing Application Security.....	109
Understanding Application Security.....	110
Forms Used to Manage Application Security.....	110
Reviewing the Current Application Security Settings for a User or Role.....	110
Adding Security to an Application.....	111
Securing a User or Role from All PeopleSoft EnterpriseOne Objects.....	112
Changing Security for an Application.....	112
Removing Security from an Application.....	113
Securing Users to a Form in an Application.....	115
Managing Action Security.....	116
Understanding Action Security.....	116
Forms Used to Manage Action Security.....	116
Reviewing the Current Action Security Settings for a User or Role.....	116
Adding Action Security.....	117
Changing Action Security.....	118

Removing Action Security.....	118
Managing Row Security.....	119
Understanding Row Security.....	119
Forms Used to Manage Row Security.....	120
Setting Up Row Security.....	120
Removing Row Security.....	121
Managing Column Security.....	121
Understanding Column Security.....	121
Forms Used to Manage Column Security.....	123
Setting Up Column Security.....	123
Removing Column Security.....	123
Managing Processing Option Security.....	124
Understanding Processing Option Security.....	124
Forms Used to Set Up Processing Option Security.....	125
Reviewing the Current Processing Option Security Settings.....	125
Adding Security to Processing Options.....	125
Changing Security for Processing Options.....	126
Removing Security from Processing Options.....	127
Managing Tab Security.....	127
Understanding Tab Security.....	128
Forms Used to Manage Tab Security.....	128
Adding Security to a Tab.....	128
Changing Security for a Tab.....	129
Removing Security from a Tab.....	129
Managing Exit Security.....	130
Understanding Exit Security.....	130
Forms Used to Manage Exit Security.....	130
Setting Up Exit Security.....	130
Adding Security to an Exit.....	131
Changing Security for an Exit.....	132
Removing Security from an Exit.....	132
Managing Exclusive Application Security.....	133
Understanding Exclusive Application Security.....	133
Forms Used to Manage Exclusive Application Security.....	133
Adding Access with Exclusive Application Security.....	133
Removing Exclusive Application Access.....	134
Managing External Calls Security.....	134
Understanding External Call Security.....	135
Forms Used to Manage External Call Security.....	135
Setting Up Security for External Calls.....	135

Adding External Call Security.....	135
Changing External Call Security.....	136
Removing External Call Security.....	136
Managing Miscellaneous Security.....	137
Understanding Miscellaneous Security.....	137
Forms Used to Manage Miscellaneous Security.....	138
Managing Miscellaneous Security Features.....	138
Copying Security for a User or a Role.....	139
Understanding How to Copy Security for a User or a Role.....	139
Forms Used to Copy Security.....	139
Copying All Security Records for a User or a Role.....	139
Copying a Single Security Record for a User or a Role.....	140
Using Alternate Methods to Delete User or Role Security.....	140
Understanding Alternate Methods of Deleting User or Role Security.....	140
Form Used to Delete User or Role Security.....	140
Deleting User or Role Security.....	140
Deleting Security on the Work With User/Role Security Form.....	141

Chapter 9

Setting Up Address Book Data Security.....	143
Understanding Address Book Data Security.....	143
Prerequisites.....	144
Setting Up Permission List Definitions.....	144
Understanding Permission List Definitions.....	144
Forms Used to Set Up Permission List Definitions.....	145
Creating Permission List Definitions.....	145
Setting Up Permission List Relationships.....	146
Understanding Permission List Relationships.....	146
Forms Used to Create Permission List Relationships.....	146
Creating Permission List Relationships.....	146

Chapter 10

Setting Up Business Unit Security.....	149
Business Unit Security Overview.....	149
UDC Sharing.....	149
Transaction Security.....	149
Working with UDC Sharing.....	150
Setting Up UDC Sharing.....	150

Setting Up Business Unit Security for UDC Sharing.....	151
Revising UDC Groups.....	152
Working with Transaction Security.....	152
Understanding How to Set Up Transaction Security.....	152
Setting Up Transaction Security.....	153
Revising Transaction Security.....	153

Chapter 11

Employing Sign-in Security.....	155
Understanding Sign-in Security.....	155
Security Table Access.....	156
Password Encryption.....	156
Security Setup.....	156
Process Flow for Sign-in Security.....	157
Sign-in Security for Web Users.....	162
Setting Processing Options for P98OWSEC.....	165

Chapter 12

Setting Up User Security.....	167
Understanding User Security.....	167
Creating and Revising User Security.....	167
Understanding How to Create and Revise User Security.....	168
Prerequisites.....	168
Forms Used to Create and Revise User Security.....	169
Creating User Security.....	169
Copying User Security.....	171
Revising User and Role Security.....	172
Revising All User Security.....	172
Changing a Sign-in Password.....	173
Requiring Sign-in Security.....	173
Reviewing Security History.....	174
Prerequisite.....	174
Forms Used to Review Security History.....	174
Managing Data Sources for User Security.....	174
Understanding Data Source Management for User Security.....	174
Forms Used to Manage Data Sources for User Security.....	175
Adding a Data Source to a User, a Role, or All Users.....	175
Revising a Data Source for a User, a Role, or All Users.....	175

Removing a Data Source for a User, Role, or All Users.....	176
Enabling and Synchronizing Security Settings.....	176
Understanding Security Setting Synchronization.....	177
Changing the Workstation jde.ini File for User Security.....	177
Setting Auxiliary Security Servers in the Workstation jde.ini.....	177
Changing the Timeout Value Due to Security Server Communication Error.....	178
Changing the Enterprise Server jde.ini File for Security.....	178
Setting Auxiliary Security Servers in the Server jde.ini.....	179
Verifying Security Processes in the Server jde.ini.....	180
Running a Security Analyzer Report.....	180
Understanding the Security Analyzer Report.....	180
Form Used to Run a Security Analyzer Report.....	181
Running the Security Analyzer by Data Source Report (R98OWSECA).....	181
Running the Security Analyzer by User or Group Report (R98OWSECB).....	182
Managing Unified Logon.....	183
Understanding Unified Logon.....	183
Modifying the jde.ini Setting to Enable or Disable Unified Logon.....	183
Setting Up a Service for Unified Logon.....	184
Removing a Service for Unified Logon.....	184

Chapter 13

Setting Up Solution Explorer Security.....	185
Understanding Solution Explorer Security.....	185
Default Security Settings.....	186
Forms Used to Set Up Solution Explorer Security.....	186
Configuring Solution Explorer Security.....	186

Chapter 14

Employing LDAP in PeopleSoft EnterpriseOne.....	187
Understanding LDAP Support for PeopleSoft EnterpriseOne.....	187
LDAP and PeopleSoft EnterpriseOne Relationships.....	188
Understanding LDAP and PeopleSoft EnterpriseOne Relationships.....	188
Implementing LDAP Support in PeopleSoft EnterpriseOne.....	191
LDAP Support Implementation Overview.....	191
Understanding How PeopleSoft EnterpriseOne Uses LDAP Server Settings.....	192
Enabling LDAP Authentication Mode.....	194
Creating an LDAP Configuration.....	194
Configuring the LDAP Server Settings.....	195

Configuring LDAP to PeopleSoft EnterpriseOne Enterprise Server Mappings.....	197
Changing the LDAP Configuration Status.....	198
LDAP Default User Profile Settings.....	199
Understanding LDAP Default User Profile Settings.....	199
Reviewing the Current LDAP Default Settings.....	199
Modifying the Default User Profile Settings for LDAP.....	200
Modifying the Default Role Relationships for LDAP.....	200
Modifying the Default User Security Settings for LDAP.....	201
LDAP-Enabled PeopleSoft EnterpriseOne Application Changes.....	201
Understanding Application Changes in LDAP-Enabled PeopleSoft EnterpriseOne.....	202
User Password Changes.....	202
User Profile Revisions Application Changes.....	202
Security Revisions Application Changes.....	202
User-Role Relationships Preferences Application Changes.....	203
Scheduler Application Changes.....	203
User Profile Self-Service Application Changes.....	203
LDAP Server-Side Administration.....	204
PeopleSoft EnterpriseOne Server-Side Administration.....	205
Using LDAP Bulk Synchronization (R9200040).....	206
Example: LDAP Bulk Synchronization (R9200040).....	207
Using LDAP Over SSL.....	207
Enabling LDAP Authentication Over SSL for Windows and UNIX.....	207
Enabling LDAP Authentication Over SSL for iSeries.....	208

Chapter 15

Understanding PeopleSoft EnterpriseOne Single Signon.....	209
PeopleSoft EnterpriseOne Single Signon Overview.....	209
PeopleSoft Authenticate Token.....	209
Understanding Nodes.....	210
How a Node Validates an Authenticate Token.....	211
How Single Signon Works.....	212
Launching an PeopleSoft EnterpriseOne Application from Enterprise Portal.....	212
Launching an PeopleSoft EnterpriseOne Application from PeopleSoft EnterpriseOne Collaborative Portal.....	214

Chapter 16

Setting Up EnterpriseOne Single Signon.....	215
Default Settings for Single Signon Node Configuration.....	215
Setting Up a Node Configuration.....	215

Understanding Single Signon Configurations and Their Relationships.....	216
Adding a Node Configuration.....	217
Revising a Node Configuration.....	217
Changing the Status of a Node.....	217
Deleting a Node Configuration.....	218
Setting Up a Token Lifetime Configuration Record.....	218
Adding a Token Lifetime Configuration Record.....	218
Deleting a Token Lifetime Configuration Record.....	218
Setting Up a Trusted Node Configuration.....	219
Adding a Trusted Node Configuration.....	219
Deleting a Trusted Node Configuration.....	219
Configuring Single Signon for a Pre-EnterpriseOne 8.11 Release.....	219
Understanding Single Signon for a Pre-EnterpriseOne 8.11.....	219
jde.ini file Node Setting Modifications for Single Signon.....	220
Sample jde.ini Node Settings for Single Signon.....	220
Example 2:.....	221
Configuring Single Signon Without a Security Server.....	221
Configuring Single Signon for Collaborative Portal.....	222
Configuring Single Signon for Portlets.....	222
Configuring tokeneng.ini File Settings.....	223
EnterpriseOne Portlet (JSR168).....	223
Collaborative Portal EnterpriseOne Menu.....	223
Hosted EnterpriseOne Portlet.....	223
CSS, ESS, SSS.....	223
EnterpriseOne Links.....	224
CRM.....	224
Configuring Single Signon Between Enterprise Portal and EnterpriseOne.....	224
Understanding Single Signon Between Enterprise Portal and EnterpriseOne.....	224
Time Zone Adjustment for Enterprise Portal.....	225
User ID Mapping for Single Signon.....	225
Managing User ID Mapping in EnterpriseOne.....	225
Managing User ID Mapping when Using LDAP.....	226
Synchronizing User Mappings Between LDAP and EnterpriseOne While Using LDAP Authentication.....	226
Viewing User ID Mapping When Using LDAP.....	227
 Chapter 17	
Setting Up PIM Synchronization for PeopleSoft EnterpriseOne CRM Users.....	229
Understanding PIM Synchronization.....	229

User Defined Codes for PIM.....	230
Prerequisites.....	230
Setting Up the PIM Server Processing Option.....	230
Setting Up Users for PIM Synchronization.....	231
Exporting PIM User Records.....	232
Importing PIM Synchronization Files into Intellisync Server.....	233

Chapter 18

Enabling Mobile Client Functionality.....	235
Understanding Distributed Next Numbers for Mobile Clients.....	235
Setting Up Distributed Next Numbers for Mobile Clients.....	235
Activating Mobile Client Functionality.....	235
Defining the Starting Next Number.....	236
Enabling Distributed Next Numbers.....	236
Setting Up Distributed Next Numbers by System.....	237
Mapping the EnterpriseOne User ID to the Distributed Next Numbers Application (P950411).....	238
Setting Up Distributed Next Numbers by Application.....	238
Scheduling Updates to Distributed Next Numbers Applications.....	240

Chapter 19

Working with Vocabulary Overrides.....	241
Understanding Vocabulary Overrides.....	241
Creating Vocabulary Overrides.....	241
Forms Used to Work with Vocabulary Overrides.....	242
Accessing Vocabulary Overrides from PeopleSoft Solution Explorer.....	242
Accessing Vocabulary Overrides from Object Management Workbench.....	243
Creating Vocabulary Overrides.....	244
Creating Batch Vocabulary Overrides.....	245
Reviewing Vocabulary Overrides.....	246
Resetting a Vocabulary Override.....	246
Resetting All Vocabulary Overrides on a Form (Interactive and Batch).....	247

Chapter 20

Using the Scheduler Application.....	249
Understanding the Scheduler Application.....	249
Working with the Job Scheduler.....	250
Understanding the Job Scheduler.....	251

Prerequisite.....	251
Forms Used to Work with the Job Scheduler.....	251
Setting Processing Options for the Job Scheduler.....	252
Scheduling a Job.....	252
Scheduling a Recurring Job.....	253
Revising a Scheduled Job.....	255
Reviewing All Jobs or Local Jobs.....	256
Using Advanced Scheduling Options.....	256
Understanding Advanced Scheduling Options.....	256
Forms Used to Work with Advanced Scheduling Options.....	257
Overriding the Environment.....	257
Overriding Job Expiration Specifications.....	257
Defining When the Scheduler Resubmits a Job.....	258
Overriding Batch Application Specifications.....	259
Adding Values to a Report Interconnect.....	260
Reviewing the Job Schedule.....	260
Understanding Job Schedule Reviewing.....	260
Forms Used to Review the Job Schedule.....	261
Reviewing All Job Schedules.....	261
Changing the Launch Status of a Job.....	262
Viewing Job Details.....	262
Setting the Job Status Manually.....	262
Resetting the Job Schedule.....	263
Working With the Scheduler Server.....	263
Understanding the Scheduler Server.....	263
Forms Used to Work With the Scheduler Server.....	265
Stopping or Restarting the Scheduler Server.....	265
Pausing the Job Launcher or Job Monitor.....	266
Resetting the Scheduler Server.....	266
Refreshing the Scheduler Server Settings.....	266
Modifying the Scheduler Server and Monitor Sleep Time.....	267
Working with Daylight Savings Rules.....	267
Understanding How to Work with Daylight Savings Rules.....	267
Forms Used to Work with Daylight Savings Rules.....	267
Adding Daylight Savings Rules.....	267
Revising Daylight Savings Rules.....	268
Running Scheduler Reports.....	268
Printing the Scheduled Jobs or Purge Scheduled Jobs Report.....	269

Chapter 21

Understanding Media Objects and Imaging.....	271
Media Objects.....	271
PeopleSoft EnterpriseOne Text Items.....	272
Imaging.....	272
Media Object Queues.....	272
Image Media Objects.....	273
OLE Media Objects.....	273
URL Media Objects.....	273
Media Object Tables.....	273
Language Considerations for Media Objects.....	273

Chapter 22

Setting Up Media Objects and Imaging.....	275
Understanding Media Object Processing.....	275
Prerequisite.....	276
Enabling EnterpriseOne to Use Media Objects.....	276
Adding a Language-Specific Media Object Attachment.....	277
Setting Up Media Object Queues.....	277
Forms Used to Set Up Media Object Queues.....	277
Adding a Media Object Queue.....	277
Defining the Location of a Media Object Queue.....	278
Deleting a Media Object Queue.....	279
Setting Up Imaging.....	279
Understanding Imaging.....	279
Forms Used to Set Up Imaging.....	282
Enabling Imaging in Media Objects.....	282

Chapter 23

Administering Text Search Indices.....	283
Understanding Verity.....	283
Defining Text Search Indices.....	283
Understanding Text Search Indices.....	283
Forms Used to Define Text Search Indices.....	284
Designating Data Sources for a Business View.....	284
Defining Media Objects for a Text Search Index.....	284
Defining Languages for a Text Search Index.....	285
Building Text Search Indices.....	285

Defining Text Search Properties.....	285
Understanding Text Search Properties.....	286
Forms Used to Define Text Search Properties.....	287
Adding a New Text Search Business View-Data Source Pair.....	287
Defining Stop Words.....	288
Defining Synonyms.....	288
Defining Topics.....	288

Chapter 24

Using the Universal Table Browser.....	289
Understanding the Universal Table Browser.....	289
Viewing the Data in Tables.....	289
Viewing Column Properties in a Table.....	290

Chapter 25

Working with Flat File Encoding.....	291
Understanding Flat File Encoding.....	291
Example: Setting Up Flat File Encoding Records.....	292
Forms Used to Work with Flat File Encoding.....	294
Adding a Flat File Encoding Record.....	294
Activating a Flat File Encoding Record.....	295

Chapter 26

Understanding Naming Conventions.....	297
Naming Conventions Overview.....	297
Path Codes.....	297
Data Sources.....	297
Package Names.....	298
Server Names.....	299
Workstation Names.....	299

Chapter 27

Understanding the Jde.ini File Settings.....	301
Jde.ini File Overview.....	301
How to Use This Section.....	301
Locating the Jde.ini File.....	302

Workstation Jde.ini Settings.....	302
[ACTIVE DIRECTORY].....	302
[DB SYSTEM SETTINGS].....	302
[DB SYSTEM SETTINGS - SECONDARY].....	305
[DEBUG].....	306
[EVEREST].....	307
[INSTALL].....	307
[JDE_CG].....	309
[JDEMAIL].....	309
[JDENET].....	310
[JDENET_KERNEL_DEFx].....	310
[LOCK MANAGER].....	311
[MAILMERGE].....	311
[NETWORK QUEUE SETTINGS].....	312
[OBJECT LIBRARIAN].....	312
[OFFLINE DB SYSTEM SETTINGS].....	313
[SECURITY].....	315
[SVR].....	315
[UBE].....	317
[WORKFLOW].....	319
iSeries Server Jde.ini Settings.....	319
[AS400].....	319
[BSFN BUILD].....	320
[DB SYSTEM SETTINGS].....	322
[DEBUG].....	325
[ENTERPRISE TIMEZONE ADJUSTMENT].....	326
[INSTALL].....	326
[INTEROPERABILITY].....	327
[JDEIPC].....	327
[JDEITDRV].....	328
[JDEMAIL].....	328
[JDENET].....	329
[JDENET_KERNEL_DEFx].....	331
[LOCK MANAGER].....	336
[LREngine].....	337
[NETWORK QUEUE SETTINGS].....	337
[SAMPLE_EVENT].....	337
[SECURITY].....	337
[SVR].....	339
[TCENGINE].....	339

[UBE].....	340
[WORKFLOW].....	341
[WORLD ENVIRONMENT MAP].....	341
[XML Dispatch].....	342
[XTS].....	342
UNIX/Linux Server Jde.ini Settings.....	342
[BSFN BUILD].....	342
[CLUSTER].....	344
[DB SYSTEM SETTINGS].....	345
[DEBUG].....	346
[ENTERPRISE TIMEZONE ADJUSTMENT].....	347
[INSTALL].....	347
[INTEROPERABILITY].....	348
[JDEIPC].....	348
[JDEITDRV].....	348
[JDEMAIL].....	349
[JDENET].....	349
[JDENET_KERNEL_DEFx].....	351
[LOCK MANAGER].....	355
[LREngine].....	355
[NETWORK QUEUE SETTINGS].....	356
[SAMPLE_EVENT].....	356
[SECURITY].....	356
[SERVER ENVIRONMENT MAP].....	357
[SVR].....	357
[WORKFLOW].....	358
[XML Dispatch].....	359
[XTS].....	359
Windows Enterprise Server Jde.ini Settings.....	359
[ACTIVE DIRECTORY].....	359
[BSFN BUILD].....	360
[BSFN Builder].....	361
[DB SYSTEM SETTINGS].....	362
[DEBUG].....	363
[ENTERPRISE TIMEZONE ADJUSTMENT].....	365
[INSTALL].....	365
[INTEROPERABILITY].....	366
[JDE_CG].....	367
[JDEIPC].....	367
[JDEITDRV].....	368

[JDEMAIL].....	369
[JDENET].....	369
[LOCK MANAGER].....	371
[LREngine].....	372
[MQSI].....	372
[NETWORK QUEUE SETTINGS].....	373
[SAMPLE_EVENT].....	375
[SECURITY].....	375
[SERVER ENVIRONMENT MAP].....	376
[SVR].....	376
Server Jde.ini Settings for WebSphere.....	377
[JDENET].....	377
[JDENET_KERNEL_DEF13].....	377
[MQSI].....	378
Web Server Jas.ini Settings.....	379
[CACHE].....	381
[JAS PREFERENCE].....	383
[JDENET].....	383
[LOGS].....	383
[OWWEB].....	384
[PORTALCONFIGURATION].....	387
[SECURITY].....	393
[SERVER].....	394
[SERVER COMPONENTS].....	395
Web Server Jdbj.ini Settings.....	395
PeopleSoft EnterpriseOne Data-Specific Sections.....	396
General Sections.....	399
Glossary of PeopleSoft Terms.....	409
Index	429

About This PeopleBook

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

This preface discusses:

- PeopleSoft application prerequisites.
- PeopleSoft application fundamentals.
- Documentation updates and printed documentation.
- Additional resources.
- Typographical conventions and visual cues.
- Comments and suggestions.
- Common elements in PeopleBooks.

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

PeopleSoft Application Prerequisites

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

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

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

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

PeopleSoft Application Fundamentals

Each application PeopleBook provides implementation and processing information for your PeopleSoft applications. For some applications, additional, essential information describing the setup and design of your system appears in a companion volume of documentation called the application fundamentals PeopleBook. Most PeopleSoft product lines have a version of the application fundamentals PeopleBook. The preface of each PeopleBook identifies the application fundamentals PeopleBooks that are associated with that PeopleBook.

The application fundamentals PeopleBook consists of important topics that apply to many or all PeopleSoft applications across one or more product lines. Whether you are implementing a single application, some combination of applications within the product line, or the entire product line, you should be familiar with the contents of the appropriate application fundamentals PeopleBooks. They provide the starting points for fundamental implementation tasks.

Documentation Updates and Printed Documentation

This section discusses how to:

- Obtain documentation updates.
- Order printed documentation.

Obtaining Documentation Updates

You can find updates and additional documentation for this release, as well as previous releases, on the PeopleSoft Customer Connection website. Through the Documentation section of PeopleSoft Customer Connection, you can download files to add to your PeopleBook Library. You'll find a variety of useful and timely materials, including updates to the full PeopleSoft documentation that is delivered on your PeopleBooks CD-ROM.

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

See Also

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

Ordering Printed Documentation

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

- Web
- Telephone
- Email

Web

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

Telephone

Contact MMA Partners at 877 588 2525.

Email

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

See Also

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

Additional Resources

The following resources are located on the PeopleSoft Customer Connection website:

Resource	Navigation
Application maintenance information	Updates + Fixes
Business process diagrams	Support, Documentation, Business Process Maps
Interactive Services Repository	Interactive Services Repository
Hardware and software requirements	Implement, Optimize + Upgrade, Implementation Guide, Implementation Documentation & Software, Hardware and Software Requirements
Installation guides	Implement, Optimize + Upgrade, Implementation Guide, Implementation Documentation & Software, Installation Guides and Notes
Integration information	Implement, Optimize + Upgrade, Implementation Guide, Implementation Documentation and Software, Pre-built Integrations for PeopleSoft Enterprise and PeopleSoft EnterpriseOne Applications
Minimum technical requirements (MTRs) (EnterpriseOne only)	Implement, Optimize + Upgrade, Implementation Guide, Supported Platforms
PeopleBook documentation updates	Support, Documentation, Documentation Updates
PeopleSoft support policy	Support, Support Policy
Prerelease notes	Support, Documentation, Documentation Updates, Category, Prerelease Notes
Product release roadmap	Support, Roadmaps + Schedules
Release notes	Support, Documentation, Documentation Updates, Category, Release Notes
Release value proposition	Support, Documentation, Documentation Updates, Category, Release Value Proposition
Statement of direction	Support, Documentation, Documentation Updates, Category, Statement of Direction

Resource	Navigation
Troubleshooting information	Support, Troubleshooting
Upgrade documentation	Support, Documentation, Upgrade Documentation and Scripts

Typographical Conventions and Visual Cues

This section discusses:

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

Typographical Conventions

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

Typographical Convention or Visual Cue	Description
Bold	Indicates PeopleCode function names, business function names, event names, system function names, method names, language constructs, and PeopleCode reserved words that must be included literally in the function call.
<i>Italics</i>	Indicates field values, emphasis, and PeopleSoft or other book-length publication titles. In PeopleCode syntax, italic items are placeholders for arguments that your program must supply. We also use italics when we refer to words as words or letters as letters, as in the following: Enter the letter <i>O</i> .
KEY+KEY	Indicates a key combination action. For example, a plus sign (+) between keys means that you must hold down the first key while you press the second key. For ALT+W, hold down the ALT key while you press the W key.
Monospace font	Indicates a PeopleCode program or other code example.
“ ” (quotation marks)	Indicate chapter titles in cross-references and words that are used differently from their intended meanings.

Typographical Convention or Visual Cue	Description
... (ellipses)	Indicate that the preceding item or series can be repeated any number of times in PeopleCode syntax.
{ } (curly braces)	Indicate a choice between two options in PeopleCode syntax. Options are separated by a pipe ().
[] (square brackets)	Indicate optional items in PeopleCode syntax.
& (ampersand)	When placed before a parameter in PeopleCode syntax, an ampersand indicates that the parameter is an already instantiated object. Ampersands also precede all PeopleCode variables.

Visual Cues

PeopleBooks contain the following visual cues.

Notes

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

Note. Example of a note.

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

Important! Example of an important note.

Warnings

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

Warning! Example of a warning.

Cross-References

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

Country, Region, and Industry Identifiers

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

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

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

Country Identifiers

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

Region Identifiers

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

- Asia Pacific
- Europe
- Latin America
- North America

Industry Identifiers

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

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

Currency Codes

Monetary amounts are identified by the ISO currency code.

Comments and Suggestions

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

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

Or send email comments to doc@peoplesoft.com.

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

Common Elements Used in PeopleBooks

Address Book Number

Enter a unique number that identifies the master record for the entity. An address book number can be the identifier for a customer, supplier, company, employee, applicant, participant, tenant, location, and so on. Depending on the application, the field on the form might refer to the address book number as the customer number, supplier number, or company number, employee or applicant id, participant number, and so on.

As If Currency Code	Enter the three-character code to specify the currency that you want to use to view transaction amounts. This code allows you to view the transaction amounts as if they were entered in the specified currency rather than the foreign or domestic currency that was used when the transaction was originally entered.
Batch Number	Displays a number that identifies a group of transactions to be processed by the system. On entry forms, you can assign the batch number or the system can assign it through the Next Numbers program (P0002).
Batch Date	Enter the date in which a batch is created. If you leave this field blank, the system supplies the system date as the batch date.
Batch Status	<p>Displays a code from user-defined code (UDC) table 98/IC that indicates the posting status of a batch. Values are:</p> <p><i>Blank:</i> Batch is unposted and pending approval.</p> <p><i>A:</i> The batch is approved for posting, has no errors and is in balance, but it has not yet been posted.</p> <p><i>D:</i> The batch posted successfully.</p> <p><i>E:</i> The batch is in error. You must correct the batch before it can post.</p> <p><i>P:</i> The system is in the process of posting the batch. The batch is unavailable until the posting process is complete. If errors occur during the post, the batch status changes to E.</p> <p><i>U:</i> The batch is temporarily unavailable because someone is working with it, or the batch appears to be in use because a power failure occurred while the batch was open.</p>
Branch/Plant	Enter a code that identifies a separate entity as a warehouse location, job, project, work center, branch, or plant in which distribution and manufacturing activities occur. In some systems, this is called a business unit.
Business Unit	Enter the alphanumeric code that identifies a separate entity within a business for which you want to track costs. In some systems, this is called a branch/plant.
Category Code	Enter the code that represents a specific category code. Category codes are user-defined codes that you customize to handle the tracking and reporting requirements of your organization.
Company	Enter a code that identifies a specific organization, fund, or other reporting entity. The company code must already exist in the F0010 table and must identify a reporting entity that has a complete balance sheet.
Currency Code	Enter the three-character code that represents the currency of the transaction. PeopleSoft EnterpriseOne provides currency codes that are recognized by the International Organization for Standardization (ISO). The system stores currency codes in the F0013 table.
Document Company	<p>Enter the company number associated with the document. This number, used in conjunction with the document number, document type, and general ledger date, uniquely identifies an original document.</p> <p>If you assign next numbers by company and fiscal year, the system uses the document company to retrieve the correct next number for that company.</p>

If two or more original documents have the same document number and document type, you can use the document company to display the document that you want.

Document Number

Displays a number that identifies the original document, which can be a voucher, invoice, journal entry, or time sheet, and so on. On entry forms, you can assign the original document number or the system can assign it through the Next Numbers program.

Document Type

Enter the two-character UDC, from UDC table 00/DT, that identifies the origin and purpose of the transaction, such as a voucher, invoice, journal entry, or time sheet. PeopleSoft EnterpriseOne reserves these prefixes for the document types indicated:

P: Accounts payable documents.

R: Accounts receivable documents.

T: Time and pay documents.

I: Inventory documents.

O: Purchase order documents.

S: Sales order documents.

Effective Date

Enter the date on which an address, item, transaction, or record becomes active. The meaning of this field differs, depending on the program. For example, the effective date can represent any of these dates:

- The date on which a change of address becomes effective.
- The date on which a lease becomes effective
- The date on which a price becomes effective.
- The date on which the currency exchange rate becomes effective.
- The date on which a tax rate becomes effective.

Fiscal Period and Fiscal Year

Enter a number that identifies the general ledger period and year. For many programs, you can leave these fields blank to use the current fiscal period and year defined in the Company Names & Number program (P0010)

G/L Date (general ledger date)

Enter the date that identifies the financial period to which a transaction will be posted. The system compares the date that you enter on the transaction to the fiscal date pattern assigned to the company to retrieve the appropriate fiscal period number and year, as well as to perform date validations.

System Administration Preface

This preface discusses the System Administration PeopleBook.

PeopleSoft Products

This PeopleBook refers to this PeopleSoft product line: PeopleSoft EnterpriseOne Tools.

PeopleSoft EnterpriseOne System Administration

The chapters within this guide contain concepts and processes for administering the various PeopleSoft EnterpriseOne Tools, such as Data Dictionary, Object Management Workbench, the Scheduler application, and so forth. It also contains information on how to manage EnterpriseOne users and security, which includes setting up user profiles, user security, and application security.

CHAPTER 1

Getting Started with PeopleSoft Tools System Administration

This chapter provides an overview of the various system administration tasks for PeopleSoft EnterpriseOne.

PeopleSoft Tools System Administration Overview

This guide is written mainly for EnterpriseOne system administrators, although those with other job functions might find the information useful or essential to their positions as well. This guide focuses primarily on how to:

- Administer the data dictionary.
- Configure Object Management Workbench (OMW) to automate many of the object management tasks that users perform in the software.
- Configure printers within EnterpriseOne.
- Monitor and manager server jobs and EnterpriseOne subsystems.
- Set up user profiles.
- Secure users and groups from EnterpriseOne applications and features.
- Employ sign-in security.
- Set up user security.
- Employ LDAP in EnterpriseOne.
- Set up single signon.
- Set up PIM synchronization for PeopleSoft EnterpriseOne CRM users.
- Enable mobile client functionality.
- Create vocabulary overrides to customize interactive and batch applications.
- Use the Scheduler application.
- Set up media objects and imaging.
- Administer text search indices.
- Use the Universal Table Browser.
- Work with flat file encoding.
- Understand naming conventions.
- Understand the jde.ini file settings.

Implementation

In the planning phase of your implementation, take advantage of all PeopleSoft sources of information, including the installation guides and other EnterpriseOne Tools guides.

Although every attempt has been made to organize the information in this guide according to related tasks, a system administrator or network administrator might find that the information to perform their duties is described in more than one EnterpriseOne Tools guide. For example, the person who is responsible for setting up path codes, environments, and data sources (described in the *EnterpriseOne Tools 8.94 PeopleBook: Configurable Network Computing Implementation*) might also be responsible for building and deploying packages (described in the *EnterpriseOne Tools 8.94 PeopleBook: Package Management*) as well as configuring single signon (described in this guide).

See Also

EnterpriseOne Tools 8.94 PeopleBook: Configurable Network Computing Implementation

EnterpriseOne Tools 8.94 PeopleBook: Package Management

EnterpriseOne Tools 8.94 PeopleBook: Server & Workstation Administration

CHAPTER 2

Administering the Data Dictionary

This chapter provides an overview of data dictionary administration and discusses how to update display decimals.

Understanding Data Dictionary Administration

Just as a dictionary contains word definitions, the PeopleSoft EnterpriseOne data dictionary is a central repository that contains data item definitions and attributes. These attributes determine how a data item:

- Appears on reports and forms.
- Validates data entry within an application.
- Assigns column and row descriptions.
- Provides text for field-sensitive help.

The data dictionary is active because changes that you make are automatically reflected in applications without having to recompile the software.

You should assign one or two people to be the data dictionary administrator for each application area in the enterprise. Data dictionary administrators should be experienced with EnterpriseOne and have a comprehensive knowledge of their product area, such as finance or manufacturing. The data dictionary administrator makes all additions, changes, and deletions to data items for the product group. Such changes are reflected in the pristine data dictionary on the enterprise server.

Data dictionary administrators should consider these issues:

- If the setup is similar to the suggested typical customer configuration, then all environments share the same data dictionary. Therefore, the administrator can log on to any environment to make changes. We recommend that you use the Security Workbench to assign application security on the Data Dictionary application (P92001) to prevent unauthorized users from making data dictionary changes.

See *EnterpriseOne Tools 8.94 PeopleBook: Configurable Network Computing Implementation*, “Typical Customer Configuration”.

- If you are running a coexistence enterprise, you must create all of the data items in both PeopleSoft World and PeopleSoft EnterpriseOne because the two products cannot share the same data dictionary.

See Also

EnterpriseOne Tools 8.94 PeopleBook: Server & Workstation Administration

Updating Display Decimals in Data Dictionary

Data items that belong to the QTYINV data item class come with the display decimal set at 0 (zero). You can change the display decimal to any number up to 8. For example, if you change the display decimal to 4, instead of seeing 100 you will see 100.0000.

Important! You should change the display decimal value in a CRP environment before any live production data is entered. The reason is because PeopleSoft EnterpriseOne does not have a data conversion feature, so if users change display decimals after users have entered data, the data entered before changing the display decimals will be wrong.

Updating Display Decimals

In PeopleSoft Solution Explorer, enter *GH9111* in the Fast Path. Double-click Batch Versions.

To update display decimals:

1. On Work With Batch Versions - Available Versions, enter *R9200100* in the Batch Application field and then click Find.
2. Choose one of the following versions and click Select:
 - Update Display Decimals for Class - Proof
The proof version produces only a report of what the process would do if run in final mode.
 - Update Display Decimals for Class - Final
The final version actually makes the changes.
3. On the Version Prompting form, click Data Selection and then click Submit.
4. On the Data Selection form, create the following statement:

If BC Data Item Class (F9210) = QTYINV

Note. QTYINV is the only data item class for which you can modify display decimals. If you modify other data item classes, you must research and test how the modifications affect the software. Also, if you modify which data items reside in the QTYINV data item class, you must research and test how the modifications affect the software.

5. Click OK.
If you changed the Data Selection statement, first click Update, and then click OK.
6. On Processing Options, complete these fields:
 - Enter *1* to run in Update Mode or *0* to run in Proof Mode. The default is 0.
 - Data Item Class
 - New Data Display Decimals
7. Click OK.
8. On each workstation, delete these spec files:

```
qlbltbl1.ddb, qlbltbl1.xdb
dddict.ddb, dddict.xdb
ddtext.ddb, ddtext.xdb
```

9. To push the display decimal changes out to users, run R92TAM on the server on which the changes were made.

CHAPTER 3

Configuring Object Management Workbench

This chapter provides an overview of Object Management Workbench (OMW) Administration and the recommended process flow for configuring OMW, and discusses:

- The configuration process flow.
- OMW application and user role security.
- Choosing a configuration option.
- Configuring OMW user roles and allowed actions.
- Configuring OMW functions.
- Configuring activity rules.
- Configuring object save locations.
- Configuring notification subscriptions.
- Working with OMW logs.

Understanding Object Management Workbench Administration

Object Management Workbench automates many of the object management tasks that users perform in the software. Much of this automation requires careful configuration by the system administrator through the Object Management Workbench Configuration program.

Use the Object Management Workbench Configuration program to configure the optional features:

- Project constants: Enables you to set general constants pertaining to OMW projects.
- SAR system integration: Enables you to disable SAR system integration with OMW.
- Logging system: Enables you to specify the project and object events to be logged. In the event that logging fails, you can also disable development or allow development but disable transfers.
- Object action notification: Enables you to enable and disable Object Action Notification,
- Notification setup: Enables developers to be notified, using subscription, when actions are performed on an object, such as checkin or checkout.
- Activity rules: Enables you to add and modify project statuses and object transfer activity rules.
- User roles: Enables you to maintain user roles.
- Allowed actions: Enables you to assign to a user role the actions allowed for each object type during a specific project status.

- Save locations: Enables you to add, modify, and delete the locations where you save objects.

Default Projects

When you run OMW for the first time, the system creates a default project and tags it with the user ID. The default project is the personal project that you can use for development and research.

You can use default projects to:

- Develop objects that are later moved into a regular project.
- Store objects to be added to a project later.
- Automatically store objects worked on outside of OMW.

A default project is similar to a project except that the project status of a default project never changes. Therefore, you cannot use a default project to transfer objects.

Non-Object Librarian objects can be accessed outside of OMW. If you access objects such as versions, user defined codes, menus, or the RDA outside of OMW, these objects are added to the default project. Any changes that you make to these objects must be tracked and managed through the default project. Modifications to non-Object Librarian objects are always logged.

If you want to advance the status of an object, use OMW to move the object from the default project to a project.

Project Constants

The Object Management Constants form enables an administrator to set these general constants pertaining to Object Management Workbench projects:

Type of Constant	Description
Project Status for Users' Personal Default Projects	The default status assigned to a default project within the Object Management Workbench. This project constant can be any one of the standard project status codes.
Project Status for All New Projects	The status assigned to a project when it is first created. This project constant can be any one of the standard project status codes or you can create a status and code for this purpose.
User Role to be Assigned to the Project's Originator	When a project is created, the originator is added as a user on the project. This project constant defines the user role assigned to the originator.
External User Role	The role to assign users when accessing objects from outside OMW. EnterpriseOne validates allowed actions against this role. This constant allows security to be configured for users who are secured out of OMW but still allows access to other available EnterpriseOne development tools, such as batch versions.

Project and Object Logging

Object Management Workbench logging tracks information about projects and objects. A major log is created whenever:

- A project is created, copied, or deleted.
- The project status is changed.
- A new or existing object is added to or removed from a project.
- An object is created, copied, or deleted.
- An object is checked in, checked out, saved, restored, transferred, or retrieved.

For every significant step or event within these actions, the system creates a detail log and attaches it to the major log record.

Activity Rules

These two types of activity rules exist:

- Project status activity rules
- Object transfer activity rules

Project status activity rules define the possible paths for an Object Management Workbench project. For a given project status, these rules define the possible next project statuses to which the project can be advanced.

For each project status activity rule, one or more object transfer activity rules exist. Each object transfer activity rule defines a FROM and TO location, where objects of this type are moved from and to for a specific software release.

For example, one object transfer activity rule can specify that all application (APPL) objects be transferred from the DV810 location to the PY810 location during a specified project status change.

Allowed Actions

The Allowed Actions form enables you to assign allowed actions to user roles for each object type during a specific project status. You must create the user role before configuring any allowed user actions.

Using allowed actions, administrators can restrict the actions that users with a specific role can perform.

Object Save Locations

The Object Save Locations form indicates the save location for Object Librarian (OL) objects. Defining the save location will enable users to transfer objects into the path code specified for the save location. Currently, only the save locations for Object Librarian objects may be defined.

Object Action Notifications

Object Action Notifications form enables you to activate or deactivate object action notification. The Object Action Notification System sends you an email each time an event, such as check-in or checkout, occurs to one of the objects. Object action notification is enabled by default.

Notification Subscriptions

The notification system sends email messages to users about changes to objects, such as object check-in and checkout, in the system. The Notification Subscriptions form enables you to add, delete, and modify notification subscriptions, as well as to sort notification subscription records by criteria that you choose.

The Configuration Process Flow

This section provides a recommended process flow for using all of the OMW configuration tools. The list contains each configuration function in the process flow, along with the topic in which you can find more information about each function.

The following configuration functions in the process flow require advance preparation:

- Assigning user roles.
- Applying allowed actions to users.
- Setting up project status rules and object transfer rules.

Before configuring these functions, make sure you understand user roles, allowed actions, project status rules, and object transfer rules.

The recommended process flow is as follows:

1. Assign user roles.

See [Chapter 3, “Configuring Object Management Workbench,” Configuring OMW User Roles and Allowed Actions, page 13.](#)

2. Apply allowed actions to users.

See [Chapter 3, “Configuring Object Management Workbench,” Configuring OMW User Roles and Allowed Actions, page 13.](#)

3. Disable SAR integration with OMW.

See [Chapter 3, “Configuring Object Management Workbench,” Configuring OMW Functions, page 20.](#)

4. Set up project constants.

See [Chapter 3, “Configuring Object Management Workbench,” Configuring OMW Functions, page 20.](#)

5. Set up project status and object transfer rules.

See [Chapter 3, “Configuring Object Management Workbench,” Configuring Activity Rules, page 23.](#)

6. Add, modify, and delete object save locations.

See [Chapter 3, “Configuring Object Management Workbench,” Configuring Object Save Locations, page 29.](#)

7. Control development in the event of logging failure.

See [Chapter 3, “Configuring Object Management Workbench,” Configuring OMW Functions, page 20.](#)

8. Control logging detail.

See [Chapter 3, “Configuring Object Management Workbench,” Configuring OMW Functions, page 20.](#)

9. Enable or disable object action notification.

See [Chapter 3, “Configuring Object Management Workbench,” Configuring Notification Subscriptions, page 31.](#)

10. Add, modify, and delete notification subscriptions.

See [Chapter 3, “Configuring Object Management Workbench,” Configuring Notification Subscriptions, page 31.](#)

11. View major and detail logs.

See [Chapter 3, “Configuring Object Management Workbench,” Working with OMW Logs, page 34.](#)

OMW Application and User Role Security

This section discusses:

- Securing OMW applications
- Securing user roles
- Securing administrative updates

Securing OMW Applications

You should secure these applications using application security:

- P98230 - OMW Configuration System
- R98210B - Object Management Log Purge
- P98231 - OMW Transfer Activity Rules Director

See Also

[Chapter 8, “Using Security Workbench,” Managing Application Security, page 109](#)

Securing User Roles

You can prevent users from adding a user to a project by using row-level security for the F98221.puomwur field. This field contains the user defined code of the user role for each user in a specific project.

However, all users must be able to add these user roles when setting up a new project:

- Originator
- Supervisor
- Manager
- Developer
- QA
- Product Support

The administrator role should be secured from all but a few users. Because manager and supervisor roles cannot be secured, consider creating a product manager role or similar role that can be secured. This new user role can be granted security attributes, such as being allowed to switch a token from one project to another.

Securing Administrative Updates

You should secure all actions, including project status change, for project statuses 40 (Production Development), 41 (Transfer Production to Prototype), and 42 (Transfer Prototype to Development). These statuses allow administrators to apply fixes to objects in the Production path code and then to promote the objects back to development. The ability to do so should be limited to administrators only.

Choosing a Configuration Option

This section provides an overview of the configuration setting indicators and discusses how to choose a configuration option.

Understanding Configuration Settings Indicators

Some of the function buttons on the Object Management Setup form have setting indicators next to them. Settings indicators describe the current setting for the SAR System Integration, Logging System, and Object Action Notification options. The purpose of each setting indicator is as follows:

Indicator	Description
SAR System Integration Indicator	Indicates whether the SAR (Software Action Request) system is integrated with the Object Management Workbench. SAR integration is enabled or disabled.
Logging System Indicator	Indicates whether full or reduced logging of project or object events is selected.
Object Action Notification Indicator	Indicates whether the object notification system is enabled or disabled.

Choosing a Configuration Option

All configuration options are set up through the OMW Configuration System application (P98230). Click the button next to the option that you want to configure.

Access the Object Management Setup form.

In PeopleSoft Solution Explorer, enter *GH9081* in the Fast Path. Double-click Object Management Configuration.

To choose a configuration option:

1. On Object Management Setup, if necessary, click the General tab to display function options.
2. Click one of these buttons to configure the corresponding function:
 - Constants
 - SAR System Integration
 - Logging System
 - Object Action Notification
 - Notification Setup
 - Activity Rules
 - User Roles
 - Allowed Actions
 - Save Locations

Configuring OMW User Roles and Allowed Actions

This section provides an overview of user roles and allowed actions and discusses how to:

- Modify a user role.
- Delete a user role.
- Set up allowed user actions.

Understanding OMW User Roles and Allowed Actions

Configuring user roles and allowed actions is one of the most important Object Management Workbench (OMW) configuration tasks. OMW's automation relies on an administrator who carefully configures these areas.

This table displays the allowed user actions that PeopleSoft EnterpriseOne recommends for each user role, the project status at which these actions should be authorized, and the responsibility of the person in that user role:

Recommended Project Status	User Role	Recommended Allowed Action	Explanation
11 - New Project Pending Review	Originator	Status Change	Originator might need to advance the status to 91 - Canceled Entered in Error
	Manager, Supervisor	Update Project	Change values for the project
		Update Users	Change values for the user
		Status Change	Advance project to the next status
21 - Programming	Developer	Add Objects	Add objects to project in order to fix or enhance
		Remove Objects	Remove objects that were incorrectly added
		Check Out	Check out objects from the server
		Check In	Check in objects to the server
		Get	Get objects from the server
		Status Change	Advance project to the next status
		Save	Move object specifications from the client development machine to the defined save location path code.
		Restore	Move object specification from the defined save location path code to the client development machine.

Recommended Project Status	User Role	Recommended Allowed Action	Explanation
		Transfer	Move object specifications between path codes or data sources.
25 - Rework-Same Issue	Developer	Status Change	Change project to 21 - Programming status
26 - QA Test/Review	Quality Analyst	Get	Get objects from the server
		Status Change	Advance project to next status
28 - QA Test/Review Complete	Manager, Supervisor	Update Project	Change values for the project
		Status Change	Advance project to the next status
		Transfer	
38 - In Production	Manager, Supervisor	Status Change	Advance project to the next status
01 - Complete	Developer	Remove Objects	Remove objects from projects at status 91 that might have been added but not removed

Note. You might want to allow the Manager and Supervisor roles to perform the same actions as the Developer role, in case the developer cannot perform assigned duties or needs to have work verified.

The Allowed Actions form enables you to assign allowed actions to user roles for each object type during a specific project status.

These default allowed actions cannot be changed. This information is provided for reference only:

Value	Description
02	Check In
03	Check Out
04	Delete
05	Add
06	Copy
08	Save
09	Restore
10	Design
11	Get

Value	Description
12	Remove Object from Project
13	Update a Project
16	Add Object to a Project
21	Switch Token
23	Force Release from Token Queue
30	Erase Check Out
38	Status Change

These default object types are provided for reference only:

Value	Description
01	Object Librarian objects
02	Data items
03	Versions
04	UDCs
05	Menus
06	Documentation record (SAR object)
11	Transfer record (SAR object)
12	History record (SAR object)

Example of Allowed Actions for an OMW Role

The following table contains the values that you would enter into the Allowed Actions form if you want the developer to be allowed to check in all object types when the project is at project status 21:

Field	Value
User Role	<i>02 - Developer</i>
Object Type	<i>*ALL</i>
Allowed Action	<i>02 - Check in</i>
Project Status	<i>21 - Programming</i>

Prerequisite

Before setting up allowed actions, you must add the user role to the User Roles UDC by using the User Defined Code form.

Forms Used to Configure OMW User Roles and Allowed Actions

Form Name	Form ID	Navigation	Usage
Object Management Setup	W98230R	Object Management menu (GH9081), Object Management Configuration (P98230)	Choose a configuration option.
Work With User Defined Codes	W0004AA	On Object Management Setup, click the User Roles button.	Modify or delete an OMW user role.
User Allowed Actions	W98230G	On Object Management Setup, click the Allowed Actions button.	Set up allowed user actions.

Modifying a User Role

Access the Object Management Setup form.

To modify a user role:

1. On Object Management Setup, click User Roles.
2. On Work With User Defined Codes, choose the user role you want to modify.
3. Double-click the first field that you want to change, and modify it.
4. Repeat step 3 to make all required modifications.
5. Click Find and verify that the modifications you made appear in the list.
6. Click OK.

Description 1

A user defined name or remark.

Description 2

Additional text that further describes or clarifies a field in the system.

Hard Coded

A code that indicates whether a user defined code is hard-coded. Values are:

- Y

The user defined code is hard-coded.

- N

The user defined code is not hard-coded.

A checkmark indicates that the user defined code is hard-coded.

Codes

A list of valid codes for a specific user defined code list.

User Defined Codes

A code that identifies the table that contains user defined codes. The table is also referred to as a UDC type.

Special Handling

A code that indicates special processing requirements for certain user defined code values. The value that you enter in this field is unique for each user defined code type.

The system uses the special handling code in many ways. For example, special handling codes defined for Language Preference specify whether the language is double-byte or does not have uppercase characters. Programming is required to activate this field.

Product Code

A user defined code (98/SY) that identifies a system. Values include:

- 01
Address Book
- 03B
Accounts Receivable
- 04
Accounts Payable
- 09
General Accounting
- 11
Multicurrency

Deleting a User Role

Access the Object Management Setup form.

To delete a user role:

1. On Object Management Setup, click the User Roles button.
2. On Work With User Defined Codes, click the cell to the left of the User Role that you want to delete.
3. Click Delete.
4. In the Confirm Delete query, click OK.
5. Repeat steps 2 through 4 to delete all desired user roles.
6. Click Find to verify that the user roles were deleted.
7. Click OK.

Setting Up Allowed User Actions

Access the Object Management Setup form.

To set up allowed user actions:

1. On Object Management Setup, click the Allowed Actions button.
2. On User Allowed Actions, click Find to display previously defined user actions.
3. To create a blank row in which to add a definition, sort on the allowed user action to be worked on.
4. Complete one or more of the query by example (QBE) columns and click Find.

5. Scroll to a blank row at the bottom of the sorted list.
6. Complete these fields in the blank row:

OMW User Role

A definition of the user's function within a project. Project managers generally assign a user to a project. When they do so, they indicate what role that user will be playing. Examples of user roles are:

- 01 Originator
Person who originated the project or the need for the project.
- 02 Developer
Person who modifies project objects.
- 03 Manager
Person who manages the project.
- 04 Quality Assurance
Person who checks the project's functionality.
- 06 Administrator
Person who configures project status, user roles, objects, and so forth.

Object Type

Actions can apply to specific Object Types. Select the Object Type for which you want to set up an allowed action.

- Batch applications
- Business functions
- Business views
- Data structures
- Event rules
- Interactive applications
- Media objects
- Tables Non-OL objects
- Data dictionary items
- UDC items
- Workflow items
- Menus
- Interactive application versions
- Batch Versions

Project Status

A value that indicates the status that the action allowed. You can enter *ALL to indicate that the action is allowed for all project statuses. Values are:

- 01 Complete
- 11 New Project Pending Review

- *21 Programming*
- *25 Rework-Same Issue*
- *26 QA Test/Review*
- *28 QA Test/Review Complete*
- *38 In Production*
- *40 Production Development*
- *41 Transfer Production to Prototype*
- *42 Transfer Prototype to Development*
- *45 Pristine Get*
- *91 Canceled-Entered in Error*

Action

A code that indicates the allowed action for the user role. You can enter **ALL* to indicate that the user role can perform all actions. You must enter a value from user defined code H92/AX. Values are:

- *01 Transfer*
- *02 Checkin*
- *03 Checkout*
- *04 Delete*
- *05 Add*
- *06 Copy*
- *08 Save*
- *09 Restore*
- *10 Design*
- *11 Get*
- *12 Remove Object From Project*
- *13 Update a Project*
- *16 Add Object to Project*
- *21 Switch Token*
- *23 Force Release From Token Queue*
- *30 Erase Checkout*
- *38 Status Change*

Note. You can enter **ALL* in any field except User Role. Typing **ALL* in a field indicates that the user role chosen can work with all object types, project statuses, or actions.

After you complete a row, a new blank row appears.

7. Repeat this procedure until all allowed user actions are set up.
8. Click OK.

Configuring OMW Functions

This section provides an overview of Object Management Workbench (OMW) functions and discusses how to:

- Disable SAR system integration.
- Control logging detail.
- Control development in the event of logging failure.
- Set up project constants.

Understanding OMW Functions

To configure OMW functions, you can disable the Software Action Request (SAR) system. This action is necessary if your company does not use SARs. You can also control logging detail and disable or limit development when logging fails. Finally, you can set up project constants to track the course of project development.

Forms Used to Configure OMW Functions

Form Name	Form ID	Navigation	Usage
Object Management Setup	W98230R	Object Management menu (GH9081), Object Management Configuration (P98230)	Choose an OMW function to configure.
SAR System Integration	W98230A	On Object Management Setup, click the SAR System Integration button.	Disable SAR system integration.
Object Management Logging System	W98230B	On Object Management Setup, click the Logging System button.	Specify which project and object events you wish to have logged. Control development in the event of logging failure.
Object Management Constants	W98230Q	Object Management Setup, click the Constants button.	Set up general constants for OMW projects.

Disabling SAR Integration

Most companies do not have the SAR (Software Action Request) system. You can verify that SAR integration is disabled by checking the settings indicator to the right of the SAR System Integration button on the Object Management Setup Form.

If you do not have the SAR system installed and the SAR System Integration settings indicator shows that SAR integration is enabled, you must disable SAR integration.

Access the Object Management Setup form.

To disable SAR system integration:

1. On Object Management Setup, click the SAR System Integration button.
2. On SAR System Integration, make sure the Integrate SAR System option is blank.

3. Verify that all other fields are unavailable for input and deselected.
4. Click OK.

Integrate SAR System

An option that specifies whether the Object Management Workbench (OMW) allows users to associate a SAR with an OMW project. The OMW SAR integration scheme allows OMW to update the SAR system. It does not allow the SAR system to update EnterpriseOne. When this option is selected, the user must set up the integration points in the User Defined Code H92/SI. The OMW SAR map exit, on the SAR Integration form, brings up the Work With User Defined Codes form for this UDC.

The OMW can:

- Change status of the associate SAR when the user changes the status of a project.
- Update the appropriate SAR section when the user adds an object to a project.
- Update the appropriate SAR section when the user adds a user to a project.

SAR Business Data

If populated, and SAR Integration is selected, OMW uses the data source from this field to open the Work Order and Address Book tables when dealing with the SAR system.

Address Book Data Source

The data source in which the following tables reside: F0001, F0006, F0101, F0111, F01131, F01132, F01133, F069116, F0901, F0911, F48001, F48002, F4801, F4802, F4826. OMW uses OCM to open these tables when dealing with the SAR System.

SAR Control Table Data

If populated, and SAR Integration is selected, OMW uses this data source to open the Next Number and User Defined Code tables when dealing with the SAR System. If you leave this field blank (regardless if SAR Integration is selected), OMW uses OCM to open these tables when dealing with the SAR System.

Controlling Logging Detail

Access the Object Management Setup form.

To control logging detail:

Note. The Object Management Logging System form enables you to specify which project and object events you wish to have logged.

1. On Object Management Setup, click the Logging System button.

Note. On Object Management Logging System, if you click the Reduce Logging Detail option, the Object Management Workbench (OMW) will reduce the logging detail for everyone in the enterprise. The reduced logging will eliminate most of the detail logging but will still keep a log of the major events such as object transfers, check-ins, and deletes.

2. Double-click the Log Actions and Detail Log Items folders.
3. Double-click items for which you do not want to log details.

A red X appears next to the deselected items.

4. Repeat step 3 to deselect all unwanted log detail items.
5. Click OK.

Controlling Development in the Event of Logging Failure

The Object Management Logging System form also allows you to disable development or to allow development but disable transfers if logging fails.

Access the Object Management Logging System form.

To control development in the event of logging failure:

1. On Object Management Logging System, to disable development if logging fails, choose the "Do not allow any development" option.

If the database logging tables fail for any reason, it is still possible to allow users to continue working. However, users will never be able to transfer objects while the logging system is down. This will ensure the integrity of production environments.

2. To permit development but disable object transfers in the event of a logging failure, choose the "Allow development but do not allow any transfers" option.

If the database logging tables fail for any reason, it is still possible to allow users to continue working. However, users will never be able to transfer objects while the logging system is down. This will ensure the integrity of production environments, but still allow development.

Note. This option is the default value.

3. Click OK.

Setting Up Project Constants

The Object Management Constants form enables you to set general constants pertaining to OMW Projects. These project constants are:

- Project status for users' personal default projects.
- Project status for all new projects.
- User role to be assigned to the project originator.
- External user role

Access the Object Management Constants form.

To set up project constants:

1. On Object Management Constants, to enter a project status for a user's personal default project, click the search button in the Enter the Project Status for user's personal default project field.
2. Double-click a project status.
3. To enter the initial project status for all new projects, click the search button in the Enter the initial Project Status for all new projects field.
4. Double-click a project status.

5. To enter the user role to use when assigning the originator to a project, click the search button in the Enter the User Role to use when assigning the originator to a project field.
6. Double-click a project status.
7. To enter the role for user who are secured out of OMW but still allowed access to certain development tools, click the search button in the External user role field to select a role.

Note. You can click the attachment buttons next to the fields to view their respective attachments.

Configuring Activity Rules

This section provides an overview of activity rules and discusses how to:

- Set up project status activity rules.
- Set up object transfer activity rules.

Understanding Activity Rules

The Activity Rules button on the Object Management Setup form enables you to set up both project status activity rules and object transfer activity rules. Project status activity rules define the phases that occur during a project development cycle. Object transfer activity rules work in conjunction with project status activity rules to define the From and To locations for moved objects.

Default Status Defaults

The installed project statuses and their definitions are as follows:

- 01 - Complete
- 11 - New Project Pending Review
- 21 - Programming
- 25 - Rework-Same Issue
- 26 - QA Test/Review
- 28 - QA Test/Review Complete
- 38 - In Production
- 40 - Production Development
- 41 - Transfer Production to Prototype
- 42 - Transfer Prototype to Development
- 45 - Pristine Get
- 91 - Canceled-Entered in Error

Project Promotion Life Cycle

The normal project promotion life cycle is as follows:

11 > 21 > 26 > 28 > 38 > 01

Where

11 = New project pending review

21 = Programming

26 = QA test/review

28 = QA test/review complete

38 = In production

01 = Complete

During a normal project promotion cycle, developers check objects out of and in to the Development path code; promote them to the prototype path code; and then promote them to the Production path code before declaring them complete.

Administrators can follow a different promotion cycle, as follows:

11 > 40 > 41 > 42 > 01

Where

11 = New project pending review

40 = Production development

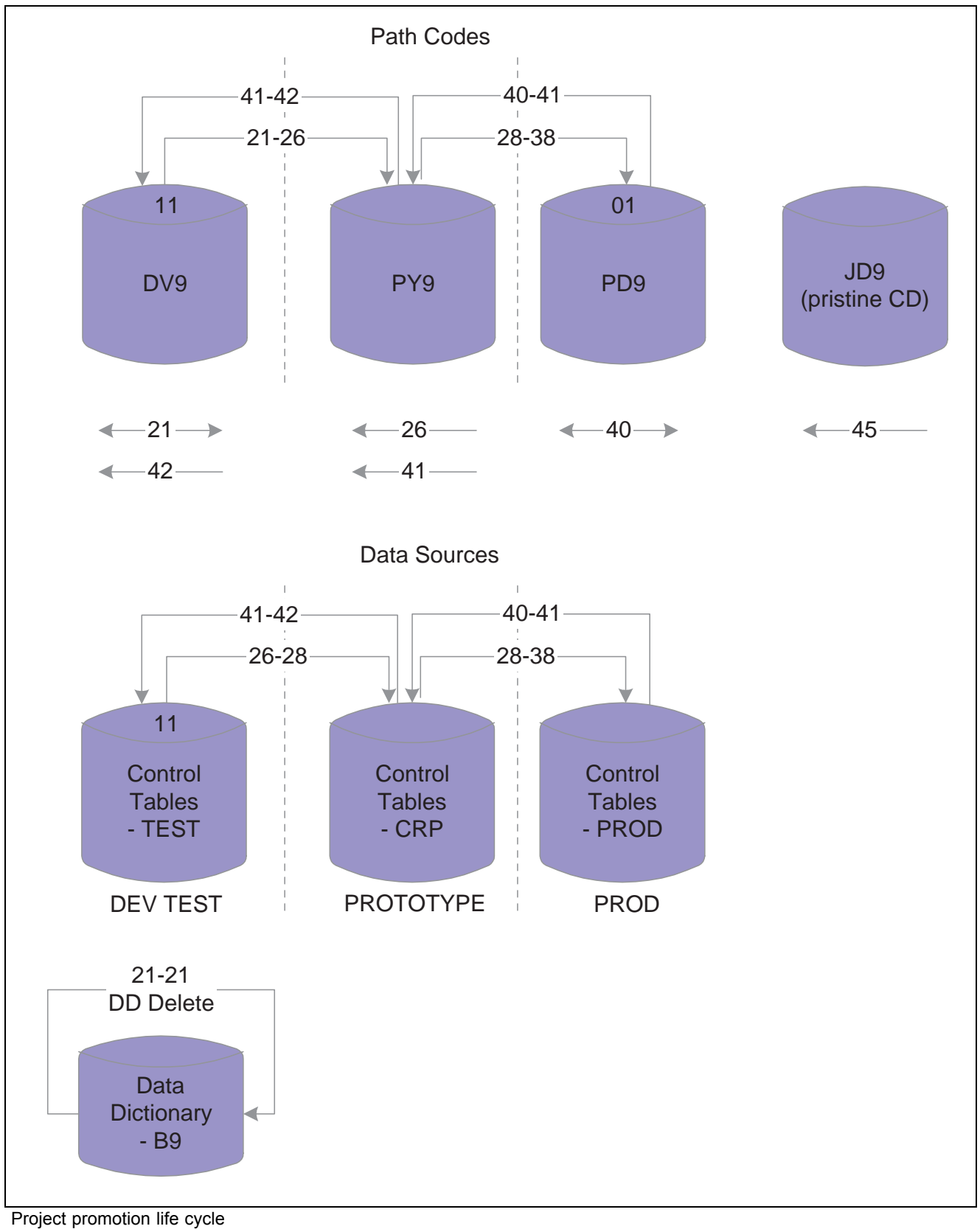
41 = Transfer from Production to Prototype

42 = Transfer from Prototype to Development

01 = Complete

During this promotion cycle, administrators check objects out of and in to the Production path code to apply fixes, and then demote the objects to the Prototype path code and the Development path code. Developers should not use this promotion cycle. PeopleSoft EnterpriseOne recommends that you apply status activity rules that limit this promotion cycle to a specific group: those with the User ID for administrators.

This illustration displays the project promotion life cycle:



Forms Used to Configure Activity Rules

Form Name	Form ID	Navigation	Usage
Object Management Setup	W98230R	Object Management menu (GH9081), Object Management Configuration (P98230)	Access forms to configure activity rules.
Work With Object Management Activity Rules	W98230O	On Object Management Setup, click the Activity Rules button.	Set up project status activity rules.
Object Transfer Activity Rules	W98230F	On Work With Object Management Activity Rules, choose a related To project status and click Select.	Set up object transfer activity rules.

Setting Up Project Status Activity Rules

You can set up statuses for a project as development progresses from one phase to the next. For example, the project might move from a programming phase to a manager review phase. For each of these transitions you will define:

- Whether this project status rule is active.
- The System Role to which this project status transition applies.
- The related "To" project status.
- The related "From" and "To" SAR* statuses.

Complete the From and To SAR status only if you have SAR integration selected.

Access the Object Management Setup form.

To set up project status activity rules:

1. On Object Management Setup, click the Activity Rules button.
2. On Work With Object Management Activity Rules, click Find.

All available From project statuses appear.

3. Select a From Project Status from the tree.
4. Click Select.

Project Status Activity Rules lists all valid "To project statuses" for the "From project status" you chose.

The current project status appears in the From Project Status field.

5. Scroll to the blank row at the bottom of the list and complete these fields:

- Active

This field can be used to allow only specific users or only users who are members of a specified group to perform a status change. To make the rule available to everyone, enter **PUBLIC* in this field.

- User/Role

The user or role for which the Project Status Activity Rule is valid. Users may perform all project status activity rules that are assigned to their user ID, role, or *PUBLIC.

Note. These are not overrides.

- To Project Status

Indicates an allowed next status for a project that is currently at the From status to be advanced to.

- From SAR Status

Complete for projects with SARs and only if you have SAR integration selected. If SAR integration is disabled, these columns are disabled.

- To SAR Status

Complete for projects with SARs and only if you have SAR integration selected. If SAR integration is disabled, this column is disabled.

A blank row appears beneath the row that you completed.

6. Repeat step 5 to set up or modify other To project status entries for this particular From Project Status.
7. Click OK when you are done.
8. Choose the next From Project Status and repeat steps 5 through 7 to set up project activity rules for each remaining From Project Status.
9. When all project activity rules are complete, click OK to return to the Work with Object Management Activity Rules Form.
10. ClickClose.

Setting Up Object Transfer Activity Rules

You must configure object transfer activity rules for each object type used in a project that you want to perform an action on.

For each object type you want to perform an action on, you must define:

- Project statuses at which users can check in, check out, and get objects ("getting" an object means copying its specifications to the work area without checking it out).
- At which status change you would like objects to be transferred.
- Project statuses at which object tokens are released.

These object location tasks must be performed when setting up object transfer activity rules:

- Define FROM and TO transfer locations for each object type at each project status transition—for example, when project status 21 (development) changes to project status 26 (prototype). In this example, objects are transferred from DV810 to PY810.
- Define checkout and get locations for Object Librarian object types.
- Define checkin locations for Object Librarian objects.

Note. Transfer activity rules can occur in any order. For example, you might have one status change that will require more than one object transfer. If you expect an object to transfer from DV810 to PY810 and then PY810 to PD810, you will want to set up rules to transfer the object from DV810 to PY810 and DV810 to PD810 because the object transfer activity rules could be retrieved in any order.

Access the Object Management Setup form.

To set up object transfer activity rules:

1. On Object Management Setup, click the Activity Rules button.
2. On Work With Object Management Activity Rules, click Find to display all available project statuses.
3. Double-click the From Project Status folder for which you want to set up object transfer activity rules.
4. Click one of the related To project statuses.

This field defines the To Project Status, which completes the From and To Project Status transition for which you want to configure object transfer activity rules. For each From and To Project Status transition, you can create multiple object transfer activity rules for different object types.

Note. When configuring checkin, checkout, and get activity rules, the From and To statuses are the same.

5. Click Select.
6. On Object Transfer Activity Rules, scroll to the blank row at the bottom of the list. Complete these fields for the object type desired:

- Active

Enter 1 for active; 0 for inactive.

- User/Role

The user or role for which the Transfer Activity Rule is valid. For a given user during the indicated status change, OMW retrieves transfer activity rules first for the user ID, then the role, and finally *PUBLIC. OMW follows this hierarchy when retrieving transfer activity rules and uses the first rules found within this hierarchy and does not continue.

Note: These are overrides. If a user defines one rule for *PUBLIC, one rule for an applicable role, and one rule for the user's ID for a given object type, OMW only uses the user ID transfer activity rule.

- Object Type

Note. *ALL may not be used when defining transfer activity rules.

- From Location

- To Location

Note. Object Librarian objects use path codes for the From Location and To Location values, whereas non-Object Librarian objects use data source values. For Versions, if a path code is entered, the F983051 record and the specs for the version are transferred (for batch versions), and if a data source is entered, just the F983051 record is transferred between the defined locations.

- Object Release

This field contains the release level of EnterpriseOne that you are currently working on. The From Release value should be the same as the To Release value.

- To Release

Currently not used. This field is populated with the From Release value.

- Release Token
- Allowed Action

A blank row appears when you have finished. When you set up transfer activity rules for Workflow objects, an additional form appears. Use the form to provide From and To Data Source values for the Task Specifications table (F98811) records.

7. Repeat this procedure to set up or modify other object types for this project status transition.
8. Click OK to return to the Work With Object Management Activity Rules form.
9. Choose the next From and To project status transition, and repeat this procedure to set up its object transfer activity rules.
10. Repeat step 9 until all object transfer activity rules are complete.
11. Click OK to return to the Work With Object Management Activity Rules form.
12. Click Close.

Note. When you set up transfer activity rules for APPL objects, you must also define rules for User Override Object types so that OMW can transfer any *PUBLIC user overrides for the APPL objects. If you do not do so, APPL objects will not transfer successfully.

Configuring Object Save Locations

This section provides an overview of object save locations and discusses how to:

- Create an object save location.
- Modify an object save location.
- Delete an object save location record.

Understanding Object Save Locations

Using Object Management Workbench (OMW), you can create a save location, which is a path code developers use to save their objects. With the save location created, you add the path code to the system, allowing saved objects to be transferred. You can also modify or delete save locations.

Forms Used to Configure Object Save Locations

Form Name	Form ID	Navigation	Usage
Object Management Setup	W98230R	Object Management menu (GH9081), Object Management Configuration (P98230)	Access forms to configure object save locations.
Object Save Locations	W98230K	On Object Management Setup, click the Save Locations button.	Add, modify, and delete an object save location.

Creating an Object Save Location

During the installation process, an additional path code might not have been created to use as the OMW save location. To use this feature, you must create a path code where developers can save their objects while they are in development. When users perform a save, their objects are checked into the path code defined as the save location; when they perform a Restore, objects are retrieved from this location.

Access the Object Management Setup form.

To create an object save location:

Note. The Object Save Locations form indicates the save-off location for Object Librarian (OL) objects. Currently, only the save locations for Object Librarian objects may be defined.

1. On Object Management Setup, click the Save Locations button.
2. On Object Save Locations, click the search button in these columns:
 - Location
Select the path code associated with the environment that is being used for development.
 - Save Location
Select the new save location. This is the path code where the Objects Specifications should be saved to.

Note. Different save locations may be configured for different environment path codes. For example, users signing into DV810 environments could save to a DVSAVE location, whereas users signing into a PY810 environment could save to a PYSAVE location.

3. Click OK.

Modifying an Object Save Location

Access the Object Management Setup form.

To modify an object save location:

1. On Object Management Setup, click the Save Locations button.
2. On Object Save Locations, click the search button in the Save Location field to select the new save location for the object.

Deleting an Object Save Location Record

Access the Object Management Setup form.

To delete an object save location record:

Note. If an Object Librarian object is deleted, you should also delete the object's save location in order to delete the save location completely from the system.

1. On Object Management Setup, click the Save Locations button.
2. On Object Save Locations, choose the record to be deleted.
3. Click Delete.
4. Click OK in the Confirm Delete box.

5. Click OK.

Configuring Notification Subscriptions

This section provides an overview of notification subscriptions and discusses how to:

- Enable or disable object action notifications.
- Add a notification subscription.
- Modify a notification subscription.
- Delete a notification subscription.
- Sort notification subscriptions.

Understanding Notification Subscriptions

Notification subscriptions allow you to alert users using email about changes to objects in the system, such as object checkins and checkouts. After you enable object notification, you can add, modify, delete, or sort notification subscriptions. The Object Action Notification System is initially enabled by default.

Forms Used to Configure Notification Subscriptions

Form Name	Form ID	Navigation	Usage
Object Management Setup	W98230R	Object Management menu (GH9081), Object Management Configuration (P98230)	Access forms to configure notification subscriptions.
Object Action Notification	W98230D	On Object Management Setup, click the Object Action Notification button.	Enable or disable action notifications.
Notification Subscriptions	W98230L	On Object Management Setup, click the Notification Setup button.	Add, delete, modify, and sort notification subscriptions.

Enabling or Disabling Object Action Notifications

Access the Object Action Notification form.

To enable or disable object action notifications:

1. On Object Action Notification, to enable object action notification, select the Activate Object Action Notification option.

If enabled, the notification system sends email messages to users regarding actions taken on EnterpriseOne objects by OMW. Use the OMW Notification Subscriptions form in the Configuration Application (P98230) to configure the notification system.

2. To disable object action notification, clear the Activate Object Action Notification option.
3. Click OK.

Note. Notification that users are added to or removed from projects always occurs, even when object action notification is disabled. In this situation, an email message is sent to the user.

Adding a Notification Subscription

Notification Subscriptions can be created for an action performed on these objects:

- All objects of the specified system code.
- All objects of a specified type.
- All objects of a combination of 1 and 2.
- A specific object name and type.

Access the Notification Subscriptions form.

To add a notification subscription:

1. On Notification Subscriptions, click Find to display the current notification subscriptions.
2. Scroll to a blank row and complete these mandatory fields:
 - OMW User Role
 - Action
3. Complete these optional fields:
 - Object Type
 - Object Name
 - Reporting System Code
 - Path Code

A new row appears when you are done.
4. Repeat steps 2 and 3 until all notification subscriptions are added.
5. Click OK.

Action

Object Name

You can set up notifications to occur based on Object Name. If the indicated action occurs to a project containing an object with the specified name, the system alerts the user. Object Name must be used in conjunction with the Object Type.

Object Type

You can set up notifications to occur based on Object Type. If the indicated action occurs to a project containing an object of the specified type, the system alerts the user.

In EnterpriseOne, an object has traditionally been a reusable entity based on software specification created by the EnterpriseOne Tools. These objects included Object Librarian Objects, such as interactive applications (APPL), as well as batch applications (UBE), and data structure (DSTR) objects. In OMW, this definition has been expanded to include other non-Object Librarian type objects or data source based rather than path code based objects, such as:

- Batch applications

- Application versions
- Batch versions
- Business functions
- Business views
- Data structures
- Event rules
- Interactive applications
- Media Objects
- Tables Non-OL Objects
- Data dictionary items
- UDC items
- Workflow items
- Menus

Path Code	The path code is a pointer to a set of objects, and is used to keep track of sets of objects and their locations.
Reporting System Code	You may set up notifications to take place based on a system code. If an object is on a project and it belongs to the system code indicated, and the action indicated takes place for or the objects are moved into the path code indicated, a message will be sent to the user.
User ID/Role	A definition of the user's function within a project.

Modifying a Notification Subscription

Access the Object Management Setup form.

To modify a notification subscription:

1. On Object Management Setup, click the Notification Setup button.
2. On Notification Subscriptions, click Find to display the current notification subscriptions.
3. Choose the fields to be modified and make the changes.
4. Click OK.

Deleting a Notification Subscription

Access the Object Management Setup form.

To delete a notification subscription:

1. On Object Management Setup, click the Notification Setup button.
2. On Notification Subscriptions, select the record to be deleted.
3. Click the Delete button.
4. Click OK in the Confirm Delete query.
5. Click OK.

Sorting Notification Subscriptions

Access the Object Management Setup form.

To sort notification subscriptions:

1. On Object Management Setup, click the Notification Setup button.
2. On Notification Subscriptions, above the rule headers, click the Query by Example column to be filtered.
If a search button appears, click it and double-click the filter criteria. In other Query by Example columns, enter the filter criteria.
3. Click Find.
The filtered notification subscriptions appear.
4. Click OK.

Working with OMW Logs

This section provides an overview of OMW logs and discusses how to:

- View project or object logs.
- Locate object logs.
- Locate project logs.
- View detail logs.
- Reorder log record fields.
- Print logs.

Understanding OMW Logs

Object Management Workbench (OMW) contains an object management logging application. Project and object logs provide an excellent way to review the development history of projects or objects. Furthermore, you can view log details for any log record currently appearing on the monitor. From the Work With Log Detail form, you can bring up the actual log entry in the View Full Log Text window.

This application also enables you to rearrange log fields to customize software development reporting. You can view all logs, view sorted logs, or show only the last logging action for an object or project. These two tasks must be performed together to produce customized project and object development reports:

- Reorder log record fields
- Print logs

Forms Used to Work with OMW Logs

Form Name	Form ID	Navigation	Usage
Work With Object Management Log	W98210A	Cross Application Development Tools (GH902), Object Management Logging (P98210).	View project or object logs. Reorder log record fields. Print logs.
Work With Object Logs	W98210C	On Work With Object Management Log, choose Object Logs from the Form menu.	Locate object logs. View detail logs.

Viewing Project or Object Logs

Access the Work With Object Management Log form.

To view project or object logs:

1. On Work With Object Management Log, perform one of these actions:
 - Click Find to view logs for all projects and their objects in OMW.
 - Enter sorting criteria in the Query by Example cells to filter search results, and then click Find.
 - Select the Show Only Last Action option to show only the last logging action for a given project or object.
2. Click Close.

Locating Object Logs

Access the Work With Object Logs form.

To locate object logs:

1. On Work With Object Logs, you can:
 - Click Find to show all OMW object logs.
 - Enter data in the Query by Example cells to narrow the search and click Find.
 - Select the Show Only Last Action option to show only the last logging action.
 - Click the Check for Attachments button to check for object attachments.
2. Click Close.

From Data Source

These fields are only valid for these object actions. They will be blank for project logs. Transfer - For Object Librarian Objects, this is the source and target deployment data sources for moving object specifications.

For Non-OL Objects, this is the source and target main data source for moving the data records. Check-in - The To field will indicate the check-in deployment data source. The From field will contain LOCAL. Check-in applies only to Object Librarian Objects. Check-out - The From field will indicate the checkout deployment data source. The To fields will contain LOCAL. Checkout applies only to Object Librarian Objects. Delete - The To field indicates the data source where the object was deleted from. The From data source is irrelevant for delete. Add - The From and To fields

will be identical. For Object Librarian Objects, this is the deployment data source of the path code where the object was created. For Non-OL objects, this is the data source where the object was created. Copy - The From and To fields will be identical. For Object Librarian Objects, this is the deployment data source of the path code where the object was copied. For Non-OL objects, this is the data source where the object was copied. Save - The From location will always be LOCAL. The To location will be the deployment data source of the save path code. Save applies only to Object Librarian Objects. Restore - The To location will always be LOCAL. The From location will be the deployment data source of the save path code. Restore applies only to Object Librarian Objects. Get - For Object Librarian Objects, the From field will indicate the deployment data source of the path code From location. For Non-OL Objects, the From field will indicate the data source of the From location. The To field will always contain LOCAL.

From Path Code or Environment

These fields are only valid for these object actions. They will be blank for project logs. Transfer - For Object Librarian Objects, this is the source and target path codes for moving object specifications. This field is empty for non-OL objects. Check-in - The To field will indicate the check-in path code location. The From field will contain LOCAL. Check-in applies only to Object Librarian Objects. Check-out - The From field will indicate the checkout path code location. The To fields will contain LOCAL. Checkout applies only to Object Librarian Objects. Delete - For Object Librarian Objects, the To field indicates the path code where the specifications were deleted from. For Non-Object Librarian Objects, the To fields indicates the environment where the object was deleted from (if applicable - this is only populated for non-OL objects if the developer deleted the object from his local environment). For Object Librarian Objects, the From field indicates the path code where they were deleted locally (if applicable - delete of local specs only happen when the developer deletes an object). The From field is always empty for non-OL objects. Add - The From and To fields will be identical. For Object Librarian Objects, this is the path code where the object was created. For Non-OL objects, this is the environment where the object was created. Copy - The From and To fields will be identical. For Object Librarian Objects, this is the path code where the object was copied.

For Non-OL objects, this is the environment where the object was copied. Save - The From location will always be LOCAL. The To location will be the path code of the save location. Save applies only to Object Librarian Objects.

Restore - The To location will always be LOCAL. The From location will be the path code of the save location. Restore applies only to Object Librarian Objects. Get - For Object Librarian Objects, the From field will indicate the path code from location. For Non-OL Objects, the From fields will indicate the environment from location. The To field will always contain LOCAL.

Project Name

An identifier for a EnterpriseOne project. A EnterpriseOne project is composed of a group of EnterpriseOne objects that have been modified or created by a developer to complete a task. All work with objects within EnterpriseOne must occur within the context of a project.

To Data Source

These fields are only valid for these object actions. They will be blank for project logs. Transfer - For Object Librarian Objects, this is the source and target deployment data sources for moving object specifications.

For Non-OL Objects, this is the source and target main data source for moving the data records. Check-in - The To field will indicate the check-in deployment data source. The From field will contain LOCAL. Check-in applies only to Object Librarian Objects. Check-out - The From field will indicate the checkout deployment data source. The To fields will contain LOCAL. Checkout applies only to Object Librarian Objects. Delete - The To field indicates the data source where the object was deleted from. The From data source is irrelevant for delete. Add - The From and To fields will be identical. For Object Librarian Objects, this is the deployment data source of the path code where the object was created. For Non-OL objects, this is the data source where the object was created. Copy - The From and To fields will be identical. For Object Librarian Objects, this is the deployment data source of the path code where the object was copied. For Non-OL objects, this is the data source where the object was copied. Save - The From location will always be LOCAL. The To location will be the deployment data source of the save path code. Save applies only to Object Librarian Objects. Restore - The To location will always be LOCAL. The From location will be the deployment data source of the save path code. Restore applies only to Object Librarian Objects. Get - For Object Librarian Objects, the From field will indicate the deployment data source of the path code From location. For Non-OL Objects, the From field will indicate the data source of the From location. The To field will always contain LOCAL.

To Path Code or Environment

These fields are only valid for these object actions. They will be blank for project logs. Transfer - For Object Librarian Objects, this is the source and target path codes for moving object specifications. This field is empty for non-OL objects. Check-in - The To field will indicate the check-in path code location. The From field will contain LOCAL. Check-in applies only to Object Librarian Objects. Check-out - The From field will indicate the checkout path code location. The To fields will contain LOCAL. Checkout applies only to Object Librarian Objects. Delete - For Object Librarian Objects, the To field indicates the path code where the specifications were deleted from. For Non-Object Librarian Objects, the To fields indicates the environment where the object was deleted from(if applicable - this is only populated for non-OL objects if the developer deleted the object from his local environment). For Object Librarian Objects, the From field indicates the path code where they were deleted locally (if applicable - delete of local specs only happen when the developer deletes an object). The From field is always empty for non-OL objects. Add - The From and To fields will be identical. For Object Librarian Objects, this is the path code where the object was created. For Non-OL objects, this is the environment where the object was created. Copy - The From and To fields will be identical. For Object Librarian Objects, this is the path code where the object was copied.

For Non-OL objects, this is the environment where the object was copied. Save - The From location will always be LOCAL. The To location will be the path code of the save location. Save applies only to Object Librarian Objects.

Restore - The To location will always be LOCAL. The From location will be the path code of the save location. Restore applies only to Object Librarian Objects. Get - For Object Librarian Objects, the From field will indicate the path code from location. For Non-OL Objects, the From fields will indicate the environment from location. The To field will always contain LOCAL.

Program ID

The number that identifies the batch or interactive program (batch or interactive object). For example, the number of the Sales Order Entry interactive program is P4210, and the number of the Print Invoices batch process report is R42565.

The program ID is a variable length value. It is assigned according to a structured syntax in the form TSSXXX, where:

T

The first character of the number is alphabetic and identifies the type, such as P for Program, R for Report, and so on. For example, the value P in the number P4210 indicates that the object is a program.

SS

The second and third characters of the number are numeric and identify the system code. For example, the value 42 in the number P4210 indicates that this program belongs to system 42, which is the Sales Order Processing system.

XXX

The remaining characters of the number are numeric and identify a unique program or report. For example, the value 10 in the number P4210 indicates that this is the Sales Order Entry program.

Date Updated

The date that specifies the last update to the file record.

Time Updated

The time that specifies when the program executed the last update to this record.

User ID

The code that identifies a user profile.

Locating Project Logs

Access the Work With Object Management Log form.

To locate project logs:

1. On Work With Object Management Log, click Form and then click Project Logs.
2. On Work With Project Logs, you can perform these functions:
 - Click Find to show all OMW project logs.
 - Enter data in the Query by Example cells to narrow the search, and then click Find.
 - Select the Show Only Last Action option to show only the last logged action for the selected project.
 - Click the Check for Attachments button to check for attachments.
3. Click Close.

From Status

This can be one of the project status codes, which are:

01 Complete
 11 Pending Review
 17 Plan or Research
 18 Design
 19 Design Review
 21 Programming
 22 Programmer Test
 23 Manager Review
 24 Transfer to Production
 25 Rework
 26 QA Test
 28 QA Test Complete

To Status

Indicates an allowed next status for a project that is currently at the From status to be advanced to.

Viewing Detail Logs

Access the Work With Object Logs form.

To view detail logs:

1. On Work With Object Logs, double-click any log record you want to research. Or, click the desired log record row to highlight it, and then click Select.
2. Click Find.

The detail log record for the selected log appears. All sequence details for the selected Log record appear in ascending numerical order.

3. To view the full text of the Description field, click it and then click Select.

The View Full Log Text window appears, showing the actual log entry.

4. You can move between detail logs by clicking the Previous and Next buttons.
5. Click Close.

Log Sequence

This is numeric sequence number to make the log detail for a particular action unique.

Machine Key

The Location or Machine Key indicates the name of the machine on the network (server or workstation).

Log Data Item

This is a log detail data item. It defines the text of log detail under a major log action such as check-in, checkout, and so forth. All these data items are glossary data items and some of them have text substitution. For a complete of log items, please see the Logging System section of the Configuration Application (P98230).

Reordering Log Record Fields

Access the Work With Object Management Log form.

To reorder log record fields:

1. On Work With Object Management Log, click Sequence.
2. Click the first column you want to sort in the Columns Available window.
3. Click the right-pointing arrow to move it to the Columns Sorted window on the right.
4. Repeat steps 3 and 4 as required until all the columns you want to view are in the correct sort order.
If you make an error, you can move columns back to the Columns Available window for resorting. Select the column to be resorted and the left-pointing arrow.
5. Click OK in the Select Grid Row Sort Order form to reorder the log columns.

Printing Logs

Access the Work With Object Management Log.

To print logs:

1. On Work With Object Management Log, click File and then Print Screen.
2. Modify print settings as required.
3. Click OK in the Print form.

CHAPTER 4

Setting Up EnterpriseOne Printing

This chapter provides an overview of EnterpriseOne printing and discusses how to:

- Set up printers.
- Search for incorrect printing records.
- Determine which batch processes are attached to printers.
- Generate and retrieve logs for the report.
- Set up a printer to use a barcode font.
- Design reports to run on line printers.

Understanding EnterpriseOne Printing

The Printers application (P98616) provides a single point of entry for configuring the printers within PeopleSoft EnterpriseOne. The application enables you to define printers for workstations and enterprise servers. These definitions reside in software tables that are maintained by the Printers application (P98616).

Printing Reports

In addition to creating reports, the software includes a number of predefined reports and report versions, which you can use or modify for the business needs. EnterpriseOne uses the batch engine to create reports, and generates these reports in PDF. You can view the PDF files or print the report using the Adobe Acrobat Reader software.

Reports process as batch applications without user interaction. When a user submits a report for processing, the user makes choices, such as the selection and sequencing of data to include in the report, the location where the report will process, logging capabilities to monitor how the report processes, and the printer on which the report prints.

When you submit a PeopleSoft EnterpriseOne report, the batch engine generates a PDF file. To create the PDF file, the batch engine uses a device context consisting of information such as page size and the printable area of a page. The software generates this information from the printer tables for all platforms.

You can view the report (the PDF file) on the workstation using Adobe Acrobat Reader, or you can send it to a printer. You can also print the report from the Adobe Acrobat Reader. When you send the report to a printer, the software uses a conversion filter to transform the PDF file into one of three Page Description Language (PDL) formats: PCL, PostScript, or line-printer text. The conversion format depends on the type of printer that prints the report.

The EnterpriseOne batch engine uses the following logical path to determine to which printer to send a report. If the first method does not return a valid printer name, the batch engine uses the subsequent method.

When the user submits the report, the following events occur:

- The batch process triggers the Do Initialize Printer event from Report Design Aid (RDA). If this process retrieves a valid printer name, the following processes are ignored.
- The user overrides the default printer name at the time that the report is submitted. If the user overrides the default printer with a valid printer name, the following processes are ignored.
- The RDA specifications pass a printer name to the batch process. If this process retrieves a valid printer name, the following process is ignored.
- From the Printer Definition table (F98616), the software determines a valid default printer based on the current user, the environment the user is signed onto, and the host that processes the report.

Running Reports on the Server

When you submit a report to the server, the engine prompts you for a printer name previously defined in the Printers application. Then the server automatically creates a PDF file using the settings associated with the selected printer, unless event rules (ER) override those printer settings. You can, however, affect how the report prints on the server before you generate a PDF file by changing settings, such as the printer, page orientation, PDL, and paper type, on the Printer Selection dialog box. When you view the report on the server, the software copies the PDF file from the server to the local\810\PrintQueue directory on the workstation.

When you run a report, you also have the option of turning on logging capabilities. You do so from the Advanced form when you submit the report. When you view a log, the workstation stores the log file in the\810\PrintQueue directory.

See Also

Chapter 4, “Setting Up EnterpriseOne Printing,” Generating and Retrieving Logs for Your Report, page 52

Running Reports on the Workstation

When you choose to run a report and view the output on the screen, the engine tries to connect to the printer defined in Report Design. If the engine cannot connect or if there is no printer defined, the engine uses the default printer from the printer tables. Using the settings that it retrieves, the engine creates a PDF file and displays the report through Adobe Acrobat Reader. The PDF file is stored in the local\810\PrintQueue directory.

When you run a report locally and send the output to a printer, the engine displays the Printer Selection dialog box, which gives you the option to change the printer, page orientation, PDL, paper type, and so on. The initial printer shown in this dialog box is the one defined in RDA or the default printer, if none was defined. The engine connects to the printer defined in the printer dialog box and retrieves the associated settings. Using these settings, the engine creates a PDF file, converts the PDF into a PDL file using the conversion filter, and sends the PDL file to a printer.

Print-Time Characteristics

The user has the option of overriding the printer at a report's print time. This option is different from the option for overriding the printer when the user first submits the report. At submit time, the user can choose any valid enterprise printer. At print time, however, the user can override the printer only with another printer that supports the same platform, PDL, and paper type as the original printer. This is because the batch engine has already created the PDF version of the report and has embedded into the PDF file the platform, PDL, and paper type information.

Print Settings for the Workstation jde.ini

The workstation jde.ini settings control whether or not a report prints immediately and whether or not PeopleSoft EnterpriseOne saves the output after processing the report.

```
[NETWORK QUEUE SETTINGS]
PrintImmediate=TRUE/FALSE
SaveOutput=TRUE/FALSE
```

Setting	Description
PrintImmediate	<p>Specifies whether or not the system automatically prints the report after processing is complete. Values are:</p> <p>TRUE. The system processes the report on the server, generates a PDF file, converts the PDF to the appropriate PDL for the defined printer, and then prints the report.</p> <p>FALSE. The system processes the report on the server but does not automatically print the report. Users must use the Work With Servers application to manually print the report.</p>
SaveOutput	<p>Specifies whether the system saves or deletes the output after you view or print the job. Values are:</p> <p>TRUE. The system saves the output after you have viewed or printed the job.</p> <p>FALSE. The system deletes the output after you have viewed or printed the job.</p>

Setting Up Printers

This section discusses how to:

- Add a printer
- Define a default printer
- Modify an existing printer
- Copy an existing printer
- Delete a printer
- Delete a paper type

Understanding Printer Setup

PeopleSoft EnterpriseOne provides a single application that uses a director interface to help you set up the printer. From this director, you can add new printers, modify existing printers, and define default printers for a combination of a user, a host, and an environment. You can also add and modify the paper types and custom conversion programs that the printers use at the time that you add and modify printer settings.

When you add a printer, the software provides a director to help you with each step of the process. Instructions appear on each form of the director to guide you through the printer addition process.

Note. You must set up printers for each server platform that you use in the enterprise.

When adding the first printer, you must define it as the default printer.

Adding a Printer

In PeopleSoft Solution Explorer, enter GH9013 in the Fast Path, and then from the Batch Processing Setup menu, select Printers (P98616) to access the Printers form.

To add a printer:

1. On the Printers form, click the Add Printer button.
2. On Printer Setup Director, review the welcome information and then click Next.

The Platform Type default value is entered automatically on the Platform Information form, depending on which operating system the software is running.

3. On Platform Information, complete the following fields:

- Print Server Name

Type the name of the print server for the printer that you are setting up. You can use any characters in the printer name that are valid for the platform. The software uses this name, along with the print shared name, to create the printer name, which appears unavailable for input on the subsequent form. For printing reports to a non-network printer, leave this field blank.

For iSeries: *library name/outqueue name*

For the iSeries, the physical printer name must be the same as the outqueue name. If you use the default QGPL library to store the outqueues, you need only enter the outqueue name in this field. Enter this information in upper case. For example, DEVDES3A.

If the outqueues reside in a library other than the default QGPL library, you need to enter the library name and the outqueue name in this field. For example, QUSERSYS/DEVDES3A.

Note. When you qualify the outqueue name with the library name, you avoid possible name conflicts that might result in the submission of the report at an unexpected outqueue.

For Windows: *\\server name\printer name*

Enter this information in lower case, for example \\corprts1\docprf2.

For UNIX: *printer name* (no slashes)

Enter this information in lower case, for example devprn16.

- Print Shared Name

Type the share name of the printer that you are setting up. You can use any characters in the printer name that are valid for the platform. The software uses this name, along with the print server name, to create the printer name, which appears unavailable for input on the subsequent form.

4. Click Next.

The Printer Setup form appears. Use this form to specify information such as the printer model, physical location of the printer, printer definition language, paper types, and encoding selection (iSeries only).

Note. When you change an existing printer, you make the modifications on this page.

See [Chapter 4, “Setting Up EnterpriseOne Printing,” Modifying an Existing Printer, page 49.](#)

5. On the General tab, complete these fields:
 - Printer Model
 - Printer Location
6. Click the Details tab:
7. On the Details tab, under Printer Definition Language, click any of these options:
 - PostScript
 - PCL
 - Line Printer

Note. If you select PostScript or PCL, EnterpriseOne disables the Line Printer option. If you choose the Line Printer option, the software disables the PostScript and PCL options. You can select multiple printer definition languages (PDLs), but only one default PDL under Default. The option under Default sets the PDL that you want to specify as the default. You can override this PDL when a batch process is submitted.

8. When you select the PostScript option, complete the following fields under Paper Source:
 - Max Number of Paper Sources
Enter a numeric value in this field to indicate the number of paper trays that this printer has available.
 - Default Paper Source
Enter a numeric value in this field to indicate the default tray number from which you want to draw paper.
9. When you select the Line Printer option, complete the following fields under Line Printers to set the paper dimensions and line parameters:
 - Characters Per Inch
The value that you enter in this field determines the number of characters that the physical printer allows in one horizontal inch.
 - Columns Per Page
The value that you enter in this field determines the number of characters that appear in one line of text in the report.
 - Line Per Inch
The value that you enter in this field determines the number of lines of text that the physical printer allows in one vertical inch.
 - Line Per Page
The value that you enter in this field determines the number of lines of text that the physical printer allows on one printed page.
 - Printer Paper Width
The value in this field is calculated automatically, based on the numbers you enter in the Line Printers box.
 - Printer Paper Height
The value in this field is calculated automatically based on the numbers you enter in the Line Printers box.

10. When you choose the Line Printer option along with an iSeries server, fields appear within a box labeled iSeries Only. You use these fields to set the iSeries encoding that the printer supports. Choose one of the following:

- ASCII Encoding
- EBCDIC Encoding

Note. If you select a PostScript or PCL printer along with an iSeries server, the ASCII Encoding option is automatically checked and the AS/400 Only box is disabled.

11. When you select the Custom option, complete the following option and fields:

Note. The custom option uses an advanced feature of the Printers application. Only users with knowledge about building parameter strings for printers should use this option.

- Select the Custom option.

A field appears below the Custom button.

- Enter the name of the conversion filter that you want to use.

You can type a conversion filter name into the field below the custom option or you can use the visual assist to choose a filter.

- To change or add a conversion filter, choose Advanced from the form menu. This option is enabled only when Custom is chosen.
- On Work with Conversion Programs, select one of the filters or click Add, and then click Select or Copy.

12. On Advanced Conversion Program, change the following fields, and then click OK:

- Conversion Program

If you clicked Add or Copy on the previous form, the Conversion Program field is enabled. Enter the name of the conversion program that you want to add or copy. If you are making a copy, the string that you highlighted on the previous form appears in the Parameter String field.

- Parameter String

The parameter string is entered automatically. It is based on the host from which you are printing (iSeries, HP9000, and so on) and the type of printer (postscript, PCL, or line). For example:

`-s string_name -l library_name -f convertPDFTToPS`

Where `-s` defines the string name, `-l` defines the library name (this value is the letter l, not the number 1), and `-f` defines the function name.

To send a PDF file directly to a printer without converting it, enter the following parameter string:

`-s script_name`

Where `script_name` is the name of a shell script that sends the PDF to a UNIX queue (such as the PCL_PRINTER script). Because the file is not being converted, the `-l` and `-f` parameters are not required.

13. In the detail area of the Printer Setup form, double-click the row header for each paper type that the printer supports.

A check mark appears in the row header for each paper type that you choose.

Note. You can add new paper types as necessary. Instructions to do so are included later in this task.

14. In the Default Type column, type the numeral 1 in the row for the paper type that you want to use as the default value.

You can choose only one default paper type. You can override the default paper type when a batch process is submitted.

15. To add a new paper type, from the Form menu, select New Paper Type.

16. On Work With Paper Types, click Add.

17. On Paper Type Revisions, complete the following fields and click OK:

- Paper Type
- Paper Height
- Paper Width
- UM

The software saves the new paper type and displays the Work With Paper Types form. After you close Work With Paper Types, the new paper type will be available in the Printer Setup detail area form. All previous paper type selections are cleared and would need to be chosen again if you want to reuse them.

18. When you finish entering information for the printer, click End.

The software saves the new printer and displays the Printer form.

Platform Type	The type of physical hardware the database resides on.
Printer Name	The name assigned to a specific printer on a network, such as Accounting_Printer_1. For EnterpriseOne, this name cannot contain a space character, even if allowed by the operating system.
Printer Model	Printer capabilities are as follows: Printer Model: the model of the printer Printer Location: where the printer physically resides Encoding: AS/400 users' only feature
Paper Type	The sizes of paper the printer will support, such as letter, legal, and A4.
Printer Paper Width	A value that specifies the width of the paper for this paper type. This value is in the unit of measure specified by Unit of Measure.
Printer Paper Height	A value that specifies the height of the paper for this paper type. This value is in the unit of measure specified by Unit of Measure.
UM	A user defined code (00/UM) that indicates the quantity in which to express an inventory item, for example, CS (case) or BX (box).
EBCDIC Encoding	Printer capabilities are as follows: <ul style="list-style-type: none"> • Printer Model. The model of the printer. • Printer Location. The location where the printer physically resides. • Encoding. AS/400 feature only.
Columns Per Page	A line printer parameter that specifies the number of columns per page, for example 80 or 132.

Characters Per Inch	The horizontal printing density. Enter the number of characters per inch supported by the printer.
Line Per Page	A line printer parameter that specifies the number of lines per page, for example 60 or 66.
Line Per Inch	<p>The line spacing should be entered as the number of lines per inch and must be supported by the printer. The values are:</p> <p>4 IBM 5219, 5224, 5225, and 3287 printers only</p> <p>6 IBM 5224 printer only</p> <p>8 IBM 5224 printer only</p> <p>9 IBM 5225 printer only</p> <p>The standard computer print is 6 LPI and 10 CPI. If you are printing on 8 1/2 x 11 paper, you would specify 8 LPI and 15 CPI.</p>

Defining a Default Printer

In PeopleSoft Solution Explorer, enter GH9013 in the Fast Path, and then from the Batch Processing Setup menu, select Printers (P98616) to access the Printers form.

To define a default printer:

1. On the Printers form, click the Define Default Printer button.

The Work With Default Printers form appears.

2. Click Add.

The Default Printer Revisions form appears.

3. Complete the following fields, and then click OK:

- User/Role

Click the visual assist to choose either a particular user for this printer or a Role. If the field is left blank, the default value is *PUBLIC.

- Report Name

Click the visual assist to choose a specific report to print. If the field is left blank, the default value is *ALL.

- Version Name

Click the visual assist to choose a specific version to run. If the field is left blank, the default value is *ALL. If the Report Name is *ALL, the version name will default to *ALL and be disabled.

- Environment

The software automatically enters the name of the environment that you are currently logged on to. You can change this information.

- Printer Name

- Host Name

Include the host server where reports will run. The visual assist displays the appropriate host names based on the printer name you chose.

- Object Status

You can make this new printer the default printer by changing its status to active. If an error occurs, it means that another printer is currently the active default. You need to change the original default printer to inactive before you can activate the new printer. You can perform multiple status changes from the Work With Default Printers form; these are explained at the end of this task.

After you click OK from the Default Printers Revision form, the Work With Default Printers form appears.

4. To change the status of a default printer from the Work With Default Printers form, select a default record and then, from the Row menu, select Change Status.

If another printer is already specified as the active default printer, an error occurs. To change the original default printer to inactive, select it, select Change Status from the Row menu, and then make the new printer the default.

Modifying an Existing Printer

In PeopleSoft Solution Explorer, enter GH9013 in the Fast Path, and then from the Batch Processing Setup menu, select Printers (P98616) to access the Printers form.

To modify an existing printer:

1. On the Printers form, click the Modify Printer button.
2. On Work With Printers, click Find to view all available printers.
3. Choose the printer that you want to modify, and then click Select.

The Printer Setup form appears. Use this form to change information for the printer, such as the printer model, physical location of the printer, printer definition language (PDL), and paper type.

4. Modify the information for the printer and click OK.

You cannot modify the printer name and platform type. If you chose a line printer, the paper-type grid at the bottom of the form is disabled.

The software saves the new printer information and returns you to the Work With Printers form.

Copying an Existing Printer

In PeopleSoft Solution Explorer, enter GH9013 in the Fast Path, and then from the Batch Processing Setup menu, select Printers (P98616) to access the Printers form.

To copy an existing printer:

1. On the Printers form, click the Modify Printer button.
2. On Work With Printers, click Find to view all available printers.
3. Choose the printer that you want to copy, and then click Copy.
4. On the Printer Setup form, complete these fields:

- Printer Name

Enter the entire printer name, including the server path. For example, if printer docprf2 is on server corprts1, the printer name for a Windows printer would be: `\\corprts1\docprf2`. If you use multiple platforms, you must define a printer for each platform using the following naming conventions:

- iSeries: *library name/outqueue name*

For the iSeries, the printer name must be the same as the outqueue name. If you use the default QGPL library to store the outqueues, you need only enter the outqueue name in this field. The information that you enter must be in upper case, for example DEVDES3A.

If the outqueues reside in a library other than the default QGPL library, you need to enter the library name and the outqueue name in this field, for example QUSERSYS/DEVDES3A.

Note. When you qualify the outqueue name with the library name, you avoid possible naming conflicts that might result in the submission of the report to an unexpected outqueue.

- Windows: *\\print server name\printer name*

This information must be entered in lower case, for example: `\\corprts1\docprf2`.

- UNIX: *printer name* (no slashes)

This information must be entered in lower case, for example `devprn16`.

- Platform Type

Enter the platform that you are printing from, such as an iSeries server.

5. On the Details tab, modify the information as needed.
6. Click OK.

Deleting a Printer

In PeopleSoft Solution Explorer, enter GH9013 in the Fast Path, and then from the Batch Processing Setup menu, select Printers (P98616) to access the Printers form.

To delete a printer:

1. On the Printers form, click the Modify Printer button.
2. On Work With Printers, click Find to view all available printers.
3. Choose a printer or choose multiple printers by holding down the Ctrl key, and then click Delete.

This action removes the printer definition from EnterpriseOne.

Deleting a Paper Type

In PeopleSoft Solution Explorer, enter GH9013 in the Fast Path, and then from the Batch Processing Setup menu, select Printers (P98616) to access the Printers form.

To delete a paper type:

1. On the Printers form, click the Modify Printer button.
2. On Work With Printers, click Find to view all available printers.
3. Choose a printer, and then click Select.
4. On Printer Setup, from the Form menu, select New Paper Type.
The Work With Paper Types form appears.
5. On Work With Paper Types, choose a paper type and click Delete.
6. On Confirm Delete, click OK.

The paper type that you deleted no longer appears in the detail area.

Searching for Incorrect Printing Records

PeopleSoft EnterpriseOne provides a batch process (R9861602) that enables you to search the Printer Capability table (F986163) for printer records that are incomplete or contain incorrect printer information. The batch process produces a report that contains this information, which can help you correct the printing records.

The report lists reports that have a logical printer name. Since logical and physical printer names are no longer used in the software, you can use this information to change existing printer settings.

Searching for Incorrect Printer Records

In PeopleSoft Solution Explorer, enter GH9111 in the Fast Path, and then select Batch Versions (P98305) to access the Work With Batch Versions - Available Versions form.

To search for incorrect printer records:

1. On Work With Batch Versions - Available Versions, enter *R9861602* in the Batch Application field and click Find.
2. Run the XJDE0001 version.
3. Using the report, find the printer record, and correct it.

Determining Which Batch Processes are Attached to Printers

You can run a batch process to determine which of the batch processes, if any, are attached to printers.

Determining Which Batch Processes are Attached to Printers

In PeopleSoft Solution Explorer, enter GH9111 in the Fast Path and then select Batch Versions (P98305) to access the Work With Batch Versions - Available Versions form.

To determine batch processes attached to logical printers:

1. On the Work With Batch Versions - Available Versions form, enter *R9861601* in the Batch Application field, and click Find.

The XJDE0001 version appears.

2. Select the row with the XJDE0001 version and then click Select to run the report.

The report lists reports that have a logical printer name. Use this information to change existing printer settings, since logical and physical printer names are no longer used in the software.

3. Use Report Design Aid (RDA) to attach a valid printer to those batch processes that had been attached to a logical printer.

Note. Only someone familiar with the Report Design tool should attempt to attach a printer.

Generating and Retrieving Logs for Your Report

When you run a report, you can specify whether you want to create logs for the report. The logs that you can create are the `jde.log` and the `jddebug.log`. These logs, which reside in a specific directory on the server, enable you to review how your reports process on the server. The `jde.ini` settings determine the location of this directory.

Understanding `jde.ini` Settings for the Report Logs Directory

The `jde.ini` settings differ slightly, depending on the platform that you use. Sample `jde.ini` settings where the report logs reside are as follows:

- iSeries

```
[INSTALL]
```

```
DefaultSystem=E810SYS
```

```
Example path: E810SYS\PRINTQUEUE
```

- UNIX

```
[INSTALL]
```

```
E810=/usr/PeopleSoft/output
```

```
Example path: /usr/PeopleSoft/output/PrintQueue
```

- Windows Server

```
[INSTALL]
```

```
E810=d:\PeopleSoft\output
```

```
Example path: d:\PeopleSoft\output\PrintQueue
```

The default directory for the log files is `PrintQueue`, which becomes a subdirectory to the directory that you designate in the `[INSTALL]` section of the `jde.ini` file. You can change the location of this directory as necessary.

Note. These `jde.ini` settings also determine where the report output resides after processing. If you set the `jde.ini` to save the output for your reports, the software saves a PDF file for the report in the report output directory.

Forms Used to Create Logs for Your Report

Form Name	Form ID	Navigation	Usage
Work With Batch Versions - Available Versions	W98305A	Report Management (GH9111), Batch Versions (P98305)	Locate and run reports and modify version detail information.
Version Prompting	W98305D	On the Work With Batch Versions - Available form, select a version to submit and click Select.	Change the data selection and data sequencing, and run a report and create the logs.
Advanced Operations	W98305J	On the Version Prompting form, select Advanced from the Form menu	Override the location where the report processes, activate the jde.log, activate the jdedebug.log, and modify the level of information that the logs include.

Creating Logs for Your Report

Access the Work With Batch Versions - Available Versions form.

To create logs for your report :

1. Enter a batch application ID in the Batch Application field and click Find.
For example, enter *R014021* to locate a version for the One Line Per Address report.
2. Select a version to submit, and then click Select.
3. Select Advanced from the Form menu.
4. Modify the following information, and then click OK:
 - Logging (JDE.log)
 - Tracing (JDEDEBUG.log)
 - UBE Logging Level

Note. When you choose a high value to receive more technical information, you also receive all the information for the lower values. For example, when you enter a value of 6 (UBE function messages), you also receive information for values 0 through 5.

5. On the Version Prompting form, click Submit to run your report and create your logs.

Logging (JDE.log)

A code that indicates whether logging is enabled for the execution of a batch job when it runs on a server. If the server is already set to perform logging, the logging occurs, regardless of this code.

Tracing (JDEDEBUG.log)

When the batch job runs on a server, this field indicates whether tracing is enabled for execution of the job. If the server is already set to perform tracing, it occurs regardless of how this field is set.

UBE Logging Level

Indicates the level of detail of error logging that occurs when the batch job runs. The following list describes the different levels:

- 0 Error Messages

- 1 Informative Messages and Log Entry
- 2 Section Level Messages
- 3 Object Level Messages
- 4 Event Rule Messages
- 5 Database Mapping Messages
- 6 UBE Internal Function Calls, Textout Values

Setting Up a Printer to Use a Barcode Font

PeopleSoft EnterpriseOne supports the use of the BC C39 3 to 1 Medium barcode font, which is included with PeopleSoft EnterpriseOne. After you set up the printers, you can assign a printer to use a barcode font for your reports.

Note. Printers that support barcodes must use either the PostScript or PCL printer definition languages.

Forms Used to Set Up a Printer to Use a Barcode Font

Form Name	Form ID	Navigation	Usage
Work With Bar Code Font	W986166A	Batch Processing Setup menu (GH9013), select Bar Code Support (P986166).	Set up a printer to use a barcode font. Delete barcode support information from a printer.
Bar Code Font Revisions	W986166B	On the Work With Bar Code Font form, click Add.	Enter, modify, or copy information for a barcode-capable printer.

Setting Up Barcode Font Printing

Access the Work With Bar Code form.

Printer Name	The name assigned to a specific printer on a network, such as Accounting_Printer_1. For EnterpriseOne, this name cannot contain a space character, even if allowed by the operating system.
Printer Font Name	A code that indicates the font used on the report.
Symbol Set ID	The symbol and symbol set ID defines the character and character mapping for a particular symbol set. You can contact the PCL printer font vendor to obtain this information.

Running Reports on Line Printers

This section discusses how to:

- Design a report to run on a line printer.
- Set up a line printer.
- Print multiple copies to a remote iSeries line printer.

Understanding How to Run Reports on Line Printers

When you run a report on a line printer, you must follow specific guidelines to ensure that the information contained in the report prints successfully. These guidelines include font family, font size, grid spacing, width of the fields on the report, paper dimensions, and line parameters.

Note. The information in this section is intended for users with previous experience creating reports and setting up printers.

See Also

[Chapter 4, “Setting Up EnterpriseOne Printing,” Printing Reports, page 41](#)

EnterpriseOne Tools 8.94 PeopleBook: Server & Workstation Administration

Forms Used to Run Reports on Line Printers

Form Name	Form ID	Navigation	Usage
Report Design Aid	NA	Report Writer (GH9111), Report Design Aid	Design a report to run on a line printer.
Printers	W98616S	Printers menu (GH9013), Printers (P98616)	Set up a line printer.

Designing a Report to Run on a Line Printer

Access the Report Design Aid.

To design a report to run on a line printer:

Note. In the Batch Versions application, create a version of the report to use only online printers. Make the following modifications to this report version. Do not make these modifications at the report level. If you make these modifications at the report level, the information in your report might not appear correctly on other printer platforms.

1. Open the report with the version that you want to modify to support line printers.
2. From the Layout menu, select Grid Alignment.
The Alignment Grid form appears.
3. Set the value in the Vertical field to 16 and click OK.
4. From the File menu, select Report Properties.
The Properties form appears.
5. Click the Font/Color tab, set the following font properties, and then click OK:

- Change the font to Courier New.

The Courier New font provides the best results; however, you can use other fixed-pitch fonts. For example, for reports that contain text in Japanese, users should use the fixed-pitch version of the MS-Gothic font.

- Change the font size to 10.
6. Select the Apply settings to all objects option to make sure these settings apply to objects that might have individual font settings applied.
 7. (Steps 7 through 11 apply to Group sections only.) After you change the font properties, you might need to increase the width of some of the fields on your report. Widen fields as necessary to provide enough room for information to appear on your report. Reposition the sections of your report so that all the report objects appear in the detail area.
 8. If some data fields still do not align correctly, press and hold the Ctrl key, and then click each field that you want to align.
Use the top edge of the last field that you choose to align the other fields.
 9. From the Layout menu, choose Align.
The Align Objects form appears.
 10. In the Apply To box, choose the Current section option to enable the Top to Bottom box.
 11. In the Top to Bottom box, choose the Top Edges option and then click OK.
 12. When you complete the modifications to your report, save your report version.

Setting Up a Line Printer

Access the Printer form.

To set up a line printer:

Note. The following steps provide information about the values for setting the paper dimensions for a line printer. These steps should be used as a supplement to the steps that describe how to set up a printer.

See [Chapter 4, “Setting Up EnterpriseOne Printing,” Setting Up Printers, page 43](#).

1. On the Printers form, click the Add Printer button.
2. On Printer Setup Director, click Next.
3. On Platform Information, complete these fields:
 - Platform Type
 - Print Server Name
 - Print Shared Name
4. Click Next.
5. On the General tab, complete the following fields:
 - Printer Model
 - Printer Location
6. Click the Detail tab, and choose Line Printer as the Printer Definition Language.

7. Set the characters per inch (CPI), columns per page (CPP), lines per inch (LPI), and lines per page (LPP) values.

These values determine the paper dimensions that the line printer will use when printing reports. For example, you would use the following values to print on an 8.5-inch x 11-inch size paper:

- CPI: 10
- CPP: 85
- LPI: 6
- LPP: 66

Note. Use the following formula to calculate the paper dimensions:

$CPP / CPI = \text{width in inches}$ ($85 / 10 = 8.5$)

$LPP / LPI = \text{height in inches}$ ($66 / 6 = 11$)

8. Click End to save these settings.

Printing Multiple Copies to a Remote iSeries Line Printer

To print multiple copies to a remote iSeries line printer:

This task is necessary only if the output queue for an iSeries line printer does not support printing multiple copies. This task applies to remote output queues only. This task must be completed by a system administrator.

1. End the remote writer to which the output queue is connected.
2. Use the Change Output Queue (CHGOUTQ) command to change the Display Options (DSPOPT) parameter so that it contains the value XAIX.
3. Restart the remote writer.

The output queue should now be able to send multiple copies of your documents to the remote printer.

CHAPTER 5

Working with Servers

This chapter provides an overview of the Work With Server program (P986116) and discusses how to:

- Manage server jobs
- Manage job queues
- Use EnterpriseOne subsystems

Understanding the Work With Servers Program

The Work With Servers program (P986116) provides a central location from which system administrators can monitor and control:

- Server jobs
- PeopleSoft EnterpriseOne subsystems

As a system administrator, you can use the Work With Servers program to print, view, remove, terminate, release, or hold any jobs that currently reside in a queue on any EnterpriseOne server. Similarly, workstation users can control only those jobs submitted by them. This option is generally restricted to only those jobs associated with a specific user ID.

Also, you can use the Work With Servers program to end and to stop EnterpriseOne subsystems, and to view the status of EnterpriseOne subsystems that are running or are waiting to process jobs.

Managing Server Jobs

This section provides an overview of server jobs and discusses how to:

- Check the status of reports.
- Change the priority and printer for jobs.
- Print jobs.
- View reports online.
- View the logs for a job.
- Terminate jobs.
- Hold and release jobs.

Understanding Server Jobs

By using the Work With Servers application, system administrators can print, view, and delete job records from the outqueue. They can also terminate, release, or hold any jobs that currently reside in a queue on any PeopleSoft EnterpriseOne server. Similarly, using the Submitted Job Search form, workstation users can, in general, control only those jobs submitted by them.

You should use EnterpriseOne security to restrict access to the Work With Servers application. In general, access to this program should be granted only to administrator-level users because the ZJDE0001 version of the Work With Servers program enables users to view and control server jobs for all users. End users should be restricted to the ZJDE0002 version, which is known as the Submitted Job Search form. This version of the application restricts users to viewing and modifying only those jobs that were submitted under their user ID initially. Both programs are located on the System Administration Tools menu (GH9011).

Job Status and Priority

After you submit the report, you can check the status of the job in the queue. Depending on the status of the job, you can perform tasks such as print or delete the report, view the report output online, and hold the report in the queue.

You can also move the priority of the job to a lower or higher status while the job is at the status of W (Waiting).

Overriding Printer Location for Jobs

You can also override the location where the job prints. For jobs with a status of D (Done) and E (Error), you can send the job directly to the default printer without viewing the PDF file online. A status of D means that the processing for the job completed successfully. A status of E means that an error occurred during processing. If you print a job with a status of E, you print an error log to aid you when you troubleshoot the report.

Viewing Reports Online

After the job finishes processing on the server, you can view the report output online. For most jobs, the output is in Portable Document Format (PDF), which can be viewed with Adobe Acrobat Reader. When you view the report output online, the system also creates a PDF file for the report in the following directory on the workstation:

```
\810\PrintQueue
```

You can attach PDF files to email messages; move or copy the files; and, because most current Web browsers can read PDF files, post the reports to a Web site. Also, you can copy text from Acrobat Reader to the clipboard and paste that text into other applications.

Job Logs

You can view logs that detail the steps taken while the job processed. From the Submitted Job Search form, you can access the `thejde.log` and the `jddebug.log` for the report. These logs are helpful if you need to troubleshoot why a report resulted in error. These logs exist on the machine where the job ran.

The `thejde.log` is a general-purpose log used to track error messages generated by EnterpriseOne processing. The `thejde.log` tracks any fault that might occur within the software, including whether the sign on is successful. When you are looking for startup errors, you should read the `thejde.log` from the top down. For other errors, you should read from the bottom up.

The `jddebug.log` contains API calls, BSFN logs, and SQL statements, as well as other messages. You can use this log to determine at what time normal execution stopped. The system does not use `jddebug.log` to track errors; instead, it uses this log to track the timing of processes.

Terminating Jobs

You can manually terminate a job that is processing. When you terminate a job, you do not delete it; rather, you move the job to the status of E (Error). With the job at the status of E, you can print an error log or delete the job.

Holding and Releasing Jobs

If a job is at the status of W (waiting), you can hold the job. You might choose to hold a job if the job is large enough to affect the performance of the server on which it processes. You can release a job when server performance is not an issue, such as after regular business hours.

Note. If you want to stop a job that is at a status of P (Processing), you must terminate the job. When you terminate a job, you do not remove the job; rather, you move the job to the status of E (Error). You cannot restart a job after you terminate the job; you must resubmit the job to the server.

See Also

EnterpriseOne Tools 8.94 PeopleBook: Server & Workstation Administration

Forms Used to Manage Server Jobs

Form Name	Form ID	Navigation	Usage
Work With Servers	W986116A	System Administration Tools (GH9011), Work With Servers (P986116).	Choose a server in which you want to locate a job.
Submitted Job Search	W986110BA	On Work With Servers, from the Row menu, select Server Jobs.	Enables you to print, terminate, hold, release, or view a job. Users can manage jobs submitted by their user ID initially. Depending on the security level, you can change the User ID field and the Job Queue field to search for other jobs.
Job Maintenance	W986110BC	On Submitted Job Search, select a job with which to work and click Select.	Review information about the batch job, modify the priority of the job, or change the printer on which the job will print.
Printer Selection	W986162B	On the Submitted Job Search form, select a job and then choose Print from the Row menu.	Provides printer-specific information as well as information about the format of the report.
View Logs	W986110BD	On Submitted Job Search, select the job for which you want to view a log, and then select View Logs from the Row menu.	View the <code>jde.log</code> and the <code>jdedebug.log</code> .

Setting Processing Options for Work with Servers (P986116)

Processing options enable you to specify the default processing for programs and reports.

For programs, you can specify options such as the default values for specific transactions, whether fields appear on a form, and the version of the program that you want to run.

For reports, processing options enable you to specify the information that appears on reports. For example, you set a processing option to include the fiscal year or the number of aging days on a report.

Do not modify EnterpriseOne demo versions, which are identified by ZJDE or XJDE prefixes. Copy these versions or create new versions to change any values, including the version number, version title, prompting options, security, and processing options.

Security

1. Security Flag

Use this processing option to specify how submitted jobs can be viewed. Values are:

Blank No Security

- 1 Allow users to view jobs by group.
- 2 Allow users to view only their own jobs.

Checking the Status of Reports

Access the Submitted Job Search form.

User ID	The default user ID is the user logged on to the current session. This user ID can be changed if you wish to work with a report submitted by a different user. You can use a wildcard (*) to find a specific user.
Job Queue	Enter the name of the logical queue on the server for which you want to view jobs.
Status	Click the search button in the Status field to read the UDCs for status codes in the installation

Changing the Priority and the Printer for Jobs

Access the Work With Servers form.

To change the priority and the printer for jobs:

1. Choose a server with which to work and, from the Row menu, choose Server Jobs.
The Submitted Job Search form appears. By default, jobs are listed for the User ID for the requesting workstation. Depending on the application security level, you can change the User ID field and the Job Queue field to search for other jobs.

Note. A job must be at a status of W (Waiting) to change the priority.

2. Select a job with which to work and click Select.
3. On Job Maintenance, modify the information in the Job Priority field and click OK.

User ID The code that identifies a user profile.

Job Queue	The job queue to which the job was submitted. On the iSeries, this is an actual system job queue. On other systems, it is an EnterpriseOne logical queue.
Job Priority	The priority level of a submitted job. Jobs will execute based on this priority. Values 0-9 are valid where 0 is the highest priority.

Printing Jobs

Access the Work With Servers form.

To print jobs:

1. On Work With Servers, from the Row menu, select Server Jobs.
2. On Submitted Job Search, select the job that you want to print, and then choose Print from the Row menu.
The Printer Selection form appears. This form provides printer-specific information as well as information about the format of the report.
3. To print the job, click OK.

Viewing Reports Online

Access the Work With Servers form.

To view reports online:

Note. Before you view the report online, verify that you have Adobe Acrobat Reader installed on the workstation.

1. On Work With Servers, select a server from the list and then click Select or select Server Jobs from the Row menu.
2. On Submitted Job Search, select the job that you want to view and then select View Job from the Row menu.
Adobe Acrobat Reader displays an online version of the report output.

Viewing the Logs for a Job

Access the Work With Servers form.

To view the logs for a job:

1. On Work With Servers, select the server that processed the job that you want to view, and click Select, or select Server Jobs from the Row menu.
2. On Submitted Job Search, select the job for which you want to view a log, and then select View Logs from the Row menu.
The View Logs form appears. On this form, you can view thejde.log and thejdedebug.log.
3. Click OK to view the logs.

Note. If you choose both thejde.log and thejdedebug.log, the logs open in the same window. To view the logs separately, you must select the logs separately.

Terminating Jobs

Access the Work With Server form.

To terminate jobs:

1. On Work With Servers, select a server from the list or use the query by example row to select a specific server.
2. Click Select or select Server Jobs from the Row menu.
3. On Submitted Job Search, select the job to terminate, and then select Terminate from the Row menu.

Note. A job must be at a status of P (processing) to terminate the job.

4. Click Find to update the detail area.

The status of the job changes to E (error).

Holding and Releasing Jobs

Access the Work With Servers form.

To hold or release a job:

1. On Work With Servers, select a server from the list or use the query by example row to select a specific server.
2. Click Select or select Server Jobs from the Row menu.
The Submitted Job Search form appears.
3. To hold a job, select the job and then select Hold from the Row menu.
4. Click Find to update the detail area.

The status of the job changes to H (Hold).

5. To release a job, select the job and then select Release from the Row menu.

The job must be at the status of H (Hold).

6. Click Find to update the detail area.

The status of the job changes to reflect the position of the job in the queue, for example, W (Waiting), S (In Queue), or P (Processing).

Managing Job Queues

This section provides an overview of how EnterpriseOne uses job queues to manage batch processes and discusses how to:

- Add a queue.
- Revise a queue.
- Copy a queue.
- Change the status of a queue.

Understanding Job Queues

Each PeopleSoft EnterpriseOne server instance starts a queue kernel process that manages batch processes across operating system platforms. The process keeps track of all jobs that are submitted and controls the order in which the jobs run.

EnterpriseOne uses two tables to maintain queue records:

- Job Control Status Master table (F986110), which maintains records on the status of each job submitted to a queue.
- Queue Control Status Master table (F986130), which stores the names of each queue, such as QBATCH, the name of the server on which the queue runs, the port number for the server instance, the queue status and type, and the maximum number of active jobs allowed.

Note. Since F986130 is a system table, be sure to account for it when you map objects using Object Configuration Manager (OCM).

The following list summarizes how the software, using the queue kernel, manages a UBE that you launch:

- Starts queue kernel when the server instance starts.
- Verifies that a record exists in the F986130 table for the queue to which the job is submitted. If the job is intended for a non-EnterpriseOne queue, verifies that the native queue (for example, iSeries) exists.
- Inserts job record into the F986110 table.
- Sends a message to the queue kernel that the new job exists.
- Adds the job to a wait list.
- Schedules the job or submits it to the native queue.
- Starts the job.
- Runs the job.
- Updates the job record in the F986110 table upon receiving a message from the UBE process that the job is complete.
- Removes the job from the list of active jobs.
- Schedules another job.

The queue kernel also follows a subroutine in scheduling jobs. The following list summarizes the subroutine that the queue kernel follows:

- Verifies that jobs in the queue are waiting to be run.
- Verifies that the number of jobs waiting to be run is less than the maximum number of jobs allowed for the queue.
- Takes the highest priority job from the wait list and updates its status to S (Submitted).
- Removes the job from the wait list and adds it to the active list.

Administering Job Queues

Use the Job Queue Maintenance application (P986130) to define and manage job queues. This application enables you to dynamically administer job queues. You can use this application to create, modify, copy, delete, or change the status of job queues, regardless of platform. For example, you can use this application to add a queue record to the Queue Control Status Master table (F986130). You can also revise an existing queue record. For example, you might want to change the maximum number of jobs that can run in a queue.

In addition, when you set up job queues, you can define a default queue in which to submit jobs.

Overriding a Job Queue

When you prepare to submit a UBE, you can change the values of the parameters that define the submission by overriding the job queue. Overriding the job queue means that you change the job queue to which the job is submitted on the server.

To override the job queue for a batch version, you launch the Batch Versions application (P98305), choose a batch version, and access the Advanced Version Prompting form (W98305I). The override queue must be one that is available for the server and port.

In working with the Advanced Version Prompting form, you can override the job queue only if the queue kernel is active and if the batch version is mapped to run on the server. If the batch version is mapped to run locally, you cannot override the job queue, even if the queue kernel is active, unless you choose the Override Location option.

Note. Overriding the job location means that you change the machine that will run the UBE. For example, a UBE might run locally by default. You can override the processing location to a server, and the UBE will run on the server. Conversely, you can change the processing location from a server to a workstation.

EnterpriseOne displays a Verify Overriding the Job Queue form if the job runs locally and you do not override the processing location.

The status of the queue kernel and the default processing location for the UBE determine the way the Override Job Queue option appears in the Advanced Version Prompting form. The following table summarizes the queue kernel status and processing location combinations that can occur, and the effect each combination has on the Override Job Queue option:

Queue Kernel Status	UBE Processing Location	Status of Job Queue Override Option
Inactive	Local or server	Not visible
Active	Local	Visible but disabled
Active	Local, but Override Location option chosen	Enabled
Active	Server	Enabled

Prerequisites

Before you complete the tasks in this section:

- To activate the queue kernel, make sure you have the following settings in the server's jde.ini file:

```
[JDENET_KERNEL_DEF14]
krnlName=QUEUE KERNEL
dispatchDLLName=jdekrnl.dlldispatch⇒
DLLFunction=_DispatchQueueMessage@28max
NumberOfProcesses=1numberofAutoSart⇒
Processes=0
[DEBUG]
QKLog=0
```

Where a value of 0 means that only an error log is generated. You can change the setting to 1 if you need to generate debug logs for troubleshooting purposes.

```
[NETWORK QUEUE SETTINGS]
QKActive=1QKOnIdle=300
```

Where a value of 1 means that the queue kernel is active and a value of 300 sets the queue kernel on idle time to 300 seconds.

- Add the following setting to the client jde.ini file:

```
[NETWORK QUEUE SETTINGS]
QKActive=1
```

Forms Used to Manage Job Queues

Form Name	Form ID	Navigation	Usage
Work With Job Queues	W986130A	Batch Processing Setup menu (GH9013), Job Queues (P986130).	Add a job queue and change the status of a queue.
Job Queue Revisions	W986130B	On Work With Job Queues, click Add.	Add information for a new job queue. Revise or copy a job queue.
Work With Batch Versions - Available Versions	W98305A	Report Management (GH9111), Batch Versions (P98305)	Override a job queue.
Version Prompting	W98305D	On Work With Batch Versions - Available Versions, select a version, and then click Select.	Access the Advanced Version Prompting form. Enter data selection or data sequencing.
Advanced Version Prompting	W98305I	On Version Prompting, select Advanced from the Form menu.	Select the Override Job Queue option.
Job Queue Search	W986130C	On Version Prompting, click Submit.	Find and choose the job queue that you want to override.

Adding a Job Queue

Access the Work With Job Queues form.

To add a job queue:

1. On Work With Job Queues, click Add.
2. On the Job Queue Revisions form, complete the following fields and option, and click OK:
 - Host
Enter the name of the server on which the queue will run.
 - Job Queue
Enter the name of the queue.

- **Job Queue Status**
Enter 01 if you want the queue to be active, or 02 if you want the queue to be inactive.
- **Queue Type**
Define whether the queue is an EnterpriseOne queue or a non-EnterpriseOne queue. A non-EnterpriseOne queue works only on the iSeries server.
- **Maximum Batch Jobs**
Define the maximum number of jobs that can run in the queue.
- **Port Number**
Identify the port number for the server instance on which the queue will run.
- **Default Queue**
Check the box for the default queue, or leave it blank for a non-default queue.

Revising a Job Queue

Access the Work With Job Queues form.

To revise a job queue:

1. On Work With Job Queues, find the queue that you want to revise and click Select.
2. On Job Queue Revisions, complete any of the following fields and option to revise the queue, and then click OK:
 - Host
 - Job Queue
 - Job Queue Status
 - Queue Type
 - Maximum Batch Jobs
 - Port Number
 - Default Queue

Copying a Job Queue

Access the Work With Job Queues form.

To copy a job queue:

1. On Work With Job Queues, find the queue that you want to copy and click Copy.
2. On Job Queue Revisions, complete any of the following fields to copy the queue and click OK:
 - Host
 - Job Queue
 - Job Queue Status
 - Queue Type
 - Maximum Batch Jobs
 - Port Number

- Default Queue

Changing the Status of a Job Queue

Access the Work With Job Queues form.

To change the status of a job queue:

1. On Work With Job Queues, find the queue whose status you want to change.
2. From the Row menu, select Change Status.

EnterpriseOne changes the status of the queue from Active to Inactive or from Inactive to Active, depending on its previous status.

Overriding a Job Queue

Access the Work With Batch Versions - Available Versions form.

To override a job queue:

1. On the Work With Batch Versions - Available Versions form, find a version of a job that you want to submit and click Select.
2. On the Version Prompting form, choose Advanced from the Form menu.
3. On the Advanced Version Prompting form, choose the Override Job Queue option and click OK.

Note. If the queue kernel is not active, this option is not visible.

4. In the Version Prompting form, select either, both, or neither of the following options and click Submit:
 - Data Selection
 - Data Sequencing
5. On the Job Queue Search form, find the name of an available queue for the host and port name.
6. Select the queue that you want to override to and click Select.
7. Complete the data selection and sequencing and the processing options required to submit the job and choose a printer, if necessary.

Managing EnterpriseOne Subsystems

This section provides an overview of EnterpriseOne subsystems and discusses how to:

- Locate subsystems running on a server.
- Review job records for subsystems.
- Terminate subsystems.

Understanding EnterpriseOne Subsystems

Within PeopleSoft EnterpriseOne, subsystems are defined as continuously running batch jobs that run independently of, and asynchronously with, EnterpriseOne applications. Subsystem jobs function within the logical process of the operating system or the queue defined for the server platform. You can configure EnterpriseOne to use one or more subsystems.

The term *subsystem* is an industry-wide generic term that usually indicates a system that is a subprocess to an operating system. On iSeries server platforms, a subsystem is a logical process that is used to run system jobs, whether they are PeopleSoft EnterpriseOne or other application jobs. For UNIX, an EnterpriseOne subsystem is functionally equivalent to a daemon. On UNIX and Windows server platforms, system jobs are processed in queues; these queues are functionally equivalent to subsystems on the iSeries platform.

How EnterpriseOne Uses Subsystems

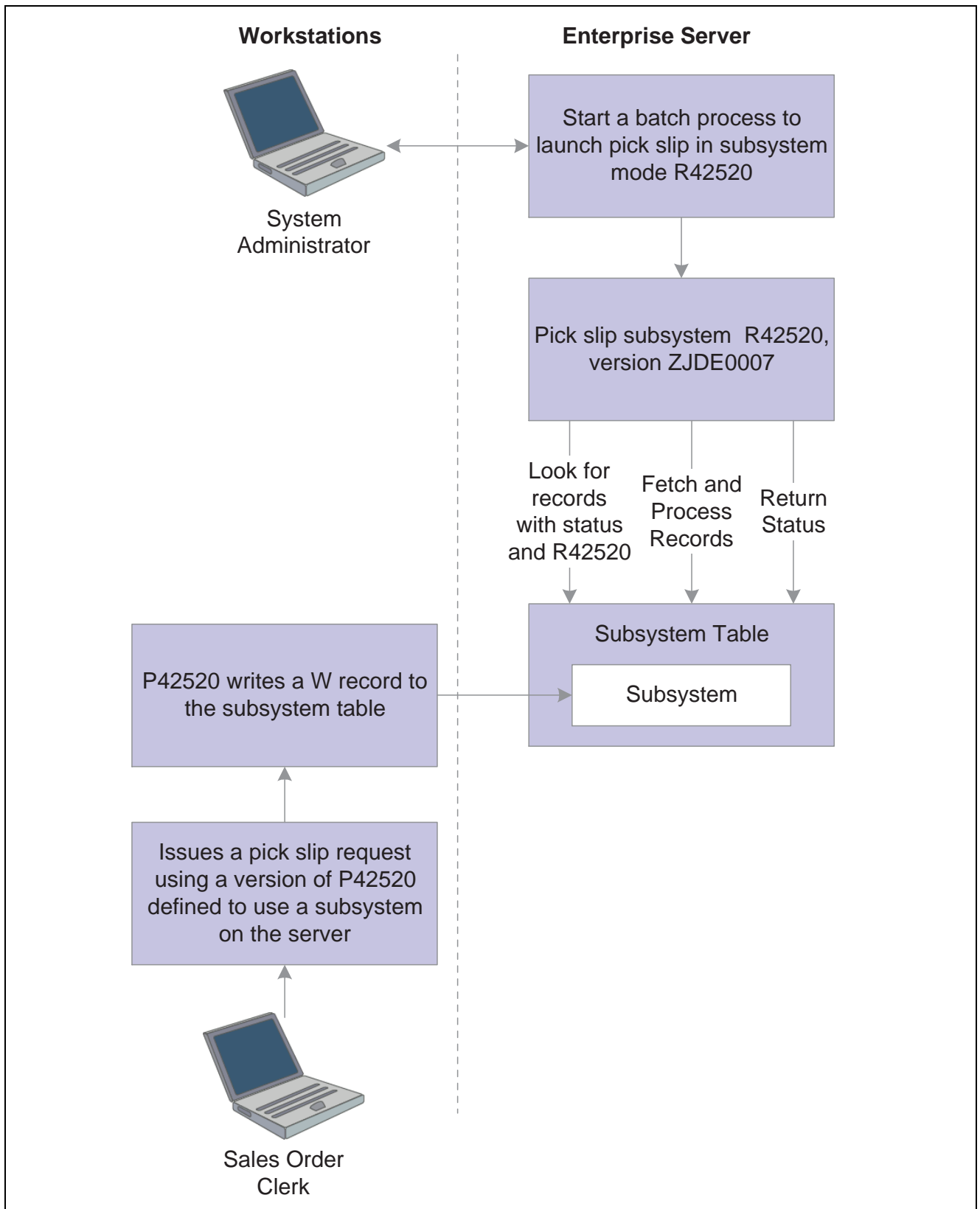
Some PeopleSoft EnterpriseOne applications are designed to use subsystems to complete needed work. For example, you can instruct Sales Order Processing to print pick slips through an EnterpriseOne subsystem. You activate a subsystem through the processing options of a batch application. Then you create a specific version of the batch application, using that processing option to run the application in subsystem mode.

You must manually start subsystems to minimize the consumption of system resources. When started, EnterpriseOne subsystems run continuously, looking for and processing requests from EnterpriseOne applications. Subsystems run until you terminate them.

Typically, you use subsystem jobs running on the enterprise server to off load processor resources from the workstation. Instead of queuing requests and running them in batches at specified times of the day, you can direct the requests to a subsystem, where they are processed in realtime. For example, you might be running the Sales Order Entry application on a workstation and want to print pick slips. If you are using a version of pick slips that has the Subsystem Job function enabled, the request is executed by a subsystem job. The pick slip request is routed to and processed by the subsystem job on the defined enterprise server. As a result, no additional processing resources are required from the workstation machine to actually print the pick slip.

When an application issues a request for a job to run in a subsystem, it places a record in the Subsystem Job Master table (F986113). These records are identified by subsystem job name and contain status and operational indicators. Embedded in the record is key information that allows the subsystem to process the record without additional interaction with the requesting application. The continuously running subsystem monitors the records in this table. If the subsystem finds a record with its process ID and appropriate status indicators, it processes the record and updates the status accordingly.

This illustration displays the logical sequence of events associated with subsystems:



Enabling Subsystems

To prevent excessive processing overhead during server startup and to prevent unnecessary uses of processor resources for subsystem jobs that might be in use, you must manually start subsystems. Generally, the system administrator or manager-level user is responsible for this task. To manually start subsystems, a version of a PeopleSoft EnterpriseOne batch process with a processing option set to enable the use of subsystems is run.

As described, the way that you initially control the creation and start-up of these subsystems and queues depends on the server platform.

Platform (Subsystem or Queue)	Description
iSeries (JDENET)	<p>One iSeries subsystem is used for EnterpriseOne. This subsystem is started automatically when you issue the EnterpriseOne startup command STRNET. The subsystem name is version-specific. For example, for release 8.10, the subsystem name is psft810.</p> <p>To process requests that are destined for EnterpriseOne subsystems, you must define a specific job queue running under the JDENET subsystem. For example, a job queue might be named QBATCH.</p> <p>User requests for EnterpriseOne subsystem-defined batch jobs are executed by the job queue that is based on definition in the iSeries user profile.</p>
UNIX (jdequeue)	<p>One or more queues can exist for EnterpriseOne. These queues can be named the same or differently. You define queues by parameters in the startup shell scripRunOneWorld.sh.</p> <p>To process requests that are destined for subsystems, you must define one or more queues. For example, a jdequeue might be named QBATCH.</p> <p>User requests for subsystem-defined batch jobs are executed by the job queue, based on the process ID.</p>
NT (jde.ini settings)	<p>One or more queues can exist for EnterpriseOne. These queues must have the same name. You define queues using settings in the jde.ini file.</p> <p>To process requests that are destined for subsystems, you must define the name and number of queues in the [NETWORK QUEUE SETTINGS] section of the jde.ini file. For example, a jdequeue might be named QBATCH.</p> <p>User requests for subsystem-defined batch jobs are executed by the job queue, based on the process ID.</p>

System administrators can display all of the subsystems that are running on a server by using the Subsystem Jobs application (P986113). Use this application to:

- Locate a list of subsystems that are running on a server.
- Locate a list of subsystem records that are unprocessed (not available for iSeries servers).
- Locate the current record that a subsystem is processing (not available for iSeries servers).
- Stop or delete any subsystem.

Subsystem Job Records

Multiple EnterpriseOne processes write records to the Subsystem Job Master table (F986113). Each record has a status code that identifies subsystem request types and operational status. You can use Work With Server Jobs to view the records in this table.

Terminating Subsystems

You can use Work With Server Jobs to terminate subsystems. The following two methods of termination are available:

- Stopping a subsystem job causes it to terminate after it completes processing the current record. Additional unprocessed records in the Subsystem Job Master table (F986113) will not be processed, and no new records can be written. Essentially, the unprocessed records will be lost; that is, the process that initiated the record is not notified that the record was not processed.
- Ending a subsystem job causes it to terminate after processing all of the existing subsystem records. No new records can be written to the Subsystem Job Master table (F986113).

Forms Used to Manage EnterpriseOne Subsystems

Form Name	Form ID	Navigation	Usage
Work With Servers	W986116A	System Administration Tools (GH9011), Work With Servers (P986116).	Select a server in which you want to locate a subsystem.
Work With Subsystems	W986113A	On Work With Servers, from the Row menu, select Subsystem jobs.	Review the status and type of the subsystem. Stop or end a subsystem.
View Jobs	NA	On Work With Subsystems, from the Row menu, select View Jobs.	Review server jobs and job types.

Locating Subsystems Running on a Server

Access the Work With Servers form.

To locate subsystems running or waiting on a server:

1. On Work With Servers, select a server from the list or use the query by example row to choose a specific server.
2. From the Row menu, select Subsystem Jobs.
3. On Work With Subsystems, select one of the following two options:

- &Processes

A process is a subsystem that is waiting for work. It is identified by an S (subsystem job) value in the Job Type field.

- &Waiting Jobs

Waiting jobs are report jobs that are queued for a subsystem. They are identified by an R (subsystem record) value in the Job Type field.

All currently running subsystems are displayed. Report number and version identify the running subsystems. The status of each subsystem is displayed by codes in the fields:

- Job Type

This field indicates whether the status is a subsystem record or a subsystem job. Values are:

Value	Definition
R	Subsystem record.
S	Subsystem job.

- Job Status

This field indicates whether the status is a subsystem job or record. Values are:

Value	Definition
W	Subsystem record waiting.
P	Subsystem record processing.
E	Subsystem record to end the job.
R	Subsystem job running.

Reviewing Job Records for Subsystems

Access the Work With Subsystems form.

To view job records for subsystems:

1. After locating a subsystem job, on Work With Subsystems, click Find.
2. Select a record in the detail area, and then select View Jobs from the Row menu.
3. On View Jobs, click Find.

A list is displayed for all server jobs in the Subsystem Job Master (F986113) with an R (subsystem job running) job type.

Terminating Subsystems

Access the Work With Subsystems form.

To terminate subsystems:

1. Select the running subsystem that you want to stop.
2. To stop a subsystem, from the Row menu, select Stop Subsystem.

Note. If you are viewing Waiting Jobs from Work With Server Jobs or if you are viewing subsystem jobs by choosing the View Jobs from Work With Server Jobs, the Stop Subsystem selection is disabled from the Row menu selection.

3. To end a subsystem, from the Row menu, select End Subsystem Job.

Note. If you are viewing Waiting Jobs from Work With Subsystems, the End Subsystem selection is disabled from the Row menu selection.

4. On End Subsystem Job, click OK.

CHAPTER 6

Working with User Profiles

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

- Add new users
- Set up user profiles
- Set up user roles

Understanding User Profiles

A user profile defines a specific user to a PeopleSoft EnterpriseOne role. Profiles define such information as the role to which one or more users belong, a list of environments that a user or role can select when signing onto EnterpriseOne, and the language preference of the user. You use the User Profile Revisions application (P0092) to add users and to set up user profiles. You can also assign roles to users. A role defines the tasks that an end user sees in PeopleSoft EnterpriseOne.

You can use the User Profile Revisions application to define specific users or roles. This definition includes:

- The role to which a user belongs.
For example, an accounts payable clerk would be part of the AP role. Roles are an important aspect of PeopleSoft EnterpriseOne. By assigning users to roles, system administrators can set user preferences and securities that are based on the roles rather than the individual user.
- The environments that the user can select when signing on to EnterpriseOne.
- The language preference and country code for the text that appears on EnterpriseOne menus, forms, and country-specific applications.

Understanding How Role Profiles Make Profiling Easier

Role preferences eliminate the need to set up preferences for each individual user profile. By assigning individual users to a role, you can perform assignments once for the role and have those settings available to all of the individual users who have that role.

You can also specify different preferences for each user. The individual user settings override the role settings, but if no user profile information exists, the software uses the information from the role profile.

PeopleSoft EnterpriseOne uses roles for these purposes:

- Environments.
- User overrides.
- Application security.
- Creation of sign-in security records.

Tables Used by the User Profile Revisions Application

The User Profile Revisions application uses these tables:

- Library Lists - User (F0092)
- User Display Preferences (F00921)
- User Display Preferences Tag File (F00922)
- User Access Definition (F00925)
- Library List Control (F0093)
- Library List Master File (F0094)
- Anonymous User Access Table (F00926)

Adding New Users

This section provides an overview of how to add new users and discusses how to:

- Add an individual user
- Add multiple users

Understanding How to Add Users

You can create user profiles one at a time by using the User Profile Revisions application, or you can simultaneously create multiple profiles by using batch processes.

Note. This section is a checklist for all the steps needed to add a new user. These steps do not include installing PeopleSoft EnterpriseOne on a workstation, nor do they address third-party setup issues such as assigning network user IDs.

How to Add Multiple Users

When you are ready to create user profiles for the first time, you might need to create hundreds of profiles simultaneously. In this case, EnterpriseOne provides batch processes to create the profiles. These batch processes automate the process of user profile creation.

When you decide which role to assign to a user, consider application security as the most important role because:

- Application security has the most extensive setup.
- Managing overrides to the role security is more difficult than, for example, managing overrides to deployment preferences.

Note. Sign-in security is not based on roles because individuals must have their own passwords. A program exists with sign-in security to quickly create individual security records by role; however, after the records are created, security is assigned by an individual.

See Also

EnterpriseOne Tools 8.94 PeopleBook: Package Management, “Deploying Packages,” Defining Machines

[Chapter 6, “Working with User Profiles,” Setting Up User Profiles, page 80](#)

[Chapter 6, “Working with User Profiles,” Creating and Modifying User Profiles, page 82](#)

[Chapter 6, “Working with User Profiles,” Creating and Modifying Role Profiles, page 84](#)

[Chapter 6, “Working with User Profiles,” Creating Profiles by Using a Batch Process, page 86](#)

Adding an Individual User

If you need to add only a few users, use the User Profile Revisions program.

These procedure details the steps that you need to perform when adding user profiles one at a time.

To add an individual user:

1. If you plan to create a new role for the user, add an address book record with a valid search type code (for example, *E* for employee).
2. If the existing role profiles are not acceptable for the new user, add a role profile.
3. Add an address book record for the new user.
4. Add a user profile.
5. Add sign-in security records for the user.
6. Use Security Workbench (P00950) to add any security overrides for the user if the user needs different security than the roles to which the user belongs.
7. Populate the machine table for the user’s machine.
8. Add any new user overrides for the user, if the user needs different user overrides than the role to which the user belongs.

Adding Multiple Users

These procedure shows the steps that you need to perform when you add multiple user profiles simultaneously.

To add multiple users:

1. Using the Address Book application (P01012), create address book records for roles that you will use in user profiles.
2. Using the User Profile Revisions application, add the role profiles.
3. Populate the various Address Book tables.
If you are migrating data from a non- EnterpriseOne system, you can populate the data tables with a table conversion. Otherwise, you can manually add data to the Address Book tables.
4. Run the Populate User Profiles (R0092) batch process to create user profile records from existing Address Book records.
Normally, this report is based on address book records with a search type for employees (*E*). You have the option of picking one default role for everyone or running the report more than once for different roles.
5. Adjust each user’s role assignments.

Determine the role in which you want to place an individual and manually assign each user to a role. Change the user environments if they are not standard to that role.

These settings are dictated by role:

- Environments
 - User Overrides
 - Application Security
6. Run the Summary of Environments, Packages and Profiles batch process (R00921) to view the new user profiles.
 7. Use Security Workbench (P00950) to apply application, action, and processing option security for roles and any individual overrides to those roles.
 8. Create sign-in security records using the EnterpriseOne Security application (P98OWSEC).
You can create sign-in security records for all individuals within a role by entering one record for the role.
 9. Manually populate the F00960 table.
This table is automatically populated each time a machine signs in to EnterpriseOne. However, if you intend to use schedule packages, you must manually populate this table.
 10. Create user overrides for roles.
Normally, you will not create any overrides for individuals because they can easily create their own as they use the software.

Setting Up User Profiles

This section provides an overview of setting up user profiles and discusses how to:

- Set processing options for User Profiles (P0092).
- Create and modify user profiles.
- Create and modify role profiles.
- Copy user and role profiles.
- Assign or delete environments to user and role profiles.
- Assign business preferences to user and role profiles.
- Create profiles by using a batch process.
- Review user and profile definitions.

Understanding User Profile Setup

You use the User Profile Revisions application to set up user profiles. When you set up profiles as a system administrator, you create role profiles and user profiles for each user in the system. You also determine the environments that are available for each role and user, and set up display preferences, such as language.

These steps outline the high-level process for setting up user profiles.

1. Create all of the role profiles for the enterprise.

2. Create a user profile for every user.
3. Assign to each role or user these preferences:
 - Environments, to determine the environments that you want to be available to each role or user.
 - Display preferences, to determine EnterpriseOne display characteristics such as language, date format, and country code.

The Display preferences are controlled on the User Profile Revisions form.

Note. If you are setting up user profiles during the installation process, you *must* log on to the deployment server using the deployment environment. After you have completed the installation process, you can add or modify user profiles from any machine *except* the deployment server.

Prerequisites

Before you complete the tasks in this section:

- Create all of the role profile information by using the User Profile Revisions application.
- Define these:
 - Role profiles.
 - Environments that each role can access.

Forms Used to Set Up User and Role Profiles

Form Name	Form ID	Navigation	Usage
Work With User/Role Profiles	W0092D	System Administration Tools (GH9011), User Management, User Profiles (P0092).	Locate and review existing roles and profiles records and access additional forms.
User Profile Revisions	W0092A	On Work With User/Role Profiles, click Add or select a record and then click Select.	Create, modify, or copy a user profile.
Role Revisions	W0092A	On Work With User/Role Profiles, select Add Role from the Form menu. Or, click the Roles Only option, click Find, select a role, and then click Select.	Create or modify a role profile.
User Environment Revisions	W0092C	On Work With User/Role Profiles, select Copy Environment from the Row menu.	Copy environment preferences from one user profile to another. Assign or delete environments from user and role profiles.
Business Preferences	W0092E	On User Profile Revisions, select Business Preferences from the Row menu.	Assign business preferences to user and role profiles.
Work With Batch Versions - Available Versions	W98305A	Report Management (GH9111), Batch Versions (P98305)	Run the Populate User Profiles batch application (R0092) and the Summary of Environments, Packages and Profiles report (R00921).

Setting Processing Options for User Profile Revisions (P0092)

On the A/B Validation tab of the Processing Options form, enter 1 to enable Address Book validation or 0 (or leave blank) to disable Address Book validation.

- When enabled, this processing option validates each new user ID against the Address Book Master (F0101) table upon the creation of a user profiles. Upon creation of a user profile, each new user ID is validated against the F0101 table. As a result, you cannot create a user profile for a user who is not already defined in the F0101 table. We recommend that you enable this setting to ensure that Work Center operates correctly. That application requires valid address book numbers.
- When disabled, this processing option allows you to create user profiles for Address Book entries that do not yet exist in the F0101 table.

Creating and Modifying User Profiles

The system administrator needs to create a user profile for every user. The user profile defines certain setup and display features, such as access to fast path, language, date format, or country code. The administrator should first create all of the role profiles that are needed for the enterprise. This action makes creating profiles easier; instead of defining specific environments, packages, and machine configurations for each user, administrators can define them for the role. If an individual in a role needs a different setup, you can assign different setups at the user level, which overrides the role settings.

If you select a country code for a user, the menu filtering process displays for that user any special menu selections unique to that country code. For example, if you enter *CA* (Canada), that user would see the Canadian Tax Information application on the appropriate menu, which users without that country code would not see.

Access the Work With User/Role Profiles form.

To create and modify user profiles:

1. On the Work With User/Role Profiles form, do one of these operations:
 - To create a new user profile, click Add.
 - To modify an existing profile, click Find, select a user profile in the detail area, and then click Select.
2. On the User Profile Revisions form, in the User ID field, enter the user ID for the individual profile.
3. In the header area of the form, complete the remaining fields.
 - Address Number
 - WhosWhoLineID
 - Menu Identification
 - Default Icon File
4. If you are creating a user profile, in the Display Preferences area, complete these fields, and then click OK:
 - Language
 - Visually Impaired
 - Date Format
 - Date Separator Character
 - Decimal Format Character
 - Localization Country Code
 - Universal Time
 - Time Format
 - Daylight Savings Rule

User ID	The code that identifies a user profile.
WhosWhoLineID	A value that references the Who's Who Line ID in Address Book.
Menu Identification	<p>The menu name, which can include up to nine characters. PeopleSoft EnterpriseOne standards are:</p> <ul style="list-style-type: none"> • Menu numbers are preceded with a G prefix. • The two characters following the prefix are the system code. • The next characters further identify the menu. • The 4th character specifies a skill level. • The 5th character distinguishes two menus of the same system with the same skill level. <p>For example, the menu identification G0911 specifies:</p> <ul style="list-style-type: none"> • 09 is the system code.

	<ul style="list-style-type: none"> • 1 is the display level or skill level. • 1 indicates that this is the first menu.
Default Icon File	The path field contains the path used for client based menus. The path describes where the application is located on the computer or network. A path includes the drive, folders, and subfolders that contain the application to be executed.
Language	A user defined code (01/LP) that specifies the language to use on forms and printed reports. Before you specify a language, a code for that language must exist at either the system level or in the user preferences.
Date Format	<p>The format of a date as it is stored in the database.</p> <p>These date formats are valid: YMD, MDY, DMY, EMD. If you leave this field blank, the system displays dates based on the settings of the operating system on the workstation. With NT, the Regional Settings in the Control Panel control the settings for the operating system of the workstation.</p>
Date Separator Character	The character to use when separating the month, day, and year of a given date. If you enter an asterisk, the system uses a blank for the date separator. If you leave the field blank, the system uses the system value for the date separator.
Decimal Format Character	The number of positions to the right of the decimal that you want to use. If you leave this field blank, the system value is used as the default.
Localization Country Code	A code that identifies a localization country. It is possible to attach specific county functionality that is triggered baed on this code using the country server methodology in the base product.
Universal Time	A code that you use to associate a time zone with a user's profile. This code represent the user's preferred time zone, and it must be a value from the UDC table (H91/TZ).
Time Format	A code that determines the user's preferred format for time-of-day. The user can choose from a 12- or 24-hour clock.
Daylight Savings Rule	A code that specifies the daylight savings rule for a region or country.

Creating and Modifying Role Profiles

Access the Work With User/Role Profiles form.

To create and modify role profiles:

1. On the Work With User/Role Profiles form, do one of these operations:
 - If you want to create a new role, select Add Role from the Form menu.
 - If you want to modify an existing profile, click the Roles Only option. Click Find, select a role in the detail area, and then click Select.
2. On the Role Revisions form, enter the name of the role, such as ACCOUNTING, in the User ID field. When you modify a role profile, this field displays the name of the role.

Note. You cannot type new information in this field when you modify a role.

3. Complete or modify these fields, as necessary:

- Address Number
Enter an address book number if the role will be used with a workflow.
 - Menu Identification
 - Default Icon File
4. Click OK.

Copying User and Role Profiles

You can copy all or part of a user profile. When you copy an entire user or role profile (display and environment preferences), you are creating a new user profile with the information from another profile. When you copy part of a user profile, you are copying the environment preferences from another profile to an already existing user profile.

Access the Work With User/Role Profiles form.

To copy user or role profiles:

1. On the Work With User/Role Profiles form, locate a user profile, and do one of these:
 - To copy an entire profile (the display, environment, and deployment preferences), click Copy.
The User Profile Revisions form appears. Because this action creates a new profile, the user profile that you create cannot already exist in EnterpriseOne.
 - To copy environment preferences, from the Row menu, select Copy Environment.
The User Environment Revisions form appears. This action copies environment preferences from one user profile to another. The user profile that you copy to must already exist.
2. In the User/Role field, enter a user ID or role name to copy the profile into and change any other information.
3. Click OK.

Assigning or Deleting Environments to User and Role Profiles

You can assign a list of environments that each role or user can choose from when starting EnterpriseOne. If a user does not have a user profile-specific environment assignment, the user can choose from the environments that are assigned from the user's role each time that the user starts EnterpriseOne. You can assign more than one environment from which a user can choose, or delete environments if they are no longer relevant to the user.

Access the Work With User/Role Profiles form.

To assign or delete environments:

1. On Work With User/Role Profiles, click Find, and then select a user profile.
2. From the Row menu, select Environments.
The User Environment Revisions form appears. This form displays the list of environments available for a particular user or role.
3. To add a new environment, complete these fields on the last row:
 - Display Seq.
 - Environment
4. To delete an environment from the list, select the environment and click Delete.

Display Seq. display sequence	A number that specifies the sequence of information.
Environment	This field represents a valid environment that can be used to run EnterpriseOne. The environment encompasses both a path code (objects) and a data source (data). When these elements are put together, users have a valid workplace within the system.

Assigning Business Preferences to User and Role Profiles

When setting up profiles, you can assign business preference codes. These codes can be used by a customized workflow process to send messages, update a database, or start an application. You define the codes for the preferences based on industry, business partner, or customer. Then, you can use the EnterpriseOne Workflow Tools applications to create a workflow process that is based on whether a specific code resides in the user profile.

For example, you assign the code *CUS* for a customer business preference, and then create a workflow process that begins whenever a user profile with the *CUS* business preference enters a sales order.

Access the Work With User/Role Profiles form.

To assign a business preference to user and role profiles:

1. On Work with User/Role Profiles, click Find.
2. Select a user profile, and then click Select.
3. On User Profile Revisions, from the Form menu, select Bus Preferences.
4. On Business Preferences, complete any of these fields and click OK:

- Industry Code

This field associates the user profile with a specific industry, such as manufacturing.

- Business Partner Code

This field associates the user profile with a specific business partner.

- Customer Code

This field associates the user profile with a specific customer.

Note. Click Cancel on the Business Preferences form to cancel the addition of the current business preference.

Creating Profiles by Using a Batch Process

If address book records already exist for employees, you can run a batch process to automatically create user profiles from those address book records. This process can save time, ensure accuracy between the Address Book and user profile records, and ease the transition of taking EnterpriseOne to production.

You can create user profiles through the Populate User Profiles batch application (R0092). With this process, you can assign display and environment preferences to users. This process enables you to create hundreds of new user profiles at a time.

Note. If you need to add just a few users, you should use the User Profile Revisions application.

Access the Work With Batch Versions - Available Versions form.

To run the R0092 batch application:

1. On Work With Batch Versions - Available Versions, enter *R0092* in the Batch Application field and click Find.
2. Select the PeopleSoft EnterpriseOne default version (XJDE0001) or the equivalent for the installation, and then click Select.
3. On the Versions Prompting form, click Data Selection, and then click Submit.
4. On the Data Selection form, create a logic statement that describes the set of users for which you want to create profiles.

This form already has a search type of *E* (employees) populated, which assumes that the users are all employees. You might want to narrow this selection by submitting it for only a range of employees.

After you complete the Data Selection form, the Processing Options form appears.

5. On the Processing Options form, enter this information:
 - Enter one of these values for option 1:

Enter *1* to run this report in proof mode, which provides an example of what would happen if you were to run the report in final mode.

Leave blank to run this report in final mode, which creates the user profiles that you specified and creates a report showing the profiles created.
 - Enter one of these values for option 2 to define the user profile record being created for each user:

Enter *1* to populate the User ID field with the users' address book numbers plus their initials. Typically, user profiles are created with the users' initials preceding their Address Book number.

Leave this field blank to use just the address book number.

Complete these user profile fields for option 2:

Fast Path

Language

Date Format

Data Separator Character

Data Format Character

Country
 - For option 3, enter any additional environments that you want the user to have access to instead of the environments already established for the user's role.

Reviewing User and Profile Definitions

The Summary of Environments, Packages and Profiles report (R00921) is useful if you need to review a list of user and role profile definitions. This report summarizes the environment or environments assigned to a role, lists the users in the role, and notes any additional environments that are assigned specifically to an individual user. EnterpriseOne provides two default versions that enables you to summarize either all roles or only specific roles.

Access the Work With Batch Versions - Available Versions form.

To run the R00921 report:

1. On Work With Batch Versions - Available Versions, select a version and click Select.

The default version XJDE0001 creates a report for all role profiles in the enterprise. The default version XJDE0002 creates a report about a specific role profile that you specify.

2. On the Versions Prompting form, click Data Selection and click Submit.
3. On the Data Selection form, create a logic statement that describes the role profiles that you want to summarize.
4. Click OK.

Setting Up User Roles

This section provides an overview of user roles and workstation initialization file parameters and discusses how to:

- Migrate roles.
- Define roles.
- Revise roles.
- Sequence roles.
- Add an environment to a role.
- Set up a role relationship.
- Choose roles for display at sign-in.
- Enable the role chooser.
- Create role-to-role relationships.
- Revise role relationships.
- Delegate roles.
- Add roles to a user.
- Add users to a role.
- Copy user roles.
- Add a language translation to a role.
- Change a role description.

Understanding User Roles

After you have set up user profiles, you can assign roles to the users in the organization. A role defines the tasks that a user sees when working in a task view of the PeopleSoft Solution Explorer. You also use roles to define a user's permissions within EnterpriseOne. You can customize each role to provide the appropriate level of access to EnterpriseOne functions.

Assigning roles accomplishes these purposes:

- Users see only those tasks and perform only those activities that relate to their jobs.

For example, a user playing the role of accounts payable clerk might not need to see all of the tasks that an accounts payable manager would need to see. You can create both of these roles and define a different set of tasks for each one.

- Users can have multiple roles.

Within an organization, a user might have many responsibilities, none of which are defined by a single role. A user who is assigned multiple roles can switch roles according to the work required.

- Administrators can set up security based on user roles.

A user's access to applications, forms, table columns, data sources, and so on is based on one or more roles to which the user is assigned.

From an administrator's point of view, the steps required to set up roles for users are summarized in this table:

Administrative Step	Applications Used	Forms Used	Tables Used
Populate the User Profile table with roles that are stored in UDC H95/RL during Roles Phase I.	R89959211, R89959212	Not applicable (NA).	F00926, F0092
Run a program to populate the Role Relationships table.	R8995921	NA.	F0092, F95921
Define roles.	P0092 (User Profile Revisions)	W0092A (User Profile Revisions); Form exit from the Work With User Profiles form (W0092D).	F0092
Sequence the roles.	P0092	W0092L (Work With Role Sequences); Form exit from the Work With User Profiles form.	F00926
Create role relationships that associate users with roles.	P95921 (Role Relationships)	W95921A (Work With Role Relationships).	F95921
Add security to roles.	P00950 (Security Workbench)	Various, depending on type of security to be applied to each role.	F00950

The Portal, PeopleSoft Solution Explorer, and client workstations use the role relationships data in the F95921 table (Role Relationships) and various APIs to retrieve data and allow users to have assigned roles.

You use EnterpriseOne to administer defined roles for which you have created role relationship records. You can add large numbers of roles to a single user, and you can add large numbers of users to a single role relationship record. You can also use EnterpriseOne to specify the language that is used for the description of a new role.

Workstation Initialization File Parameters

At the EnterpriseOne sign-in, you can choose one or more roles, depending on how many are assigned to you. If you choose **ALL*, you enter EnterpriseOne in all of the assigned roles that are flagged as Include in **ALL*. Two parameters relate to roles in the workstation jde.ini file. This table displays the parameters, the .ini file section in which they are found, and the default settings. These settings are defined by the administrator when EnterpriseOne is first configured, so you should not have to perform this task when performing routine administrative tasks.

Jde.ini Parameter	Jde.ini Section	Default Setting
LASTROLE	[SIGNON]	*ALL Defines the role that appears for the user to choose at sign-in.
Default Role	[DB SYSTEM SETTINGS]	*ALL

The LASTROLE parameter value defines the role that appears in the sign-in screen when EnterpriseOne is launched.

See Also

Chapter 6, “Working with User Profiles,” Choosing Roles for Display at Sign-in, page 97

Forms Used to Set Up User Roles

Form Name	Form ID	Navigation	Usage
Work With User / Role Profiles	W0092D	Systems Administration Tools (GH9011), User Management, User Profiles (P0092).	Locate and review existing roles and access additional forms to add or revise roles.
Role Revisions	W0092A	On Work With User/Role Profiles, from the Form menu, select Add Role.	Add a role or revise information for an existing role.
Work With Role Sequences	W0092L	On Work With User/Role Profiles, from the Form menu, select Role Sequence.	Define the sequence of roles.
User Environment Revisions	W0092C	On Work With User/Role Profiles, select a role, and then select Environments from the Row menu.	Add an environment to a role.
Work With Role Relationships	W95921A	On Work With User/Role Profiles, select Role Relationships from the Form menu.	Set up, revise, and remove roles for a user.
Role Revisions	W95921C	On Work With Role Relationships, select a role from the Available Roles tree and click the left-arrow button.	Enter dates on which you want the role to start and end (optional). You can also select an option to add the role to the user's *ALL sign-in.
Enable/Disable Role Chooser	W95921E	On Work With Role Relationships, select Enable Role Chooser from the Form menu.	Enable user to choose role from a list of all assigned roles at sign-in.

Page Name	Object Name	Navigation	Usage
Work with Distribution Lists	W95921A	On Work With Role Relationships, select Distribution Lists from the Form menu.	Create role-to-role relationships.
Work With Delegation Relationships	W95921J	On Work With Role Relationships, select Roles Delegation from the Form menu.	Delegate a role from one user to another.
Add Roles to User	W95921P	On Work With Role Relationships, from the Form menu, select Add Roles to User.	Add roles to a user.
Add Users to Roles	W95921Q	On Work With Role Relationships, from the Form menu, select Add Users to Roles.	Add users to a role relationship record.
Copy User Roles	W95921O	On Work With Role Relationships, complete the User field and click Find. Click Copy.	Copy roles from one user to another.
Work With Language Role Descriptions	W0092J	On Work With User/Role Profiles, click the Roles Only option. Select a role, and from the Row menu, select Role Description.	View a role to which you want to add a language translation. Change a role description.
Language Role Description Revisions	W0092I	On Work With Language Role Descriptions, click Add.	Add a language translation to a role.

Migrating Roles

On a client machine, open the Batch Versions application in EnterpriseOne, and run these universal batch engines (UBEs) to migrate generic roles into the environments.

Run the TC R89959211

Table Conversion (TC) R89959211 takes all of the current roles in the UGRP field in the Library Lists - User table (F0092) and adds a Description record for them in the Anonymous User Access Table (F00926). Both the role and description are populated with the group name (for example, OWTOOL). A sequence number is added to the record in the F00926 table as well. This sequence number begins at 1500 and increments by 5 with each record that is written.

This TC has no processing options.

The performance of this TC is directly dependent upon the number of *GROUP records in the F0092 table. It should finish quickly.

After processing, this TC produces no report. To verify that the table conversion completed, open the Universal Table Browser (UTB) and check the F00926 table for some of the groups that are defined in the F0092 table. For example, check the field USER for *OWTOOL*, the field ROLEDESC for *OWTOOL*, and the field SEQNO for a sequence number that is greater than 1500.

Run the TC R8995921

TC R8995921 takes all of the current user profile records in the F0092 table and inserts a user/role relationship record that is based on the F0092.USER and F0092.UGRP tables. The record that is added to the F95921 table contains the user, role (formerly the group for this user in the F0092 table), and effective and expiration dates. Some of these values are based upon the values in the processing options.

The recommended processing option values are:

- Final/Proof Modes

It is recommended that the TC be run in proof mode first. This mode inserts records to the F95921 table, but it does not remove the group from the user's profile. After the UBE is successfully run in proof mode, check some of the records in the F95921 table to see if they were added successfully. You can re-run the TC in final mode with the same processing options. A new record is not inserted for the user if the effective date is the same as the previously run TC's effective date, so you only remove the group data from the F0092.UGRP field for that user.

- Effective Date

The start date of the role relationship. With current users (those in F0092 table), you want to use the date that the TC is run. (When running in final mode, use the date that the TC was run in proof mode to prevent the system from adding a new set of records into the F95921 table.) This field must not be modified within the role relationship record later.

- Expiration Date

The end date of the role relationship. If this date is left blank, the relationship never expires. With the current users (those in the F0092 table), you should leave this blank so they do not expire from their current group or role.

This field can be modified within the role relationship record later.

- Included In All

This flag indicates that the security of this role is applied when the user chooses to enter EnterpriseOne under the role of *ALL. Use this flag if a user is being added to a sensitive role, such as Payroll or PVC. This field can be modified within the role relationship record later.

The performance of this TC directly depends upon how many user records are in the F0092 table. It should finish quickly.

This TC produces no report. To verify that the TC completed in proof mode, open the UTB and check the F95921 table for some of the users who were defined in the F0092 table. See that their old group (F0092.UGRP) is now their Role F95921.RLFRROLE. To verify that the TC has completed in final mode, view the F0092 table through the UTB, and verify that no data is in the UGRP fields.

Sequence the Roles

Roles must be sequenced for security to work. The previous UBE and TCs sequence the roles, but probably not in the desired order. Sequence the roles through the Sequence Roles menu option. This displays all of the current roles in a parent/child tree. Expand the tree and view the current sequence number. You can drag and drop these roles into the desired sequence. You *must* click the exit Set Sequence to commit the roles sequence to the database.

Add Environments

Environments can be added to roles in the same way that they were previously added to groups. When a user selects a particular role at sign-in, the environments that are associated with that role appear in the Environment Selection List form. If the user selects *ALL environments, all of the environments that are associated with all of the users roles which have been marked as "included in all" appear in the Environment Selection List form. All environments are validated against the User's Pathcode.

Set up the JDE.INI/JAS.INI file

Open the jde.ini file and jas.ini file and verify these settings:

Note. You should not have to add or change these settings.

```
[SECURITY]
DefaultRole=*ALL
[REPLICATION]
DefaultRole=*ALL
[SIGNON]
LastRole=<Users Last Role>
This value is populated when a user signs into EnterpriseOne.
[DB_SYSTEM SETTINGS]
DefaultRole=*ALL
```

Server Executables

Run a PortTest.

Set Up Security

Complete these Universal Batch Engines (UBEs) to set up user security.

Run the UBE R98OWPU

UBE R98OWPU performs a select distinct on the F98OWSEC table to find all unique combinations of Proxy (System) User and Data Source. After these records are found, the UBE inserts this record into the F98OWPU table. The record contains the Proxy User, Data Source, Password, and audit information.

Note. This UBE must be run locally because the business function resides only on the client machine.

This UBE has no processing options.

The performance of this UBE is directly dependant upon how many proxy users are associated with user records in F98OWSEC table. It should finish quickly.

To verify that the UBE completed successfully, open the UTB and check the F98OWPU table for some of the proxy users that are in F98OWSEC table.

If you want to change a proxy user password, you have to change it only once for each proxy user and not for every record in the F98OWSEC table that contains the proxy user.

Run the UBE R98OWUP (Optional)

UBE R98OWUP updates the current F98OWSEC table records, based upon the processing options that you select. This UBE can populate these new fields for current users, as their F98OWSEC table records do not contain values for these options:

- Password Change Frequency
- Allowed Sign-in Attempts
- Enable / Disable User
- Daily Password Change Limit
- Force Password Change

Set these procession options:

- Proof or Final

Indicates whether to run in proof or final mode. Proof mode does not commit records.

- Password Change Frequency

For a given user, this option determines the maximum number of days before the system requires a password change.

- Allowed Attempts

The number of times that users can unsuccessfully attempt to log on before their EnterpriseOne account is disabled.

- Enable/Disable User

Indicates if the user's account is enabled or disabled. A disabled account is not allowed into EnterpriseOne.

- Daily Password Change Limit

The number of times that users can change their password in one day. Because the last ten passwords of a user are stored in the BLOB, it is a security hole to allow users to change their password as many times as they want. If users want to keep their current password, they can change it 11 times in one day so that they are not back to the original.

- Force Immediate Password Change

This option requires users to immediately change their password. You might not want to set this option for all users.

The performance of this UBE is directly dependant upon how many proxy users are associated with user records in the F98OWSEC table. It should finish quickly.

To verify that the UBE completed successfully, access the User Security application (P98OWSEC), and find a user or role whose record should have changed. Verify that the values are correct.

Defining Roles

As part of the system setup, you must define the roles for users in the organization. These roles define the tasks that users see when they work in the EnterpriseOne Menu and determine what authority the users have in EnterpriseOne. After you have defined a role, you can associate users with it and apply security to it.

EnterpriseOne stores the role descriptions in the F00926 table. If you previously defined roles using the UDC table H95/RL, you can run the Populate Role Descriptions From F0092 report (R89959211) to populate the Anonymous User Access Table with those older role descriptions.

See *EnterpriseOne Tools 8.94 PeopleBook: Solution Explorer*, "Using the Menu Design Mode," Applying Roles to a Task.

See [Chapter 8, "Using Security Workbench," page 109](#).

Access the Work With User/Role Profiles form.

To define a role:

1. From the Form menu, select Add Role.

Note. You cannot add a role by clicking the Add button on the toolbar of the Work With User/Role Profiles form.

2. On the Role Revisions form, complete these required fields:

- Role

Enter the name of the role and a description.

- Sequence Number

You must enter a number to specify the sequence number of the role in relation to other roles.

For a user assigned to more than one role, the sequence number determines which role is chosen when a security conflict exists among the different roles.

3. Complete any of the remaining fields, as necessary, and click OK.

Revising Roles

Using the Work With User/Role Profiles form, you can find all of the roles that you have defined. You can then choose a role and modify its properties by using the Role Revisions form. The Role Revisions form enables you to change the properties of the role, including its description, address number, and menu identification.

Access the Work With User/Role Profiles form.

To revise roles:

1. Select the Roles Only option.
2. Select a role that you want to revise and click Select.
3. On the Role Revisions form, make needed changes and click OK.

Sequencing Roles

The Work With Role Sequences form contains all of the roles that you defined and enables you to assign a sequence to each role. The sequence defines a hierarchy of roles and determines which role is active when a security conflict exists among a user's roles.

To sequence roles, you use the User Profile Revisions application.

Access the Work With Role Sequences form.

To sequence roles:

1. Select a role from the tree structure and drag it to the point in the sequence that you want.
2. After you have set the order that you want, select Set Sequences from the Form menu and click Close.
3. If you decide you do not want to change the sequence, select Close Without Set from the Form menu and click Close.

Adding an Environment to a Role

You define each role when you set up roles in the User Profile Revisions application. You can assign one or more environments to each role, and then, when the user signs on to EnterpriseOne, the Environment Chooser and Role Chooser present each user with a list of valid roles and environments.

Use the Work With User/Role Profiles form to assign a new environment to a role or to change an existing environment for a role.

See [Chapter 6, “Working with User Profiles,” Choosing Roles for Display at Sign-in, page 97](#).

Access the Work With User/Role Profiles form.

To add an environment to a role:

1. On the Work With User/Role Profiles form, select the Roles Only option and click Find.

Note. The Both Users and Roles option also allows you to perform the same task, although the Roles Only option is the simplest way to add an environment.

2. Select a role from the detail area of the grid, and select Environments from the Row menu.
3. On the User Environment Revisions form, complete these fields and click OK:

- Display Seq.(display sequence)

This value specifies the order in which the environments will be presented in the Environment Chooser at EnterpriseOne sign-in.

- Environment

You can choose from a list of values that appears when you click the visual assist.

Note. If you want to change an existing environment for a role, enter a new value for the Environment parameter and click OK.

Setting Up a Role Relationship

A role relationship associates a user with a defined role. You can assign more than one user to a role, or you can assign more than one role to a user. To establish a role relationship, you use the Role Relationships application (P95921), which enables you to add, remove, or revise a role relationship for a user.

Access the Work With Role Relationships form.

To set up a role relationship:

1. Complete the User field and click Find.

The system displays the user's assigned roles and the available roles in separate tree controls.

2. Select a role from the Available Roles tree control and click the left arrow button to add it to the list of assigned roles.
3. On the Role Revisions form, enter an effective date if you want an effective date that is different from today's date.

Today's date is the default value for the Effective Date field. If you do not use the default value, enter a date later than today's date; otherwise the software returns an error message.

4. Enter an expiration date, if one is needed.

The role will not expire if you do not complete the Expiration Date field.

5. Select the Include in ALL* option if you want the role to be one that the user can play if the user enters EnterpriseOne playing all roles, and click OK.

If you do not select the Include in *ALL option, this role will not be part of the active roles when the user enters EnterpriseOne using *ALL as his role at sign-in. To activate a role that is not included in *ALL, the user must select that particular role when signing on to the system. The chosen role will be the only active role during that session.

Choosing Roles for Display at Sign-in

After the administrator has defined roles and created role relationships, users can sign in to EnterpriseOne by using the Role Chooser if this feature is activated. At the EnterpriseOne sign-in form, the user enters a user ID and password. The user must then enter a valid environment and role before entering EnterpriseOne.

User roles and assigned environments are dependent on each other. The user can choose an environment, which then determines what roles appear in the Role Chooser; or the user can choose a role, which determines what environments appear in the Environment Chooser.

This table summarizes the scenarios that can occur when the user encounters the Environment and Role fields at sign-in, and EnterpriseOne behavior in each scenario:

Sign-in Scenario	EnterpriseOne Behavior
User enters values in both the Environment and Role fields.	The software validates the role against the environment. If the role is not valid for the chosen environment, the Environment Chooser appears and the user must choose a valid environment for the role.
User enters a value only in the Role field.	The Environment Chooser displays only the valid environments for the chosen role.
User enters a value only the Environment field.	The Role Chooser displays only the valid roles for the user and the chosen environment.
User does not enter a value in either the Environment field or the Role field.	<p>The Role Chooser appears, containing only the valid roles for the user and the default environment that is defined in the jde.ini file, followed by the Environment Chooser, containing only the valid environments for the chosen role.</p> <p>If you do not enter an environment, the Role Chooser displays the roles that are assigned to the default environment, which is defined in the jde.ini file.</p>

Enabling the Role Chooser

By adding the role to the user's list of assigned roles, the user is able to choose the role at signon by using the Role Chooser. The Role Chooser is a visual assist button on the EnterpriseOne signon screen that displays a user's assigned roles. You can limit the freedom that a user has to choose roles by disabling the Role Chooser. With the Role Chooser disabled, the user must enter EnterpriseOne with all of the assigned roles active.

Note. Users can either choose one role by using the Role Chooser or activate all roles by using *All.

Access the Work With Role Relationships form.

To enable the role chooser:

1. On Work With Role Relationships, from the Form menu, select Enable Role Chooser.
2. On Enable/Disable Role Chooser, select the Enable Roles to be picked option if you want the user to select the new role from a list of all assigned roles at sign-in, and click OK.

If you do not select this option, the user must enter EnterpriseOne playing all assigned roles (*ALL).

Creating Role-to-Role Relationships

The Work With Distribution Lists form lets you create lists of roles that are subsets of another role. For example, you might create an ADMIN role that includes users with the greatest number of administrative responsibilities and the broadest access to applications in EnterpriseOne. You might also create other roles that include individuals with limited administrative responsibilities and access to fewer applications in EnterpriseOne. If you create a distribution list based on roles, you might want to include on the list all roles with some level of administrative responsibility. Anyone in a role that is part of the distribution list would receive messages sent to the ADMIN role.

You use the Work With Distribution Lists form to add or remove roles from the distribution list as needed.

Access the Work With Role Relationships form.

To create role-to-role relationships:

1. From the Form menu, select Distribution Lists.
2. On the Work with Distribution Lists form, complete the Role field and click Find.
3. To add a role to the distribution list, select a role from the Available Roles tree control and click the left-arrow button.
4. On Role Revisions, complete these fields and click OK:
 - Effective date
Enter an effective date if you want the delegation to occur at a date other than the current date.
 - Expiration date
 - Include in *All
Select this option if you want the role to be one that the user can use if the user enters EnterpriseOne playing all roles.
5. Select the *ALL option if you want the role to be one that the user can play if the user enters EnterpriseOne playing all roles.
EnterpriseOne adds the role to the Assigned Roles tree control.
6. To remove a role from the distribution list, select a role from the Assigned Roles tree control and click the right-arrow button.

Note. EnterpriseOne does not currently support multilevel roles.

Revising Role Relationships

After you have created one or more role relationships for a user, you can revise the relationships using the Work With Role Relationships form and the Role Revision form. Role relationships are revised by removing an assigned role or by changing the expiration date for an assigned role. You can also exclude an assigned role from *ALL or add a role to *ALL that was previously excluded.

Access the Work With Role Relationships form.

To revise a role relationship:

1. Complete the User Field and click Find.
2. To remove an assigned role, select a role from the Assigned Roles tree control and click the right-arrow button.
3. To revise an existing role relationship, select a role from the Assigned Roles tree control and click Select.
4. In the Roles Revision form, make changes to either or both of these and click OK:
 - Expiration Date field
 - Include in *ALL option

Delegating Roles

You can delegate the role relationship records to other users by using the Work With Delegation Relationships form. You might want to delegate one or more of the roles to another user if you will be unavailable.

When you delegate the role relationship records, you can copy existing records to another user. You cannot add role relationships to another user unless those roles are already assigned to you.

Access the Work With Role Relationships form.

To delegate roles:

1. From the Form menu, select Roles Delegation.
2. On the Work With Delegation Relationships form, complete the Delegate field by entering the user ID of the user being delegated to and click Find.
 The roles of the user who is delegating appear in the Available Roles tree control. The roles of the user who is being delegated to appear in the Assigned Roles tree control.
3. To delegate a role, select the role from the Available Roles tree control and click the left-arrow button.
4. Complete these fields and click OK:
 - Effective date
 Enter an effective date if you want the delegation to occur at a date other than the current date.
 - Expiration date
5. Select the *ALL option if you want the role to be one that the user can play if the user enters EnterpriseOne playing all roles.
 EnterpriseOne adds the delegated role to the Assigned Roles tree control on the Work With Delegation Relationships form.

Note. You can use the right-arrow button in the Work With Delegation Relationships form only to remove a role that you delegated to another user. If you try to remove a role that you did not delegate to the user, the software will display a dialog box notifying you that the action is invalid.

Adding Roles to a User

The Add Roles to User form enables you to copy one or more role relationship records to a single user, which is a particularly useful action if you want the user to play many roles. You can copy as many records as you want at one time.

Access the Work With Role Relationships form.

To add roles to a user:

1. From the Form menu, select Add Roles to User.
2. Complete the User ID field and click Find.
3. Select the roles that you want to add to the user and click Select.
Hold down the Control key to select more than one role to add.
4. On the Role Revisions form, complete these fields:
 - Effective Date
Enter a date if you want the effective date to be different from the current date.
 - Expiration Date
 - Include in *All
5. Select the *ALL option if you want the role to be one that the user can play if the user enters EnterpriseOne playing all roles.
6. Click OK.
7. If you are adding more than one role relationship record, complete the Role Revisions form for each record that you are adding.

Adding Users to a Role

Access the Work With Role Relationships form.

To add users to a role:

1. Select Add Users to Roles from the Form menu.
2. Complete the Role field and click Find.
3. Select the users that you want to add to a role and click Select.
Hold down the Control key to select more than one user to add.
4. In the Role Revisions form, complete these fields:
 - Effective Date
Enter a date if you want the effective date to be different from the current date.
 - Expiration Date
 - Include in *All
5. Select the *ALL option if you want the role to be one that the user can play if the user enters EnterpriseOne playing all roles.
6. Click OK.
7. If you are adding more than user record, complete the Role Revisions form for each record you are adding.

Copying User Roles

You can copy the role relationship records of one user to another from Role Relationships (P95921). You can either copy and add the records, which means that EnterpriseOne adds the copied records to the user's existing records; or you can copy and replace the records, which means that the copied records replace the user's existing records.

Access the Work With Role Relationships form.

To copy user roles:

1. Complete the User field and click Find.
The user's roles appear in the Assigned Roles tree control.
2. Click Copy.
3. On the Copy User Roles form, select one of these options:
 - Copy and Add
 - Copy and Replace
4. Complete the To User field to specify the user to whom you want the records copied.
5. Click OK.

Adding a Language Translation to a Role

Using the Language Role Description Revisions form, you can either set up the translation of any role that you have defined, or you can change role descriptions for any language.

If you want to view the descriptions of any role in all the languages into which it is being translated, use the Work With Language Role Description form.

Access the Work With User/Role Profiles form.

To add a language translation to a role:

1. On Work With User/Role Profiles, select the Roles Only option.

Note. The Both Users and Roles option also enables you to perform this task.

2. Select a role from the detail area of the grid and select Role Description from the Row menu.
3. To add a language to a role, click Add.
4. On Language Role Description Revisions, complete these fields and click OK:
 - Role
Enter the name of the role to which you want to add a language.
 - Language
Click the visual assist to see a list of the user defined codes for each supported language.
 - Role Description

Changing a Role Description

Access the Work With User / Role Profiles form.

To change a role description:

1. Select the Roles Only option from the Work With User / Role Profiles form.
2. Select a role from the detail area of the grid and from the Row menu, select Role Descriptions.
3. On the Work With Language Role Descriptions form, click Find.
4. Select a role from the detail area of the grid and click Select.
5. On the Language Role Description Revisions form, enter a description in the Role Description field and click OK.

CHAPTER 7

Understanding PeopleSoft EnterpriseOne Security

This chapter provides an overview of PeopleSoft EnterpriseOne security and discusses:

- Users, roles, and *PUBLIC.
- How PeopleSoft EnterpriseOne checks security.
- Cached security information.
- Security types.
- Object-level security.

PeopleSoft EnterpriseOne Security Overview

PeopleSoft EnterpriseOne security enables a security administrator to control security for individual users and for groups of users. The security administrator can control (secure or unsecure) users and groups from these categories:

- Application security
Controls access to or installation of specific applications or application versions.
- Action security
Controls the ability to perform specific actions, such as adding, changing, deleting, selecting, or copying.
- Table row security
Controls access to a specific list or range of records within a table.
- Column security
Controls access to a specific column within a table. PeopleSoft EnterpriseOne represents columns as a field on a form or report. Column security can be set on a table, form, application, or version of an application.
- Processing option security
Controls whether users can view or change the values for processing options, which affects how the associated application or application version works. It also controls whether users are allowed to prompt for versions of that application.
- Tab security
Controls access to tabs on a form.
- Exit security
Controls access to the menu bar exits on forms.
- Exclusive application security

Controls access to secured information using one exclusive application.

- External calls security

Controls access to external call applications.

- Solution Explorer security

Controls access to PeopleSoft Solution Explorer features.

- Miscellaneous security

Controls read-only reports and workflow status monitoring.

- User sign-in and database security

Controls user access to PeopleSoft EnterpriseOne.

- Portal security

Controls access to portal components.

The Security Workbench application (P00950) uses the F00950 table.

The EnterpriseOne Security application (P98OWSEC) uses the F98OWSEC table.

The Security Workbench application is also used to set up security for eight portal features. Setting up security correctly ensures that users in the system have permission to perform only those actions that are essential to the completion of their jobs.

Understanding Users, Roles, and *PUBLIC

The PeopleSoft EnterpriseOne security administrator can set up security for:

- A particular user

This option controls security by specific PeopleSoft EnterpriseOne user ID.

- A user role

This option controls security by role, which enables you to group users based on similar job requirements. An example is putting all of the accounts payable clerks in one role, such as Accounts Payable (AP).

- All users

This option controls security for all users who are designated by ID type **PUBLIC* in the User or Role field. The designation **PUBLIC* is a special ID within PeopleSoft EnterpriseOne that automatically includes all of the users within it. You can use this ID to apply security even if you do not have a specific record set up for it in user profiles.

Understanding How PeopleSoft EnterpriseOne Checks Security

When a user attempts to access an application or perform an action, PeopleSoft EnterpriseOne checks security for that particular user ID. If security exists for that user ID, the software displays a message indicating that the user cannot proceed.

If the user ID has no security, the software checks role profiles (if that user is part of a specific role), and then *PUBLIC for security. If no security is established at any of these levels, the software allows the user to continue.

PeopleSoft EnterpriseOne also provides software license security through protection codes, and it requires user validation at sign-in and when accessing new data sources.

Understanding Cached Security Information

PeopleSoft EnterpriseOne caches security information from the F00950 table in the workstation's memory cache for PeopleSoft EnterpriseOne. If system administrators make changes to this table, those changes are not immediately realized on workstations that are logged on to the system while security revisions are being made. The workstations must sign off and sign back on before the security changes are enabled.

Understanding Security Types

At specific object levels, you can set these levels of security, alone or in any combination, for users and groups:

Level of Security	Description
Application security	Secures users from running or installing, or both, a particular application, an application version, or a form within an application or application version.
Action security	Secures users from performing a particular action, such as adding, deleting, revising, inquiring, or copying a record.
Row security	<p>Secures users from accessing a particular range or list of records in any table.</p> <p>For example, if you secure a user from accessing data about business units 1 through 10, the user cannot view the records that pertain to those business units.</p>
Column security	<p>Secures users from viewing a particular field or changing a value for a particular field in an application or application version. This item can be a database or non-database field that is defined in the data dictionary, such as the work/calculated fields.</p> <p>For example, if you secure a user from viewing the Salary field on the Employee Master application, the Salary field does not appear on the form when the user accesses that application.</p>

Level of Security	Description
Processing option security	<p>Secures users from viewing or changing the values of processing options, or from prompting for versions and prompting for values for specific applications or application versions.</p> <p>For example, if you secure a user from changing the processing options for Address Book Revisions, the user could still view the processing options (if you did not secure the user from prompting for values), but would not be able to change any of the values.</p> <p>If you secure a user from prompting for versions, the user would not be able to see the versions for a specific application, so the user would not be able to choose a different version of an application from the version that the administrator assigned.</p>
Tab security	Secures users from viewing or changing fields in a tab or tabs on a given form.
Exit security	Secures users from menu bar exits on PeopleSoft EnterpriseOne forms. These exits call applications and allow users to manipulate data. Exit security also restricts use of the same menu options.
Exclusive application security	Overrides row security that is set for an application. When you set exclusive application security for a user, the system overrides row security for every table that is accessed by the application that is specified. All other security still applies.
External calls security	Secures users from accessing standalone executables that exist external to PeopleSoft EnterpriseOne. These external executables, which might include design tools, system monitors, and debugging tools, are specific to PeopleSoft EnterpriseOne.
Solution Explorer security	Secures users from accessing or making changes to these PeopleSoft Solution Explorer features: EnterpriseOne Portal, Task Documentation, Fine Cut, Favorites, Solution Explorer, Rough Cut, and Universal Director.
Miscellaneous security	Miscellaneous security controls two separate functions: Read Only reports and Workflow Status monitoring. Read Only reports security denies access to table I/O and business functions, and prevents users from writing to tables. Workflow Status security monitors and controls access to the workflow status.

Understanding Object-Level Security

PeopleSoft EnterpriseOne security is at the object level. This level means that you can secure specific objects within PeopleSoft EnterpriseOne, which provides flexibility and integrity for your security. For example, you can secure a user from a specific form and then, no matter how the user tries to access the form (using a menu or any application that calls that form), the software prevents access to the form. The software simplifies the process of setting up security by allowing you to set security for hundreds of objects at one time by securing all objects on a specific menu or by securing all objects under a specific system code.

Note. Only the objects are secured; the software does not support menu or system code security. Object security provides a higher level of integrity.

For example, if you secured a specific menu to prevent users from accessing the applications on that menu, the users might still be able to access those applications through another menu or another application that accesses the applications that you wanted to secure.

CHAPTER 8

Using Security Workbench

This chapter provides an overview of the items that you can secure using Security Workbench and discusses how to:

- Manage application security.
- Manage action security.
- Manage row security.
- Manage column security.
- Manage processing option security.
- Manage tab security.
- Manage exit security.
- Manage exclusive application security.
- Manage external calls security.
- Manage miscellaneous security.
- Copy security for a user or a role.
- Use alternate methods to delete user or role security.

Understanding Security Workbench

The Security Workbench application (P00950) enables you to apply application, action, and processing option security to users, roles, and *PUBLIC. PeopleSoft EnterpriseOne stores security information in the F00950 table and caches the security information in each workstation's memory. Changes that you make to security as an administrator are applied by each workstation after the user disconnects and signs back in.

You can apply various types of security. For example, you can secure a row in a database table, or you can secure processing options in a PeopleSoft EnterpriseOne application. You can also secure objects within PeopleSoft EnterpriseOne, thus preventing some users from accessing forms or tables, and you can apply object-level security by user.

Managing Application Security

This section provides an overview of application security and discusses how to:

- Review the current application security settings for a user or role.

- Add security to an application.
- Secure a user or role from all PeopleSoft EnterpriseOne objects.
- Change security for an application.
- Remove security from an application.
- Secure users to a form in an application.

Understanding Application Security

Application security enables you to secure these types of items from users:

- Applications

When you secure an application, you secure all versions and forms associated with the application.

- Versions

You can secure access to a version of an application, while leaving other versions available to the user.

- Forms

You can secure access to a single form in an application or application version.

You can secure users from running or installing (or both) a particular application, version, or form within an application.

This section also explains how to add a *ALL object, how to change all of the applications for a particular user or role from unsecured to secured, and how to set security for all but one form in an application.

Forms Used to Manage Application Security

Form Name	Form ID	Navigation	Usage
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Enables you to access the forms that you can use to apply application security.
Application Security	W00950M	On Work With User/Role Security, from the Form menu, select Setup Security, and then select Application.	Review, add, change, or remove application security settings for a user or role.

Reviewing the Current Application Security Settings for a User or Role

Access the Application Security form.

To review the current application security settings for a user or role:

1. On Application Security, enter the user or role ID in the User / Role field.
Enter a complete user or role, which includes *PUBLIC but not wildcards.
2. In the Display Secured Item area, complete the appropriate fields to determine which items have already been secured for the user or role, and then click Find:

- Application

Enter an application name, such as P0101. You can also enter *ALL to display all applications.

- Version

Enter a version name (for example, ZJDEC0001) if you want only to check on a specific version of an application. You can also use an asterisk to display all versions.

- Form Name

Enter a form name, such as W0101G. You can also enter an asterisk to display all forms.

Current security settings for the user or role appear under the Secured node in the tree. Expand the node to view the individual applications and forms that are secured. After you expand the node, the secured applications and forms also appear in the detail area.

Adding Security to an Application

Access the Application Security form.

To add security to an application:

1. On Application Security, enter the user or role ID in the User / Role field.

Enter a complete user or role, which includes *PUBLIC but not wildcards.

2. In the Display UnSecured Items area, complete the appropriate fields and then click Find.

You must perform this step before you can add new security. This step provides a list of applications, versions, and forms from which to select.

- Application

- Version

You can enter a particular version of the application that you entered in the Application field. If you leave this field blank, all versions associated with the application will appear in the UnSecured node.

- Product Code

You can enter a product code to display all applications, versions, and forms associated with a particular product code. This field does not work in conjunction with the Application or Version fields.

The search results appear under the UnSecured node.

3. Expand the UnSecured node to view the individual applications or versions, and the forms associated with each, that do not already have security set for them.

After you expand the node, the individual items also appear in the grid.

4. In the Create with area, select one or both of these options:

- Run Security

Select this option to secure users from running the application.

- Install Security

Select this option for just-in-time installation only.

5. Do one of these:

- Drag applications, versions, or forms from the UnSecured node to the Secured node.
- From the Row menu, select All Objects to move all applications to the Secured node.

- From the Row menu, select Secure to All to move all objects that are beneath the UnSecured node to the Secured node.

If you secured an individual form, only the form appears under the Secured node. If you secured an application or version, the application or version and the forms associated with each appear under the Secured node.

Securing a User or Role from All PeopleSoft EnterpriseOne Objects

Access the Application Security form.

To secure a user or role from all PeopleSoft EnterpriseOne objects:

1. On Application Security, enter the user or role ID in the User / Role field.
Enter a complete user or role, which includes **PUBLIC* but not wildcards.
2. In the Display UnSecured Items area, enter **ALL* in the Application field to select *all* PeopleSoft EnterpriseOne objects, and then click Find.
3. Expand the UnSecured node and then click **ALL* in the detail area.
4. In the Create with area, select one or both of these options:
 - Run Security
Use this option to secure users from running all applications.
 - Install Security
Use this option for just-in-time installation only.
5. Do one of these:
 - Drag **ALL* from the UnSecured node to the Secured node.
 - From the Row menu, select All Objects to move **ALL* to the Secured node.
 - From the Row menu, select Secure to All to move **ALL* from UnSecured node to the Secured node.

Changing Security for an Application

Access the Application Security form.

To change security for an application:

1. On Application Security, under Display Secured Item, select an application, version, or form.
2. Select one or both of these options:
 - Run Security
 - Install Security

Important! Use the Install Security option for just-in-time installation only.

3. From the Row menu, select Revise Security.
In the detail area, the values under the Run and Install fields change accordingly.

Removing Security from an Application

Access the Application Security form.

To remove security from an application:

On Application Security, do one of these:

- Under the Secured node, select an application, version, or form and click Delete.
- Drag an application, version, or form from the Secured node to the UnSecured node.
- On the Row menu, select Remove All to move *all* items from the Secured node to the UnSecured node.

User / Role

The code that identifies a user profile.

Object Name

The name that identifies a system object. PeopleSoft EnterpriseOne architecture is object-based. Discrete software objects are the building blocks for all applications, and developers can reuse the objects in multiple applications. The Object Librarian tracks each object. Examples of system objects include:

- Batch applications (such as reports)
- Interactive applications
- Business views
- Business functions
- Business functions data structures
- Event rules
- Media object data structures

Object Description

A user-defined name or remark.

Security Type

Security Type options are:

- Action Security
Places security to enable or disable users from using specified functions such as Add, Change, Delete, and Copy.
- Application Security
Places security to enable or disable users from viewing or using specified applications or reports.
- Column Security
Places security on specified data fields to be nondisplay or read-only.
- Row Security
Places security to enable or disable users from performing Add, Change, Delete or View actions to records from the database.
- Process Option Security
Places security on viewing or changing the values of processing options, or places security on prompting for versions for specific applications.
- Row/Form Exit

- Tab Exit
- External Calls
- Exclusive Application
- Solution Explorer

Data Item

An identifier that refers to and defines a unit of information. It is a 32-character, alphabetical field that does not allow blanks or special characters such as %, &, or +.

The data item cannot be changed.

It forms the C-code data name (for example AddressNumber) that is used in business functions, data structures, and event rules.

Data items are also identified by the alias or alpha description.

Version / From Value

The From Data value is used by the row security routines to determine a lower range for the data item in the specified table. It is used in conjunction with the Thru Data value to define the range of data that the security applies to.

Thru Value

The Thru Data value is used by the row security routines to determine an upper range for the data item in the specified table. It is used in conjunction with the From Data value to define the range of data that the security applies to.

Alias

A code that identifies and defines a unit of information. It is an alphanumeric code up to 8 characters long that does not allow blanks or special characters such as %, &, or +. You create new data items using system codes 55-59. You cannot change the alias.

Add

This code designates whether a user has the authority to perform an add, either on a specific application or form (action and column security) or for a specific table and data item (row security). This code is set up through Security Workbench by user or group for every table, application, or form requiring security. The **ALL* value can be used to designate all tables or applications.

Change

This code designates whether a user has the authority to perform changes, either on a specific application or form (action, processing option, and column security) or for a specific table and data item (row security). This code is set up through Security Workbench by user or group for every table, application, or form requiring security. The **ALL* value can be used to designate all tables or applications.

Delete

This code designates whether a user has the authority to perform deletes, either on a specific application or form (action security) or for a specific table and data item (row security). This code is set up through Security Workbench by user or group for every table, application, or form requiring security. The **ALL* value can be used to designate all tables or applications.

OK/ Select

This code designates whether a user has the authority to perform operations associated with the OK or Select buttons on a specific application or form (action security).

Copy

This code designates whether a user has the authority to perform operations associated with the Copy button on a specific application or form (action security).

Scroll to End	This code designates whether a user is given the option to scroll to the end of the data selected or only be allowed to view a page at a time. This option is application- or form-specific (action security).
Prompt for Versions	This code designates whether a user will be allowed to prompt for the version of an application to run from a menu selection. This option is application-specific and is set up by the user.
Prompt for Values	This code designates whether an operator has the authority to view records in programs that are using Action Code Security. The code is set up in Action Code Security Revisions (P0003) by user for every program requiring security by action code.
Run	This code designates whether a user has the authority to run a specific application.
Install	This code designates whether a user has authority to perform a Just In Time Install (JITI) for a specific application.
Product Code	A user defined code (98/SY) that identifies a system. Values include: <i>01</i> : Address Book <i>03B</i> : Accounts Receivable <i>04</i> : Accounts Payable <i>09</i> : General Accounting <i>11</i> : Multicurrency

Securing Users to a Form in an Application

You might want to set up security so that only a specified user or group of users can access a single form in an application. These users are otherwise restricted from using the application.

To accomplish this restriction, you create a security record for the form that you want to allow users to access, and then create a security record that prevents users from accessing any other forms in the application.

Access the Work With User/Role Security form.

To secure users to a form in an application:

1. On Work With User/Role Security, enter a user or role ID in the User / Role field and click Find.
2. Select a row displaying *Application Security* in the Description column and click Select.
Alternatively, from the Form menu, select Setup Security, and then select Application.
3. On Application Security, in the Display UnSecured Items area, enter the name of an application in the Application field and click Find.
4. Expand the UnSecured node and any child nodes to see the forms for the application.
5. Click the name of the form that you want users to see, and drag it to the Secured node.

Note. Do not select the Run Security and Install Security options to allow users to see the form.

6. Click Find.
7. Expand the UnSecured Node and select the application you want to secure.

8. Select the Run Security option to prevent users from accessing the application unless they want to run the unsecured form.

Important! Do not select the Install Security option. Doing so will prevent the just-in-time installation (JITI) of anything necessary to run the application.

After you complete these steps, users that you have secured can access only the unsecured form in the application. If a user tries to access a secured form in the application, an error message appears.

Managing Action Security

This section provides an overview of action security and discusses how to:

- Review the current action security settings for a user or role.
- Add action security.
- Change action security.
- Remove action security.

Understanding Action Security

You can secure users from performing a particular action, such as adding, deleting, revising, inquiring, or copying a record.

Forms Used to Manage Action Security

Form Name	Form ID	Navigation	Usage
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Enables you to access the form that you can use to apply action security.
Action Security	W00950M	On Work With User/Role Security, from the Form menu, select Setup Security, and then select Action.	Review current action security settings. Add, change, and remove action security.

Reviewing the Current Action Security Settings for a User or Role

Access the Work With User/Role Security form.

To review the current action security settings for a user or role:

1. On Work With User/Role Security, from the Form menu, select Setup Security and then select Action.
2. On the Action Security form, enter the user or role ID in the User / Role field and click Find.

You can enter **PUBLIC*, but not wildcards.

Current action security settings for the user or role appear under the Secured node in the tree.

3. To see if an action security is applied to a particular application, version, or form, complete a combination of these fields in the Display Secured Item area, and then click Find:

- Application

Enter an application name, such as P0101.

- Version

Enter a version of the application entered in the Application field to see if action security is applied to the version.

- Form Name

Enter a form name, such as W0101G.

Current security settings for the user or role appear under the Secured node in the tree. After expanding the node and clicking a secured item, the system displays which actions are secured for that item in the detail area.

Adding Action Security

Access the Work With User/Role Security form.

To add action security:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Action.
2. On Action Security, enter the user or role ID in the User / Role field and click Find.

You can enter **PUBLIC*, but not wildcards.

Current action security settings for the user or role appear under the Secured node in the tree.

3. To find the applications, versions, or forms to which you want to apply action security, complete any of these fields under the Display UnSecured Items heading, and then click Find:

- Application

Enter an application name, such as P0101. Enter **ALL* to display all applications.

- Version

Enter a version of the application you entered in the Application field. If you leave this field blank, all versions associated with the application will appear in the UnSecured node.

- Product Code

The search results appear under the Unsecured node. Expand the node to view individual applications, versions, and forms. As you expand the node, the individual applications, versions, and forms appear in the detail area.

4. In the Create with area, select any of these options:

- Change
- Add
- Delete
- OK/Select
- Copy
- Scroll To End

5. To secure the actions on an application, version, or form, do one of these:

- Drag the application, version, or form from the Unsecured node to the Secured node.

- From the Row menu, select All Objects to move all items to the Secured node.
- From the Row menu, select Secure to All to move all objects beneath the UnSecured node to the Secured node.

For example, to set delete security on an application, select the Delete option. Next, drag the application from the UnSecured node to the Secured node. The detail area will reflect the delete security that you set for this application, which means that the user whom you entered cannot perform the delete action on this application.

The applications or forms now appear under the Secured node, with the appropriate action security.

Changing Action Security

Access the Work With User/Role Security form.

To change action security:

1. On Work With User/Role Security, from the Form menu, select Setup Security and then select Action.
2. On Action Security, enter the user or role to which you want to change action security in the User / Role field.
3. Under the Secured node, select an application or form for which you want to change action security.
4. In the Create with area, select any of these options:
 - Change
 - Add
 - Delete
 - OK/Select
 - Copy
 - Scroll to End
5. From the Row menu, select Revise Security.

The values under the Add, Change, Delete, OK, Select, Copy, and Scroll to End options in the detail area change accordingly.

Removing Action Security

Access the Work With User/Role Security form.

To remove action security:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Action.
2. On Action Security, enter the user or role for which you want to change action security in the User / Role field, and then click Find.
3. To delete action security from an application, version, or form, do one of these:
 - Under the Secured node, select an application, version, or form and click Delete.
 - Under the Secured node, drag an application, version, or form from the Secured node to the UnSecured node.
 - On the Row menu, select Remove All to move *all* applications and forms from the Secured node to the UnSecured node.

Managing Row Security

This section provides an overview of row security and discusses how to:

- Set up row security.
- Remove row security.

Understanding Row Security

Row security enables you to secure users from accessing a particular range or list of data in any table. Use row security sparingly because it can have an adverse effect on performance. Additional processing occurs for each data item that you set with row security.

You can set up row security at three levels:

- User
- Group
- *PUBLIC

PeopleSoft EnterpriseOne first looks for row security at the user level, then at the group level, and then at the *PUBLIC level. If you set any of the security at a higher level, such as at the user level, the software ignores lower-level security settings, such as at the group or *PUBLIC levels.

Before you set up row security for an item in a table, you should verify that the item is actually in that table. For example, the F0101 table contains the data item AN8. Therefore, you can set up row security on that item. However, the same table does not contain data item PORTNUM. Setting row security on this item for the F0101 table has no effect.

You set up row security on a table, not on a business view. You should verify that the object that you want to secure uses a business view over a table containing the object. For example, the Work With Environments application (P0094) uses business view V00941 over the F00941 table. You could secure the data item RLS (Release) because it is in the F00941 table. On the other hand, the same item is not in the F0094 table. If you attempt to secure the item on the F0094 table, data item RLS is not secured.

Note. You can find the tables, applications, forms, business views, and so on that use a data item by launching the Cross Reference application (P980011) after you build cross-reference tables (F980011 and F980021).

Forms Used to Manage Row Security

Form Name	Form ID	Navigation	Usage
Work With Data Items	W92001B	Data Dictionary Design (GH951), Work With Data Dictionary Items (P92001)	Search for the data item that you want to secure.
Data Item Specifications	W92001C	On Work With Data Items, select the data item that you want to secure and click Select.	Select the Row Security option.
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Select the appropriate menu item to access the form that is used to apply row security.
Row Security Revisions	W00950F	On Work With User/Role Security, from the Form menu, select Setup Security, and then select Row.	Add, change, or remove row security.

Setting Up Row Security

Before you can set up row security, you must activate row security in Data Dictionary Design.

Access the Work With Data Items form.

To set up row security:

1. On Work With Data Items, click Find.

Note. You can enter search criteria in the Search Description field and the QBE row to narrow the search.

2. Select the data item that you want to secure, and click Select.
The Data Item Specifications form appears.
3. On the Item Specifications tab, select the Row Security option and click OK.
This option must be selected for row security to work.
4. Click OK.
5. Exit the data dictionary application.
6. In PeopleSoft Solution Explorer, enter *P00950* in the Fast Path and press Enter.
7. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Row.
8. On the Row Security Revisions form, complete the User / Role field and then click Find to display current row security.
9. Complete these fields, either in the first open detail area row (to add security) or in a pre-existing detail area row (to change security):
 - Table
You can enter **ALL* in this field.
 - Data Item
This field is required.

- From Value
This field is required.
- Thru Value
- Add
- Change
- Delete
- View

10. Click OK to save the security information.

Removing Row Security

Access the Work With User/Role Security form.

To remove row security:

1. On Work With User/Role Security, select an object.
2. From the Form menu, select Setup Security, and then select Row.
3. On the Row Security Revisions form, complete the User / Role field and click Find.

Note. If you accessed the Row Security Revisions form from the Work With User/Role Security form for a specific record, the user or role associated with the security record appears in the User / Role field by default.

4. Select the security record or records in the detail area, and then click Delete.
5. On Confirm Delete, click OK.
6. Click OK when you finish deleting row security.

If you do not click OK after you delete the row security records, the system does not save the deletion.

Managing Column Security

This section provides an overview of column security and discusses how to:

- Set up column security
- Remove column security

Understanding Column Security

This section explains how to add and revise column security. You can secure users from viewing a particular field or changing the value for a particular field. This item can be a database field, or a field that is defined in the data dictionary but is not in the database.

Note. You can find the tables, applications, forms, business views, and so on, that use a data item by launching the Cross Reference application (P980011) after you build the cross-reference tables (F980011 and F980021).

You can set up column security on a table, an application, an application version, or a form. Even if an application uses a business view that does not contain the data item that you want to secure, you can still secure it, as long as the item appears on a form in the application.

Column Security on a Table

Before you set up column security on a table, do these:

- Verify that the object that you want to secure is in the table.
- Verify that the object that you want to secure is part of an application that uses a business view over a table containing the object.
- Verify that the object that you want to secure uses a business view that includes the column containing the object.

For example, if you want to apply column security to data item RLS (Release Number) in the F00941 table, RLS must be an item in that table, and it must also be part of an application using a business view over that table. Finally, the business view over the F00941 table must include a column containing the data item RLS.

If all of these conditions are met, you can successfully apply column security to the data item. Setting column security on a table also means that you set security on the data item for any other applications that use the F00941 table.

Column Security on an Application

Before you set up column security on an application, do these:

- Verify that the object that you want to secure is in the application.
- Verify that you are securing the correct data item in an application (data item descriptions can be similar, if not identical).

For example, if you want to apply column security to data item UGRP (UserRole) in the Object Configuration Manager application (P986110), you first verify that the item is in the application. Because it is in the application, you can apply security to the data item. However, note that data items UGRP, MUSE, USER, and USR0 all contain the identical data description of *User ID*. Verify the item by its alias, not by its data description.

Column Security on an Application Version

You can secure users from using columns (or fields) in a version of an application. When you secure a column in a version, the system secures the column in all forms associated with that application version.

Before you set up column security on an application version, do these:

- Verify that the object that you want to secure is in the version of the application.
- Verify that you secure the correct data item in an application (data item descriptions can be very similar, if not identical). Verify the item by its alias, not by its data description.

Column Security on a Form

Security Workbench enables you to secure the column in one particular form, either in an application or in a version of an application.

Before you set up column security on a form, do these:

- Verify that the object that you want to secure is in the form.

- Verify that you secure the correct data item in the form (data item descriptions can be very similar for different data items).

Forms Used to Manage Column Security

Form Name	Form ID	Navigation	Usage
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Enables you to access the form that you can use to apply column security.
Column Security Revisions	W00950O	On Work With User/Role Security, from the Form menu, select Setup Security, and then select Column.	Add, change, or remove column security.

Setting Up Column Security

Access the Work With User/Role Security form.

To set up column security:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Column.
2. On Column Security Revisions, complete the User / Role field, and then click Find to display current column security for the user or role.
3. To add new security, go to the last row of the detail area and enter information into any of these fields:
 - Table
 - Application
 - Version

If you want to add column security to a particular version, enter a version of the application you entered in the Application field.

- Form Name

You can enter **ALL* in any of these fields; however, after **ALL* is entered for a table, application, or form for a specific data item, you cannot enter **ALL* again for that data item.

4. Complete these fields:
 - Data Item
 - View
 - Add
 - Change
5. To change security, change the row values in the detail area.
6. Click OK to save the security information.

Removing Column Security

Access the Work With User/Role Security form.

To remove security on the Column Security Revisions form:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Column.
2. On the Column Security Revisions form, complete the User / Role field, and then click Find.

Note. If you accessed the Column Security Revisions form from the Work With User/Role Security for a specific record, the user or role associated with the security record appears in the User/Role field by default.

3. Highlight the security record or records in the detail area and click Delete.
4. On Confirm Delete, click OK.
5. Click OK when you finish deleting column security.

If you do not click OK after you delete the security records, the system does not save the deletion.

Managing Processing Option Security

This section provides an overview of processing option security and discusses how to:

- Review the current processing option security settings.
- Add security to processing options.
- Change security for processing options.
- Remove security from processing options.

Understanding Processing Option Security

This section explains how to add, revise, and remove processing option security. You can secure users from changing, prompting for values, and prompting for versions of specific processing options. By itself, setting security that prohibits users from prompting for versions does not prevent them from changing values in the processing option. If you do not want users to use processing option values, you might want to set security so that users are secured from the "prompt for" value and "prompt for" versions.

For example, to set prompt-for-values security, which also automatically sets change security, select the Prompt for Values option. Next, drag one application at a time from the UnSecured node to the Secured node. The detail area reflects the prompt-for-values and change security that you set for these applications. This procedure means that the user whom you entered cannot prompt for values or change processing options on any applications that you dragged to the Secured node.

This task also explains how to add a *ALL object and how to move all of the applications for a particular user or role from unsecured to secured.

Forms Used to Set Up Processing Option Security

Form Name	Form ID	Navigation	Usage
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Enables you to access the form that you can use to apply processing option security.
Processing Option Security	W00950M	On Work With User/Role Security, from the Form menu, select Setup Security, and then select Processing Option.	Add, change, or remove processing option security.

Reviewing the Current Processing Option Security Settings

Access the Work With User/Role Security form.

To review the current processing option security settings:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Processing Option.
2. On the Processing Option Security form, enter a user or role ID in the User / Role field.
Enter a complete user or role, which includes **PUBLIC* but not wildcards.
3. In the Display Secured Item area, complete these fields, and then click Find:
 - Application
Enter an application name, such as P0101. Enter **ALL* to display all applications.
 - Version
Enter a version of the application you entered in the Application field.

Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.

Adding Security to Processing Options

Access the Work With User/Role Security form.

To add security to processing options:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Processing Option.
2. On the Processing Option Security form, enter the user or role ID in the User / Role field and then click Find.
Enter a complete user or role, which includes **PUBLIC* but not wildcards.
3. In the Display UnSecured Items area, complete the appropriate fields and then click Find:
 - Application
Enter an application name, such as P0101. Enter **ALL* to display all applications.

- Version

You can enter a particular version of the application that you entered in the Application field. If you leave this field blank, all versions associated with the application will appear in the UnSecured node.

- Product Code

You must perform this step before you can add new security. This step provides a list of applications from which you can apply processing option security.

The search results appear under the UnSecured node. Expand the node to view applications (interactive and batch) and menus with interactive or batch applications. After you expand the node, the applications appear in the detail area.

For example, to set security on applications within the 00 product code, you would enter *00* in the Product Code field and click Find. All of the applications (interactive and batch) attached to product code 00 would appear after you expand the UnSecured node.

4. Under the Create with heading, select one or more of these options, and then drag applications from the UnSecured node to the Secured node:

- Change

- Prompt for Values

When you select this option, you automatically activate the Change option.

- Prompt for Versions

- Prompt for Data Selection

5. Do one of these:

- Drag applications from the UnSecured node to the Secured node.

- From the Row menu, select All Objects to move all applications to the Secured node.

- From the Row menu, select Secure to All to move all objects beneath the UnSecured node to the Secured node.

The applications now appear under the Secured node with the appropriate security.

Changing Security for Processing Options

Access the Work With User/Role Security form.

To change security for processing options: :

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Processing Option.
2. On the Processing Option Security form, enter the user or role ID to which you want to change processing option security in the User / Role field.

Enter a complete user or role, which includes **PUBLIC* but not wildcards.

3. In the Display Secured Items area, complete the appropriate fields and then click Find:

- Application

Enter an application name, such as P0101. Enter **ALL* to display all applications.

- Version

Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications or application versions. After you expand the node, the items that are secured also appear in the detail area.

4. Under the Secured node, select an application or application version, and select one or more of these options:

- Change
- Prompt for Values

When you select this option, you automatically activate the Change option.

- Prompt for Versions
- Prompt for Data Selection

The values under the Change, Prompt for Data, Prompt for Values, and Prompt for Versions fields in the detail area change accordingly.

5. From the Row menu, select Revise Security.

Removing Security from Processing Options

Access the Work With User/Role Security form.

To remove security from processing options:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Processing Option.
2. On Processing Option Security, enter a user or role ID to which you want to remove processing option security in the User / Role field.

Enter a complete user or role, which includes **PUBLIC* but not wildcards.

3. Click Find.

Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.

4. Do one of these:
 - Under the Secured node, select an application or application version and click Delete.
 - Under the Secured node, drag an application or application version from the Secured node to the UnSecured node.
 - On the Row menu, select Remove All to move *all* items from the Secured node to the UnSecured node.

Managing Tab Security

This section provides an overview of tab security and discusses how to:

- Add security to a tab.
- Change security for a tab.

- Remove security from a tab.

Understanding Tab Security

You can secure users from changing the name of the tab and viewing the form that you call by using the tab. For example, to set up change security, select the Change option. Next, drag tabs one at a time from the UnSecured node to the Secured node. The detail area reflects the change security that you set for the tabs. This security means that the user whom you entered cannot change the tabs that you dragged to the Secured node.

Note. If you secure a user from an application, you cannot also secure the user from certain tabs on a form in that application. This restriction prevents redundant double security. Similarly, if you secure a user from a tab, you cannot secure the user from the application that contains the tab.

Forms Used to Manage Tab Security

Form Name	Form ID	Navigation	Usage
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Enables you to access the form that you can use to apply tab security.
Tab Exit Security	W00950M	On Work With User/Role Security, from the Form menu, select Setup Security, and then select Tab Security.	Add, change, or remove tab security.

Adding Security to a Tab

Access the Work With User/Role Security form.

To add security to a tab:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Tab Security.
2. On Tab Exit Security, complete these fields and click Find:

- User / Role

Enter a complete user or role, which includes **PUBLIC* but not wildcards.

- Application

You can view security for a specific application, or enter **ALL* to display all applications.

Current security settings for the user or role appear under the Secured node in the tree. Expand the nodes to view the secured tabs. After you expand the node, the secured tabs also appear in the grid.

3. Complete *only one* of these fields that appear in the Display UnSecured Items heading and click Find:

- Application

Enter **ALL* in this field to select *all* PeopleSoft EnterpriseOne objects.

In the detail area, this special object appears as **ALL* and displays the security that you defined for the object, such as Run Security or Install Security. The **ALL* object acts as any other object, and you can use the Revise Security and Remove All options from the Row menu.

- Product Code

You must perform this step before you can add new security. This step provides a list of applications from which to select.

The search (application or product code) appears under the UnSecured node. Expand the nodes to view applications (interactive and batch) and the associated tabs. After you expand the node, the applications or tabs also appear in the detail area.

For example, to set security for tabs in applications within the 00 product code, you would enter *00* in the Product Code field and click Find. All of the applications (interactive and batch) attached to product code 00 would appear after you expand the UnSecured node.

4. In the Create with area, select one or more of these options:

- Change

Select this option to prohibit a user or role from changing information on the tab page.

- View

Select this option to hide the tab from the user or the role.

5. Drag tabs from the UnSecured node to the Secured node.

These tabs will now appear under the Secured node.

Changing Security for a Tab

Access the Work With User/Role Security form.

To change security for a tab:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Tab Security.

2. On Tab Exit Security, complete these fields and click Find:

- User / Role

Enter a complete user or role, which includes **PUBLIC* but not wildcards.

- Application

You can view security for a specific application, or enter **ALL* to display all applications.

Current security settings for that user or role appear under the Secured node in the tree. Expand the nodes to view the secured tabs. After you expand the node, the secured tabs also appear in the grid.

3. Under the Secured node, select a tab and select one or more of these options:

- Change

Select this option to prohibit a user or role from changing the name of the tab.

- View

Select this option to hide the tab from the user or the role.

4. From the Row menu, select Revise Security.

The values under the Change and View fields in the detail area change accordingly.

Removing Security from a Tab

Access the Work With User/Role Security form.

To remove security from a tab:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Tab Security.
2. On Tab Exit Security, complete these fields and click Find:
 - User / Role
Enter a complete user or role, which includes **PUBLIC* but not wildcards.
 - Application
You can view security for a specific application, or enter **ALL* to display all applications.
Current security settings for that user or role appear under the Secured node in the tree. Expand the nodes to view the secured tabs. After you expand the node, the secured tabs also appear in the grid.
3. Do one of these:
 - Under the Secured node, select a tab and then click Delete.
 - Under the Secured node, drag a tab from the Secured node to the UnSecured node.
 - On the Row menu, select Remove All to move all tabs from the Secured node to the UnSecured node.

Managing Exit Security

This section provides an overview of exit security and discusses how to:

- Set up exit security.
- Add security to an exit.
- Change security for an exit.
- Remove security from an exit.

Understanding Exit Security

Menu bar exits call applications and allow users to manipulate data. You can secure users from using these exits. Exit security also provides restrictions for menu options.

Forms Used to Manage Exit Security

Form Name	Form ID	Navigation	Usage
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Enables you to access the form that you can use to apply exit security.
Exit Security	W00950M	On Work With User/Role Security, from the Form menu, select Setup Security, and then select Exit Security.	Set up, add, change, or remove exit security.

Setting Up Exit Security

Access the Work With User/Role Security form.

To set up exit security:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Exit Security.
2. Complete these fields and click Find:
 - User / Role
Enter a complete user or role, which includes **PUBLIC* but not wildcards.
 - Application
View security for a specific application. Enter **ALL* to display *all* applications.
Current security settings for the user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as interactive and batch. After you expand the nodes, the secured hyper-button exits also appear in the detail area.
3. In the Display UnSecured Items area, complete only one of these fields and then click Find:
 - Application
You can enter **ALL* in this field.
 - Product Code
You must perform this step before you can add new security. This step provides a list of applications from which to select.
The search results appear under the UnSecured node. Expand the nodes to view applications (interactive and batch) and hyper-button exits. After you expand the nodes, the hyper-button exits also appear in the detail area.
For example, to set security on hyper-buttons in applications within the 00 product code, you would enter *00* in the Product Code field and click Find. All of the applications (interactive and batch) attached to product code 00 would appear after you expand the UnSecured node.
4. Perform the necessary actions to add, change, or remove exit security.

Adding Security to an Exit

Access the Work With User/Role Security form.

To add security to an exit:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Exit Security.
2. Complete these fields and click Find:
 - User / Role
Enter a complete user or role ID, which includes **PUBLIC* but not wildcards.
 - Application
View security for a specific application. Enter **ALL* to display all applications.
Current security settings for the user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as interactive and batch. After you expand the nodes, the secured hyper-button exits also appear in the detail area.
3. Complete only one of these fields in the Display UnSecured Items heading, and click Find:
 - Application
You can enter **ALL* in this field.

- Product Code

You must perform this step before you can add new security. This step provides a list of applications from which to select.

The search (application, product code, or menu) appears under the UnSecured node. Expand the nodes to view applications (interactive and batch) and hyper-button exits. After you expand the nodes, the hyper-button exits also appear in the detail area.

For example, to set security on hyper-buttons in applications within the 00 product code, you would enter 00 in the Product Code field and click Find. All of the applications (interactive and batch) attached to product code 00 would appear after you expand the UnSecured node.

4. In the Create with area, select the Run Security option.
5. Drag exits one at a time from the UnSecured node to the Secured node.

The exits that you dragged now appear under the Secured node. The grid reflects the security that you set for these exits. This security means that the user that you entered cannot use the exit.

Changing Security for an Exit

Access the Work With User/Role Security form.

To change security for an exit:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Exit Security.
2. Complete these fields and click Find:

- User / Role

Enter a complete user or Role ID, which includes **PUBLIC* but not wildcards.

- Application

View security for a specific application. Enter **ALL* to display *all* applications.

Current security settings for the user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as interactive and batch. After you expand the nodes, the secured hyper-button exits also appear in the detail area.

3. Under the Secured node, select an exit and select the Run Security option.
4. From the Row menu, select Revise Security.

The values under the Run field in the detail area change accordingly.

Removing Security from an Exit

Access the Work With User/Role Security form.

To remove security from an exit:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Exit Security.
2. Complete these fields and click Find:

- User / Role

Enter a complete user or role ID, which includes **PUBLIC* but not wildcards.

- Application

View security for a specific application. Enter **ALL* to display *all* applications.

Current security settings for the user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as interactive and batch. After you expand the nodes, the secured hyper-button exits also appear in the detail area.

3. Do one of these:

- Under the Secured node, select an exit, and click Delete.
- Under the Secured node, drag an exit from the Secured node to the UnSecured node.
- On the Row menu, select Remove All to move all exits from the Secured node to the UnSecured node.

Managing Exclusive Application Security

This section provides an overview of exclusive application security and discusses how to:

- Add access with exclusive application security.
- Remove exclusive application security.

Understanding Exclusive Application Security

Exclusive application security enables you to grant access to otherwise secured information through one exclusive application. For example, assume that you use row security to secure a user from seeing a range of salary information; however, the user needs to run a report for payroll that includes that salary information. You can grant access to the report, including the salary information, using exclusive application security. PeopleSoft EnterpriseOne continues to secure the user from all other applications in which that salary information might appear.

Forms Used to Manage Exclusive Application Security

Form Name	Form ID	Navigation	Usage
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Enables you to access the form that you can use to apply exclusive application security.
Exclusive Application Security	W00950B	On Work With User/Role Security, from the Form menu, select Setup Security, and then select Exclusive Application.	Add or remove exclusive application access.

Adding Access with Exclusive Application Security

Access the Work With User/Role Security form.

To add access with exclusive application security:

1. On Work With User/Role Security, from the Form menu, select Setup Security and then select Exclusive Application.
2. On Exclusive Application Security, complete the User / Role field.
Enter a complete user or role, which includes **PUBLIC* but not wildcards.
3. Complete these fields in the detail area:
 - Object Name
Enter the name of the exclusive application for which you want to allow access (the security). For example, to change the security for a user of the Vocabulary Overrides application, enter *P9220* in this field.
 - Run Application
4. Click OK to save the information.

Removing Exclusive Application Access

Access the Work With User/Role Security form.

To remove access on the Exclusive Application Security form:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select Exclusive Application.
2. On Exclusive Application Security, complete the User / Role field and click Find:

Note. If you accessed the Exclusive Application Security form from the Work With User/Role Security for a specific record, the user or role associated with the security record appears in the User/Role field by default.

3. Highlight the security records in the grid and click Delete.
4. On Confirm Delete, click OK.
5. Click OK when you finish deleting exclusive application security.

If you do not click OK after you delete the security records, PeopleSoft EnterpriseOne does not save the deletion.

Managing External Calls Security

This section provides an overview of external call security and discusses how to:

- Set up security for external calls.
- Add external call security.
- Change external call security.
- Remove external call security.

Understanding External Call Security

This section discusses how to secure users and roles from access to external call applications. In PeopleSoft EnterpriseOne, certain applications exist that are not internal to PeopleSoft EnterpriseOne; they are standalone executables. For example, the Report Design Aid, which resides on the Cross Application Development Tools menu (GH902), is a standalone application. You can also call this application externally using the RDA.exe. By default, this file resides in the \E810\SYSTEM\Bin32 directory.

Forms Used to Manage External Call Security

Form Name	Form ID	Navigation	Usage
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Enables you to access the form that you can use to apply external calls security.
External Calls	W00950C	On Work With User/Role Security, from the Form menu, select Setup Security, and then select External Calls.	Set up and remove security for external calls.

Setting Up Security for External Calls

Access the Work With User/Role Security form.

To set up security for external calls:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select External Calls.
2. Complete these fields and click Find:
 - User / Role
Enter a complete user or role, which includes **PUBLIC* but not wildcards.
 - Display Secured Item
 - Executable
Enter the name of a secured executable, such as *debugger.exe*. When you enter information into this field, the system searches only for the indicated executable.
 - Display Unsecured Items
 - Executable
Enter the name of an unsecured executable.
Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as *debugger.exe*.
3. Add, change, or remove security for external calls.

Adding External Call Security

Access the Work With User/Role Security form.

To add external call security:

1. On Work With User/Role Security, from the Form menu, select Setup Security, and then select External Calls.
2. Complete these fields, and click Find:
 - User / Role
Enter a complete user or group ID, which includes **PUBLIC* but not wildcards.
 - Executable
Enter the name of the external application, such as *debugger.exe*. When you enter information into this field, the software searches only for the indicated application.

Current security settings for that user or group appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as debugger.exe.
3. In the Create with area, select the Run Security option.
4. Do one of these:
 - Drag applications from the UnSecured node to the Secured node.
 - To move all applications to the Secured node, select All Objects from the Row menu.
The external call applications now appear under the Secured node with the appropriate security.
For example, to set run security on the Business Function Design application, select the Run Security option and then drag the Business Function Design node from the UnSecured node to the Secured node. The detail area reflects the run security that you set for this application, which would mean that the user whom you entered could *not* run the Business Function Design application.

Changing External Call Security

Access the Work with User/Group Security form.

To change external call security:

1. On Work with User/Group Security, from the Form menu, select Setup Security, and then select External Calls.
2. Complete these fields, and click Find:
 - User / Role
Enter a complete user or group ID, which includes **PUBLIC* but not wildcards.
 - Executable
Enter the name of the external application, such as *debugger.exe*. When you enter information into this field, the software searches only for the indicated application.

Current security settings for that user or group appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as debugger.exe.
3. Under the Secured node, select an application, and then select the Run Security option.
4. From the Row menu, select Revise Security.
The values for the Run field in the detail area change accordingly.

Removing External Call Security

Access the Work with User/Group Security form.

To remove external call security:

1. On Work with User/Group Security, from the Form menu, select Setup Security, and then select External Calls.
2. On External Calls Security, complete these fields and click Find:
 - User / Role
Enter a complete user or group ID, which includes **PUBLIC* but not wildcards.
 - Executable
Enter the name of the external application, such as *debugger.exe*. When you enter information into this field, the software searches only for the indicated application.

Current security settings for that user or group appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as debugger.exe.
3. Do one of these:
 - Under the Secured node, select an application and click Delete.
 - Under the Secured node, drag an application from the Secured node to the UnSecured node.
 - On the Row menu, select Remove All to move *all* applications from the Secured node to the UnSecured node.

Managing Miscellaneous Security

This section provides an overview of miscellaneous security and discusses how to manage miscellaneous security features.

Understanding Miscellaneous Security

PeopleSoft EnterpriseOne security enables you to secure users and roles from:

- Read/Write Reports
- Workflow Status Monitoring

Read/Write Reports Security

PeopleSoft EnterpriseOne enables administrators to prevent specific users and roles from running reports that update PeopleSoft EnterpriseOne database tables (read/write reports). Administrators can assign users to a user profile called No Update Report Creation User (NUR), which restricts users to running only Read Only reports. When an NUR user runs a report, PeopleSoft EnterpriseOne prevents the report from making table I/O calls to databases that can affect business data. Users assigned to this profile can create and run read-only reports, but are restricted from creating or running existing UR reports. NUR users can copy existing UR reports and run the copied report, although the software disables the report's ability to change business data and displays a warning that the copied report is non-updateable. NUR users can edit NUR reports in RDA, but are prevented from even opening existing UR reports in RDA.

Workflow Status Monitoring Security

Users can access Workflow Modeler, (a scaled-down version of Process Modeler) to design PeopleSoft EnterpriseOne workflow models. Process Modeler Server includes a PeopleSoft EnterpriseOne Portal-based component called Model Viewer, which enables users with appropriate access to monitor the status of a workflow and perform workflow administration tasks directly from the Viewer.

Miscellaneous security includes these Workflow Status Monitoring settings, which determine the operations a user can perform from the Model Viewer:

- **Secured**
Restricts users from accessing any Model Viewer tasks using the Portal.
- **Partial**
Allows users to view workflow models and monitor their status, but restricts these users from performing any administrative tasks.
- **Full**
Allows users access to all Model Viewer tasks using the PeopleSoft EnterpriseOne Collaborative Portal. Users can view workflow statuses and perform administrative tasks.

Forms Used to Manage Miscellaneous Security

Form Name	Form ID	Navigation	Usage
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Enables you to access the form that you can use to apply miscellaneous security.
Miscellaneous Security Revisions	W00950R	On Work With User/Role Security, select Setup Security, and then select Misc Security.	Manage miscellaneous security features.

Managing Miscellaneous Security Features

Access the Work With User/Role Security form.

To manage miscellaneous security features:

1. On Work With User/Role Security, select Setup Security from the Form menu, and then select Misc Security.
2. Complete the User / Role field and click Find.
Enter a complete user or role, which includes **PUBLIC* but not wildcards.
3. To change Read-Only Report security, select one of these options:
 - Read / Write
 - Read Only
4. To change Workflow Status Monitoring security, select one of these options:
 - Secured
Prevents users from viewing or administering workflow.

- View
Allows users to view workflow but prevents them from making changes.
 - Full
Allows users to view and administer workflow.
5. Click OK to accept the changes.

Copying Security for a User or a Role

This section provides an overview of copying security and discusses how to:

- Copy all security records for a user or a role.
- Copy a single security record for a user or a role.

Understanding How to Copy Security for a User or a Role

You can copy the security information for one user or role, and then use this information for another user or role. When you copy security, you can either overwrite the current security for the user or role, or you can add the new security information to the existing security information. You can also copy all of the security records for a user or role, or you can copy one security record at a time for a user or role.

Forms Used to Copy Security

Form Name	Form ID	Navigation	Usage
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in Fast Path.	Enables you to access the form that you can use to copy security for a user or a role.
Copy Security	W00950D	On Work With User/Role Security form, from the Form menu, select Copy Security.	Copy a single security record or all security records.

Copying All Security Records for a User or a Role

Access the Work With User/Role Security form.

To copy all security records for a user or a role:

1. On Work With User/Role Security, select Copy Security from the Form menu.
2. Select one of these options:
 - Copy and Add
When you copy and add security settings, you do not overwrite preexisting security for user or role.
 - Copy and Replace
When you copy and replace security settings, the software deletes the security information for a user or role, and then copies the new security information from the selected user or role.

3. Complete these fields and click OK:

- From User / Role
- To User / Role

The system saves the security information and returns you to the Work With User/Role Security form.

Copying a Single Security Record for a User or a Role

Access the Work With User/Role Security form.

To copy a single security record for a user or a role:

1. On Work With User/Role Security, locate a security record.
2. Select the security record row that you want to copy, and then click Copy.
3. Complete the To User / Role field and click OK.

The system saves the security information and returns you to the Work With User/Role Security form.

Using Alternate Methods to Delete User or Role Security

This section provides an overview of alternate ways of deleting user security and discusses how to:

- Delete user or role security.
- Delete security on the Work With User/Role Security form.

Understanding Alternate Methods of Deleting User or Role Security

In addition to deleting security records on the forms that are specific to the security type, such as application, row, or external calls, you can delete security records on the Work With User/Role Security form.

Form Used to Delete User or Role Security

Form Name	Form ID	Navigation	Usage
Work With User Security	W00950A	Security Maintenance (GH9052), User Security (P98OWSEC)	Find the user or role, and then select the appropriate record in the tree structure to delete.

Deleting User or Role Security

Access the Work With User Security form.

To delete user security:

1. On the Work With User Security form, find the user or role, select the appropriate record in the tree structure, and then click Delete.

Note. If you select a record from the detail area and click Delete, you will remove the data source for the user but not remove user security.

2. Click OK to delete all user security records for the user or role.

Deleting Security on the Work With User/Role Security Form

To delete security on the Work With User/Role Security form:

1. On Work With User/Role Security, click Find, select a record in the grid, and then click Delete.

Note. Enter search criteria in the query by example line to narrow the search.

2. On Confirm Delete, click OK.

Security Workbench deletes the security record and refreshes the grid.

CHAPTER 9

Setting Up Address Book Data Security

This chapter provides an overview of Address Book data security and discusses how to:

- Set up permission list definitions.
- Set up permission list relationships.

Understanding Address Book Data Security

The Address Book data security feature enables you to restrict users from viewing address book information that you have determined is personal. After performing the required setup for this feature, secured users can see the fields that you specify as secured, but the fields are filled with asterisks and are disabled. You can set up data security for these fields:

- Tax ID
- Addl Ind Tax ID (Additional Tax ID)
- Address
Includes Address Lines 1–7, City, State, Postal Code, Country, County
- Phone Number
Includes Phone Number and Phone Prefix
- Electronic Address
Includes only electronic addresses with Type E.
- Day of Birth, Month of Birth, and Year of Birth
- Gender

Note. In addition to these fields, the system enables you to designate up to eight other user-defined fields as secured. Included in the eight fields are: five string, one math numeric, one character, and one date type. To secure additional fields, you must modify the parameter list in the call to the business function B0100095. For example, if you want to designate Industry Class as a secured field, you must modify the call to the B0100095 business function to map Industry Class in the parameter list.

The Address Book data security feature provides an additional level of security by not allowing secured users to locate valid personal information using the query based example (QBE) line. For example, if a user enters numbers in the Tax ID field in the QBE line, the system does not display the matching record in the event that the user happens to enter a valid tax ID number.

Setting up Address Book data security involves these steps:

1. Selecting the Activate Personal Data Security constant in the Address Book Constants.

Personal data security is inactive unless the Activate Personal Data Security constant is selected.

2. Setting up permission list definitions.

Use the Permission List Definitions program (P01138) to create one or more permission lists that specify which fields in the Address Book are secured.

3. Setting up permission list relationships.

Use the Permission List Relationships program (P95922) to determine the users or roles that are subject to each permission list.

Once you have set up Address Book data security, keep in mind that users can still view their own address book information, and secured fields are not protected under these circumstances:

- Adding new Address Book records.
- Running reports that contain the secured fields.
- Viewing records in the Universal Table Browser (UTB).

You can set up data security for any other system within EnterpriseOne. To use the data security feature for another system, you must create new programs and related tables for permission list definitions.

Prerequisites

Select the Activate Personal Data Security constant in the Address Book Constants.

See Setting Up the Address Book System in the PeopleSoft EnterpriseOne Address Book 8.11 PeopleBook.

Set up users and roles in the User Profiles program (P0092) for each user that you want to secure from Address Book information.

See [Chapter 6, “Working with User Profiles,” Setting Up User Profiles, page 80](#).

Setting Up Permission List Definitions

This section provides an overview of permission list definitions and discusses how to set up permission list definitions.

Understanding Permission List Definitions

The Permission List Definition program enables you to create multiple lists that determine which Address Book fields are secure. When you create permission lists, you specify a permission list name and a search type, and then select each field that you want to secure. The system stores permission list definitions in the F01138 table.

Forms Used to Set Up Permission List Definitions

Form Name	Form ID	Navigation	Usage
Work With Permission List Definitions	W01138A	Permission List Management (JDE029160), Address Book Data Permissions	Review existing permission list definitions.
Add/Edit Permission List Definitions	W01138B	Select Add from the Work With Permission List Definitions form.	Create new permission list definitions or revise existing definitions.

Creating Permission List Definitions

Access the Add/Edit Permission List Definitions form.

Add/Edit Permission List Definitions form.

After entering the Permission List Name and the Search Type, select each field that you want to secure.

Permission List Name Enter a name for the permission list. Enter up to 15 alphanumeric characters.

Search Type Select the search type for which the permission list applies.

Setting Up Permission List Relationships

This section provides an overview of permission list relationships and discusses how to set up permission list relationships.

Understanding Permission List Relationships

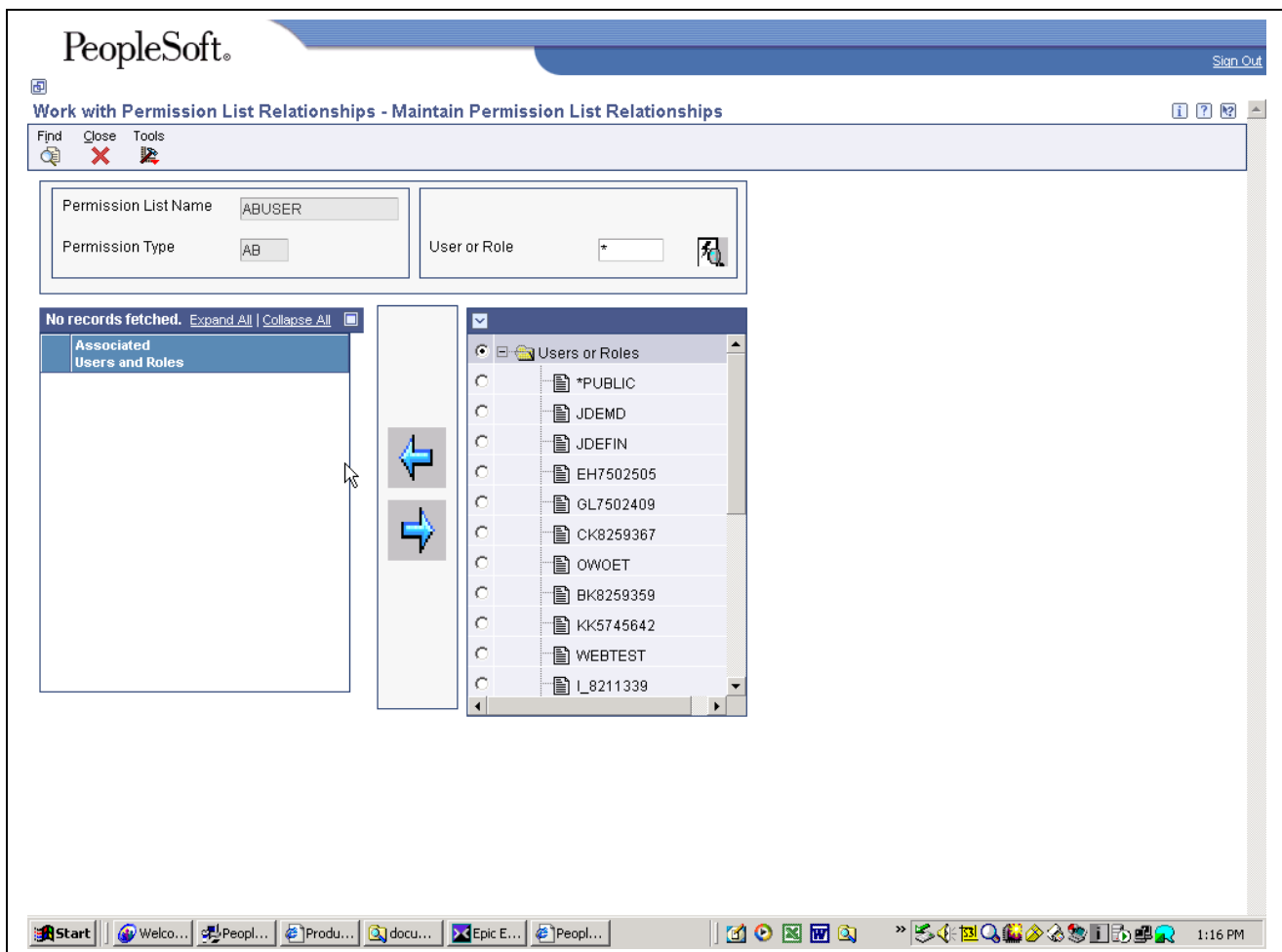
After you have set up permission list definitions, use the Permission List Relationships program to assign them to previously defined user IDs and roles. You can attach a user ID or role to only one permission list. The system stores permission list relationships in the F95922 table.

Forms Used to Create Permission List Relationships

Form Name	Form ID	Navigation	Usage
Work With Permission List Relationships	W95922A	Permission List Management (JDE029160), Work With Permission List Relationships	Search for a permission list.
Maintain Permission List Relationships	W95922D	Click Select on Work With Permission List Relationships.	Set up permission list relationships.

Creating Permission List Relationships

Access the Maintain Permission List Relationships form.



Maintain Permission List Relationships

User or Role

Enter the User ID or Role that you want to attach to a permission list.



Click the Find.gif button after entering a value in the User or Role field.



Click the right_arrow.gif button to attach a User ID or Role to a permission list.



Click the left_arrow.gif button to remove a User ID or Role from a permission list.

CHAPTER 10

Setting Up Business Unit Security

This chapter provides an overview of business unit security and discusses:

- Working with UDC sharing.
- Working with transaction security.

Business Unit Security Overview

EnterpriseOne business unit security provides the ability to filter data by business unit for user defined codes (UDCs) and for transaction tables. For UDCs, you create subgroups of values that can be shared among various business units or may be unique to one particular business unit. This is referred to as UDC sharing. For transaction tables, business unit security enables you to limit the transaction records that a user has access to based on business unit. This is called transaction security.

UDC Sharing

With UDC sharing, PeopleSoft EnterpriseOne provides the ability to control, or regulate, how organizational data among different business units is shared. UDC sharing enables you to define a subset of UDC values for a business unit. You can share multiple UDC values among multiple business units.

For example, a company's customer service department may provide support for appliances, consumer electronics, and sporting goods. Typically, a representative would choose from an extensive list of values to specify the repair code for a particular type of product. However, with UDC sharing, the company can associate a subset of the repair code UDC values, such as for appliances, to a business unit. As a result, the representatives associated with the business unit would only have to choose from a list of repair codes relevant to appliances.

Transaction Security

Another feature of EnterpriseOne business unit security is transaction security. Transaction security enables you to determine the transaction records a user can view. Transaction security ensures that users can only access and modify transaction data for the business unit to which they are associated.

See Also

Setting Up Business Units in the PeopleSoft EnterpriseOne Financial Management Solutions Application Fundamentals 8.11 PeopleBook.

Working with UDC Sharing

This section discusses how to:

- Set up UDC sharing.
- Set up business unit security for UDC sharing.
- Revise a UDC group.

Setting Up UDC Sharing

EnterpriseOne provides a wizard-like program to assist with setting up UDC sharing. The program leads you through the appropriate tasks to configure these items:

- UDC group

A UDC group serves as a container for the UDC values that you want to share among different business units. You create the UDC group by naming it and assigning the UDC types that contain UDC values. For example, if you are sharing UDC values that represent various states and countries in geographic regions, you might name the UDC group GEO, and then assign the UDC types that contain the appropriate UDC values for the states or countries.

- Set-ID

A set-ID allows you to further categorize the UDC values within a UDC group. For example, you can further categorize the UDC values in the GEO UDC group into subsets, such as Europe, Canada, Pacific Rim, and so forth. Each subset, or set-ID, can contain values that are specific to that region.

In PeopleSoft Solution Explorer, enter GH9052 in the Fast Path, select Business Unit Security, and then select Set-up UDC Sharing to access the UDC Group Revisions form.

To set up UDC sharing:

1. On UDC Group Revisions, complete these fields to name and describe the UDC group:
 - UDC Group
 - Group Description
2. In the detail area, click the search button in these fields to add UDC types to the UDC group:
 - Product Code
Choose the product code of the UDC type that you want to add.
 - User Defined Code
Choose the UDC type that contains the values for the UDC group.

Note. A UDC type cannot be associated with more than one UDC group.

3. Click Next.
4. On Set-ID Definition Revisions, complete these fields to create set-IDs for the UDC group:
 - Set-ID
Enter a name for the set-ID.
 - Description

5. Click Next. On Maintain Set-ID, the system displays the UDC types that you assigned to the UDC group in the right pane. The left pane contains the set-IDs that you defined for the UDC group.
6. Assign UDC values to the Set-IDs.
 - a. Choose a set-ID in the left pane.
 - b. Click a UDC type in the right pane, and then choose from the list of UDC values.
 - c. Click the left arrow to assign the UDC value to the chosen Set-ID.
7. After you assign UDC values to the set-IDs, click Done.

Setting Up Business Unit Security for UDC Sharing

EnterpriseOne provides a wizard-like program to assist you with setting up business unit security for UDC sharing. The program leads you through these tasks:

- Define a business unit type.

A business unit type serves as a logical grouping of business units. To define it, you give it a name and then specify the table (typically the F0006 table) and the data item within the table that contains the business unit values.

- Associate a user ID or role to a business unit.

Note. You can associate users to business units when setting up UDC sharing or when setting up transaction security.

- Associate a UDC group to a business unit.

In PeopleSoft Solution Explorer, enter GH9052 in the Fast Path, double-click Business Unit Security, and then select Set-up Business Unit Security to access the Business Unit Security Definition Revisions form.

To set up business unit security for UDC sharing:

1. On Business Unit Security Definition Revisions, complete these fields in order:
 - Business Unit Type
 - Business Unit Definition Table
Enter the table object name that contains the individual business unit values (for example, F0006).
 - Business Unit Definition Data Item
Enter the data item in the Business Unit Definition Table that contains the unique business unit name (for example, MCU).
2. Press Tab and then click Next to continue.
3. On User/Role to Business Unit Relationships, assign the users or roles in the right panel to the appropriate business units in the left panel. You can search for particular business unit values and users or roles by clicking the search button next to the Business Unit Value and User/Role fields respectively.

Note. You can click the Skip button if you choose not to perform this step here. You can also assign users to business units when setting up transaction security.

4. After securing users to the appropriate business units, click Next to continue.
5. On Maintain Transaction Security Tables, click the Skip button. This form is only used for transaction security.

6. On UDC Group/Set-ID/Business Unit Relationship, assign the set-IDs within the UDC groups to the appropriate business units in the left panel. You can search for particular business unit values and UDC groups by clicking the search button next to the Business Unit Value and UDC Group fields respectively.

Remember that you must first configure UDC sharing to be able to assign set-IDs to business units on this form.

7. Click Done.

Revising UDC Groups

In PeopleSoft Solution Explorer, enter GH9052 in the Fast Path, double-click Business Unit Security, and then select Maintain UDC Sharing to access the Work With UDC Sharing form.

To revise a UDC group:

1. On Work With UDC Sharing, select the UDC group that you want to revise.
2. To add or delete a UDC type in a UDC group, from the Row menu, select Group Revisions.
3. To add or delete a set-ID, from the Row menu, select Set-ID Definition.

Note. You cannot delete a set-ID that is part of a business unit and UDC group relationship.

4. To revise the UDC values that are assigned to the set-IDs, from the Row menu, select Maintain Set-ID.

To delete a UDC group:

On Work With UDC Sharing, select the UDC group and then click Delete.

Note. You cannot delete a UDC group that is part of a business unit relationship.

Working with Transaction Security

This section provides an overview of how to set up transaction security and discusses how to:

- Set up transaction security.
- Revise transaction security.

Understanding How to Set Up Transaction Security

Transaction security enables you to define which transaction records a user can access, based on the business unit(s) they are associated with. Transaction security for business units is inclusive, which means that you define which transactions users can access based on the business unit to which the user ID or role is associated. To set up transaction security, you must define these items:

- Business unit type.

A business unit type serves as a logical grouping of business units. To define it, you give it a name and then specify the table (typically the F0006 table) and the data item within the table that contains the business unit values.

Note. If you are setting up transaction security for an existing business unit type, use the Maintain Business Unit Security menu to add transaction security.

- Tables that are to be included in a transaction security definition.
- Users associated with the business units.

Setting Up Transaction Security

In PeopleSoft Solution Explorer, enter GH9052 in the Fast Path, double-click Business Unit Security, and then select Set-up Business Unit Security to access the Business Unit Security Definition Revisions form.

To set up transaction security:

1. On Business Unit Security Definition Revisions, complete these fields in order:
 - Business Unit Type
 - Business Unit Definition Table
Enter the table object name that contains the individual business unit values (for example, F0006).
 - Business Unit Definition Data Item
Enter the data item in the Business Unit Definition Table that contains the unique business unit name (for example, MCU).
2. Press Tab and then click Next to continue.
3. On User/Role to Business Unit Relationships, assign the users or roles in the right panel to the appropriate business units in the left panel. You can search for particular business unit values and users or roles by clicking the search button next to the Business Unit Value and User/Role fields respectively.
4. After securing users to the appropriate business units, click Next to continue.
5. On Maintain Transaction Security Tables, complete these columns in the grid:
 - Transaction table
Enter the table name that contains the data item that you want to secure.
 - Data item
Enter the data item of the column that you want to secure.
You can use this form to secure multiple tables.
 - Click Next to continue.
 - On UDC Group/Set-ID/Business Unit Relationship, click Done.

Revising Transaction Security

In PeopleSoft Solution Explorer, enter GH9052 in the Fast Path, double-click Business Unit Security, and then select Maintain Business Unit Security to access the Work With Business Unit Security form.

To revise transaction security:

1. On Work With Business Unit Security, select the business unit security type record that you want to revise.
2. To revise the users or roles associated to a business unit, from the Row menu, select Associate User/Role.
3. To revise the UDC values that are assigned to business units, from the Row menu, select UDC Groups for BU.
4. To revise a transaction table record, from the Row menu, select Transaction Tables.
5. To delete transaction security for a business unit type, select the record and then click Delete.

To delete transaction security:

On Work With Business Unit Security, select the business unit security type record that you want to delete, and then click Delete.

CHAPTER 11

Employing Sign-in Security

This chapter provides an overview of sign-in security and discusses:

- Security table access.
- Password encryption.
- Security setup.
- Process flow for sign-in security.
- Sign-in security for web users.

Understanding Sign-in Security

PeopleSoft EnterpriseOne security runs on a logic server in a dedicated internal process. You create a security table on the data server that stores information, such as:

Value	Description
EnterpriseOne User	The user ID used to sign in to PeopleSoft EnterpriseOne.
EnterpriseOne Password	The user's password, which the software validates when the user signs in to PeopleSoft EnterpriseOne.
System User and System Password	The actual user and password used to connect to all database management systems (DBMS). If the PeopleSoft EnterpriseOne environment includes more than one DBMS, you can create different system users and passwords for each data source.
Change Frequency	The frequency of password changes required by the software.
Last Change	The date that the password was last changed.

You must define a security record for each user either by group or by individual. It is recommended that you map multiple users to the same system user. For example, each user can use the same system user that the software uses to connect to PeopleSoft EnterpriseOne database management systems. By setting up the security in this manner, you can simplify database administration of users and passwords.

You can also set up unified logon with PeopleSoft EnterpriseOne to simplify sign-in security. When you set up unified logon, PeopleSoft EnterpriseOne uses Windows Authentication to verify security. This verification allows sign-in security to use the network logon information that a user supplies when logging on to Windows; PeopleSoft EnterpriseOne does not require the user to enter another user ID and password when signing in.

Security Table Access

If you keep the system user and password secure, no users have direct access to the Security table (F98OWSEC). The exception to this situation is for system administrators who maintain the security information. The PeopleSoft EnterpriseOne security server has access to the F98OWSEC table through JDENet.

You must perform all of the validation and changes of PeopleSoft EnterpriseOne passwords through a JDENet message to the enterprise server with the F98OWSEC table. Upon validating a PeopleSoft EnterpriseOne password, the JdeNet message returns the system user and password that you enter. These words are encrypted across the network. Internally, this system password is used for all connections to databases.

Using the database management system, you should place database security on the F98OWSEC table. You should also assign PeopleSoft EnterpriseOne object security to the F98OWSEC table so that users cannot access the object except to enter User Password Revisions (W98OWSECD).

See Also

[Chapter 12, “Setting Up User Security,” page 167](#)

Password Encryption

You can enter the initial sign-in password for each user in these ways:

- Type it manually.
- Use a default password established through the sign-in security processing options.
- Have PeopleSoft EnterpriseOne enter it automatically because the user has an existing security record.

When typing a password manually or when using the processing option default password, you cannot see the password for a new user because you are typing it in. When you revise this record, however, the system encrypts the password so that all you see are asterisks. The number of asterisks does not represent the number of characters in the password. The user security application does not know what the password is. The application is given a flag that indicates that a password was entered. The system stores the actual password on the security server within a binary object in the F98OWSEC table. The system accesses the binary object when the user security application requests a change or inquiry.

Security Setup

This checklist is an overview of the steps that are required to set up security:

Determine location of the F98OWSEC table.	<p>Ensure that the F98OWSEC table is located in the system data source on the enterprise server, and ensure that the table is mapped to the correct data source through the Object Configuration Manager.</p> <p>If your system data source resides on the enterprise server, the F98OWSEC table should reside in the system data source. However, if the system data source is located on the deployment server (or other servers), the F98OWSEC table should be moved to the server map data source for the enterprise server.</p> <p>If you have more than one logic server, you should use only one as the security server.</p>
Set database security on the F98OWSEC table.	From within the DBMS, place database security on this table to prevent a user from accessing the object, except to enter passwords through User Password Revisions.

Place security on the logic server's jde.ini file.	The DBMS user ID and password to the Sign On Security table are stored in this file.
Create security records for individual users.	<p>Assign these:</p> <ul style="list-style-type: none"> • Data source • System user • System password • EnterpriseOne password • User Status • Allowed number of invalid sign-on attempts (optional) • Change frequency (optional) <hr/> <p>Note. If you intend to use a unified logon, every user in the PeopleSoft EnterpriseOne security database requires a unique user ID.</p> <hr/>
Verify and modify the jde.ini file on the PeopleSoft EnterpriseOne logic server for the platform environment.	If you use a unified logon, you need to change the settings for a unified logon in the [SECURITY] section as well as in the PeopleSoft EnterpriseOne [SECURITY] settings.
Set up a unified logon server.	<p>If you use a unified logon with the PeopleSoft EnterpriseOne security, set up a unified logon server for each instance of PeopleSoft EnterpriseOne on each server. For example, if you have an NT server with multiple releases of PeopleSoft EnterpriseOne, you need a unified logon server for each release on the server.</p> <p>The unified logon server differentiates instances of PeopleSoft EnterpriseOne based on the port numbers for these instances. For example, if the port number for PeopleSoft EnterpriseOne is 6104, the port number for the associated unified logon server is 6104. Other instances and unified logon servers use different port numbers.</p>
Verify and modify jde.ini file.	Verify and modify the jde.ini file that will be deployed to the server's workstation installations.
Set up sign-in security.	Require sign-in security for all machines.

Process Flow for Sign-in Security

PeopleSoft EnterpriseOne provides sign-in security with an architecture that is designed to provide user security for PeopleSoft EnterpriseOne and the logically attached database management systems. The security architecture prevents you from viewing the database or system password, and therefore, bypassing PeopleSoft EnterpriseOne applications to view and change data.

This text explains the process flow for standard sign-in security:

- Workstations sign in to PeopleSoft EnterpriseOne by using their user ID and password.

These workstations can be networked or standalone workstations, laptop computers, or other PeopleSoft EnterpriseOne hosts.

If you enter a valid user ID and password, as validated against the local workstation installation, the start-up process continues.

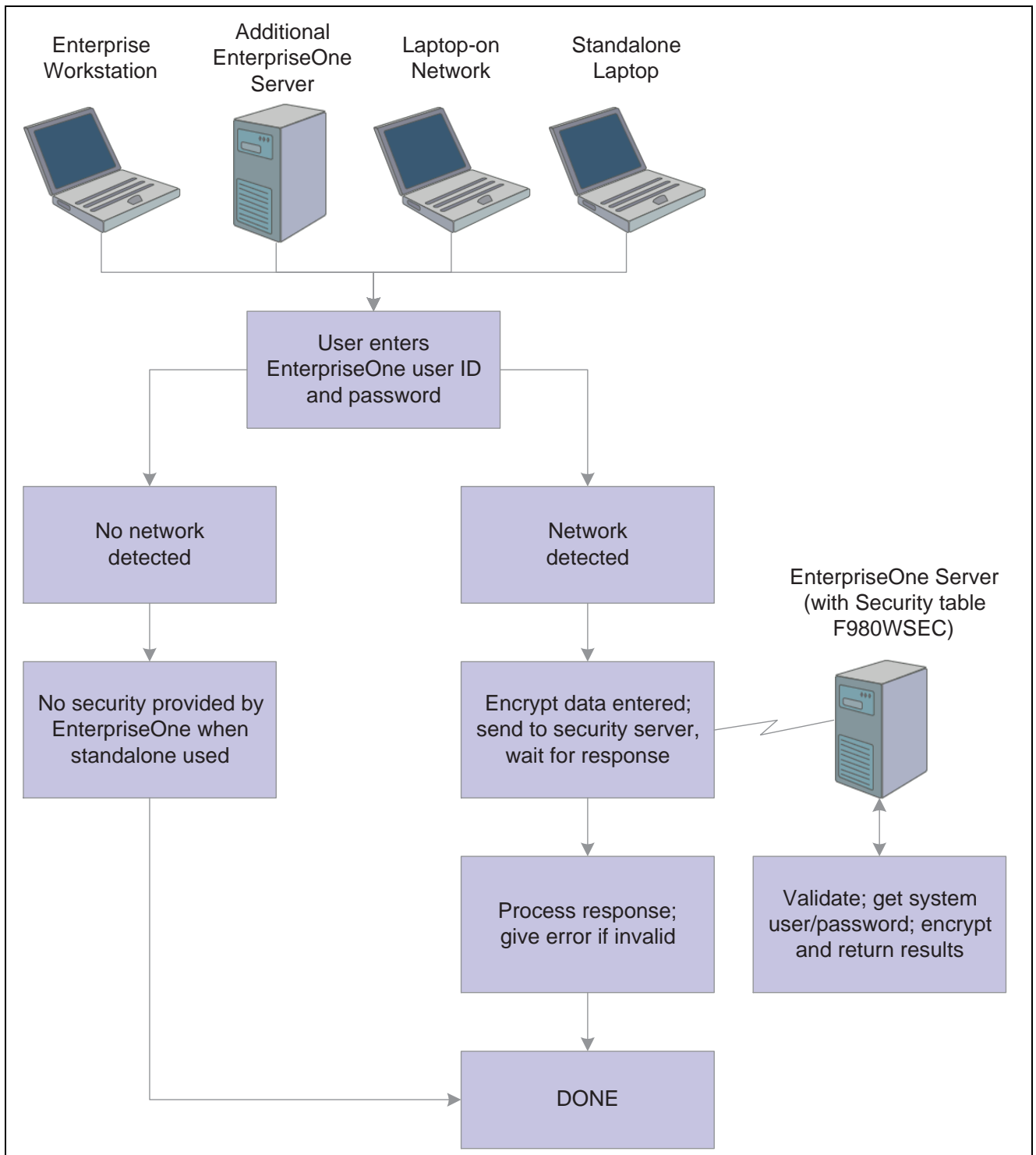
- As the software starts up, it tries to detect an operational network environment.

If a network is not detected, the software allows local operation in a store-and-forward mode. Because the workstation or laptop computer is not connected to a network or an enterprise server, no validation can be performed against the F980WSEC table. Therefore, security is limited to that provided by the local workstation or laptop installation.

If a network is detected, the software encrypts the password information and sends it over the network to the PeopleSoft EnterpriseOne enterprise server.

The enterprise server checks the incoming validation request against a table of valid users and passwords. If the user ID and password information are valid, the software accepts the sign-in values and returns the system ID and password to the logically attached database servers. This information is also encrypted on the enterprise server prior to broadcast on the network.

This graphic displays a process flow model for standard sign-in security:



Process flow model for standard PeopleSoft EnterpriseOne sign-in security

The process flow for sign-in security with a unified logon is as follows:

- A user starts up PeopleSoft EnterpriseOne on a workstation.
- PeopleSoft EnterpriseOne verifies that the unified logon is active and then sends an authentication request to the unified logon server, based on the domain user ID.

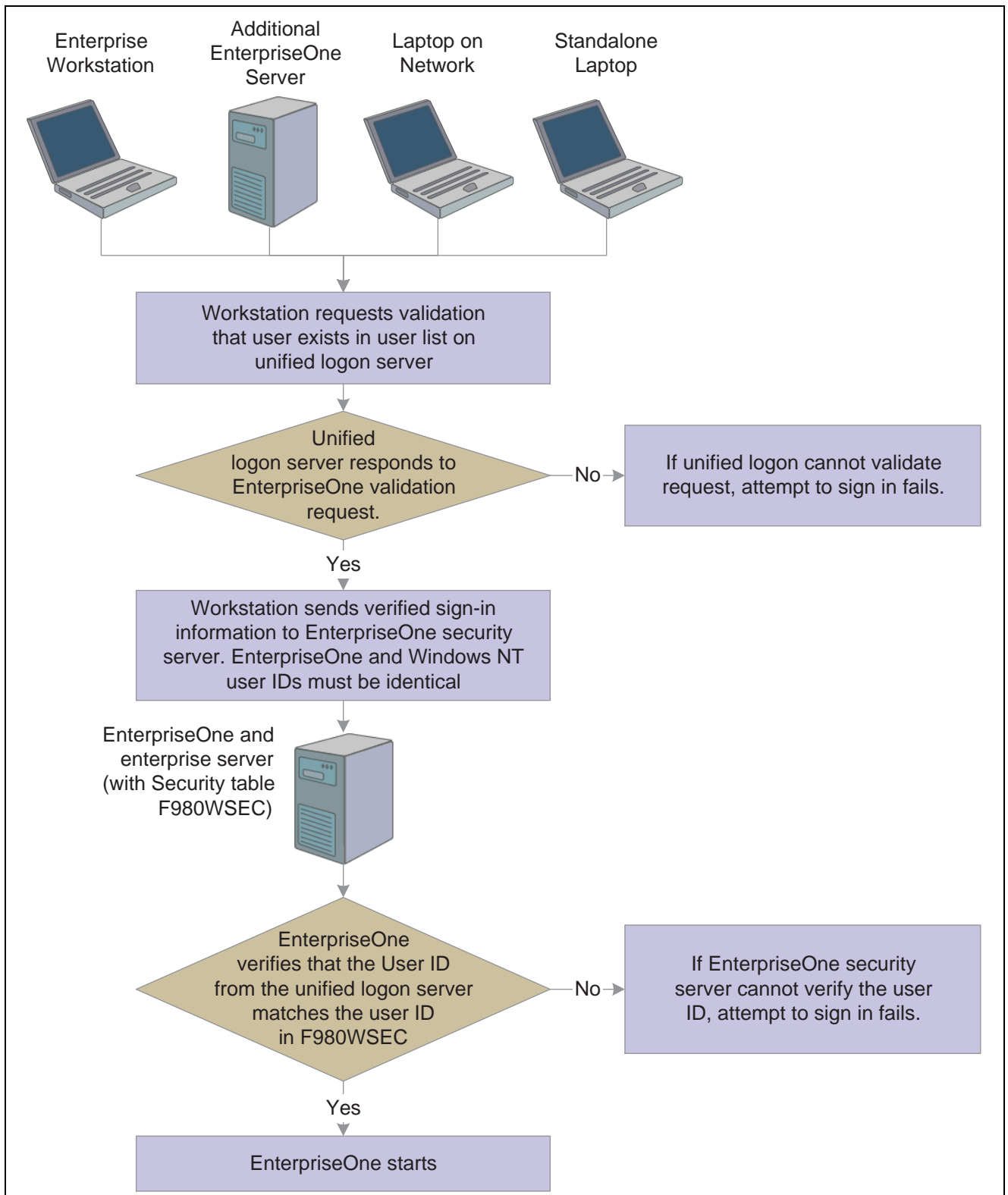
Note. The unified logon server is not a physical server. It is a device that verifies sign-in security against the domain sign-in security maintained by Windows.

During jdesnet initialization, jdesnet activates the unified logon server thread. The unified logon server ends automatically when jdesnet ends.

- The unified logon server searches its user list for an entry that matches the domain user ID. When the server finds a match, the server sends a validation request to the enterprise server.
- The enterprise server verifies that the response from the unified logon server matches the security information in the F980WSEC table.
- If the security information from the user list on the unified logon server matches the security information in table F980WSEC on the enterprise server, the start-up process continues.
- The first time that a user signs in to PeopleSoft EnterpriseOne with the unified logon, the Environment Selection appears.

The user must enter an environment in the Environment field. Select the option to set the environment as the default, and avoid the Environment Selection form on subsequent sign-in attempts.

This illustration displays the process flow for unified logon:



Unified logon process flow

ShowUnifiedLogon Setting

The ShowUnifiedLogon setting in the [SECURITY] section of the jde.ini file allows users to reset whether the Environment Selection form appears at sign-in. This feature allows users to change the environment later. This table describes the jde.ini file setting for the [SECURITY] section:

Value	Description
0	A value of 0 for ShowUnifiedLogon disables the Environment Selection form. When you click the option on the Environment Selection form to set a default environment, you set this value to 0.
1	A value of 1 for ShowUnifiedLogon enables the Environment Selection form. When a user signs in to PeopleSoft EnterpriseOne, the Environment Selection form appears and allows the user to choose an environment. This setting is the default for ShowUnifiedLogon.

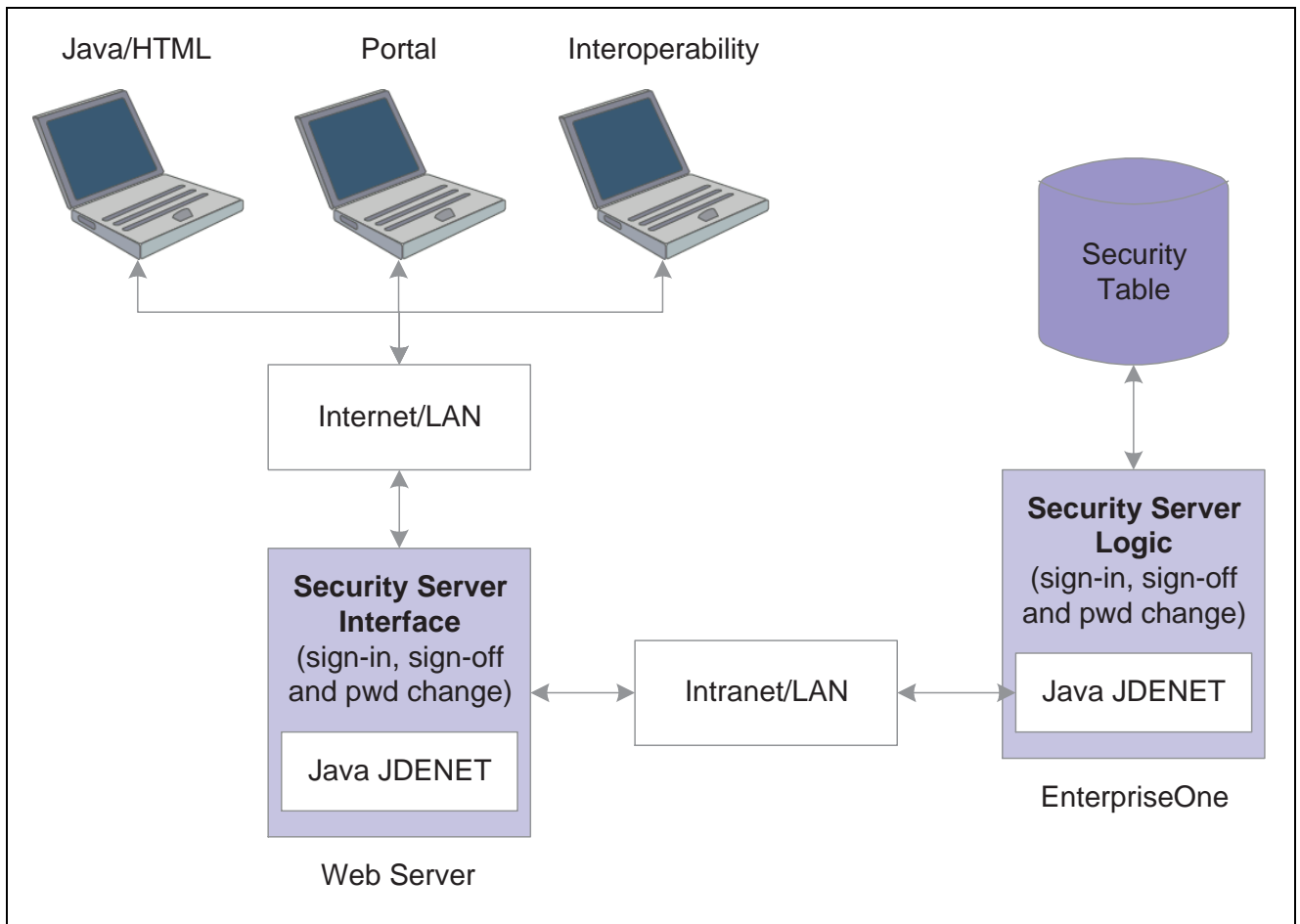
Sign-in Security for Web Users

The PeopleSoft EnterpriseOne security server and the F98OWSEC table authenticate Java/HTML, Portal, and Interoperability users who sign in to PeopleSoft EnterpriseOne across the internet to the JAS security server. The JAS security server acts as an interface between the web user's client workstation and the security server.

When web users sign in, disconnect, or make a password change, the JAS server sends the request using a JDENET message to the security server, which, in turn, accesses the F98OWSEC table. The security server then returns the authentication through a JDENET message to the JAS security server. If the user is authenticated, the security info is cached to the JAS security server.

The JAS security server acts as an intermediary between the Java/HTML, Portal, and Interoperability client and the security server.

This graphic displays a process flow for sign-in security with unified logon for web users:



Sign-in security with unified login for web users

As the security intermediary, the JAS security server handles this tasks:

- Connecting to the PeopleSoft EnterpriseOne security server for user security authentication and password when a web user signs in.
- Switching to a secondary PeopleSoft EnterpriseOne security server when the primary server is down, provided the correct jas.ini settings are defined.
- Notifying Java/HTML, Portal, and Interoperability client workstations when a user password has expired. If an Interoperability user's password has expired, sign-in fails without notification of the cause.
- Sending error message to user log after the web user has attempted unsuccessfully to sign in x number of times to PeopleSoft EnterpriseOne, where x is the number of sign-in attempts defined in the F98OWSEC table.
- Allowing Java/HTML and Portal users to change name and password.
- Encrypting JDENET messages sent between the JAS security server and the PeopleSoft EnterpriseOne security server.
- Keeping a valid user session open until the user signs off or the session expires.

To the web user, sign-in and sign-out function the same as they do to a user on Windows, UNIX, or iSeries platforms.

To set up security for web users through the PeopleSoft EnterpriseOne security server, add these parameters to those that already exist in the jas.ini file:

[SECURITY] Parameter in jas.ini File	Parameter Value
NumServers	Total number of PeopleSoft EnterpriseOne security servers that are available to web users signing on to the system. If this parameter is missing, the default value is 1 and the primary security server handles the sign-in.
SecurityServer	Name of the primary security server.
SecurityServerN	Name of the secondary security server. The value of N is 1 for the first secondary server, 2 for the second, and so on. Assign values to this parameter if you want sign-in to switch to a secondary server if users cannot sign in to the primary server.
UserLogonCookie=	If the value is TRUE, the user can save signon information (username, password, and environment) in an encrypted cookie on the workstation and does not have to type the information in for subsequent sign-ins. If the value is FALSE, the feature is disabled.
#CookieLifeTime unit	Unit of time used to measure a cookie's lifetime. For example, the parameter value day means that the cookie's lifetime is measured in days.
Cookie LifeTime	Amount of time before a cookie expires. The unit of measure is defined by the #CookieLifeTime unit parameter value. If that value is day and the value of the Cookie LifeTime parameter is 7, the cookie expires in seven days.

If you define one primary server and two secondary servers, the jas.ini file [SECURITY] settings look like this example:

```
NumServers=3
SecurityServer=JDED
SecurityServer1=JDEC
SecurityServer2=corowhp2
UserLogonCookie=TRUE
#CookieLifeTime unit is day
CookieLifeTime=7
```

If you define one or more secondary servers, sign-in fails over to the secondary server if the primary server is down. If both the primary PeopleSoft EnterpriseOne security server and a secondary server as defined in the jas.ini file fail, the JAS server fails the user sign-in.

If you do not define a server number or any secondary servers, the jas.ini [SECURITY] settings look like this example:

```
[SECURITY]
SecurityServer=JDED
UseLogonCookie=TRUE
CookieLifeTime unit is day
CookieLifeTime=7
```

Setting Processing Options for P98OWSEC

The User Security (P98OWSEC) program has processing options that you can use to set a default password when creating user security for users or roles, and to set a default change frequency for the password:

Default

Although processing options are set up during PeopleSoft EnterpriseOne implementation, you can change processing options each time that you run a program.

- 1. Enter a '1' to default the User ID into the password field.**
- 2. Enter in the default Change Frequency.**
- 3. Enter the number of sign-on attempts a user is given prior to being disabled.**
- 4. Enter if a new user is to default to as enabled or disabled.**
- 5. Enter a '1' to force immediate password change of new users.**

Password

Although processing options are set up during PeopleSoft EnterpriseOne implementation, you can change processing options each time you run a program.

- | | |
|---|---|
| 1. Enter the daily password change limit that will be applied to all users when attempting to change a password. | If this field is 0 or is left blank, there will be no limit on daily password changes. |
| 2. Enter the minimum password length that is to be used when users attempt to change a password. | If this field is 0 or is left blank, the password will not be checked for a minimum length. |
| 3. Enter the minimum number of character that must be used within a password. | If this field is 0 or is left blank, the password will not be checked for characters. |
| 4. Enter the minimum number of numerics that must be used within a password. | If this field is 0 or is left blank, the password will not be checked for numerics. |

5. Enter the maximum number of consecutive characters that can be used in a password.

If this field is 0 or is left blank, the password will not be checked for consecutive characters.

6. Enter the minimum number of special characters that must be within a password.

If this field is 0 or is left blank, the password will not be checked for special characters.

CHAPTER 12

Setting Up User Security

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

- Create and revise user security.
- Review security history.
- Manage data sources for user security.
- Enable and synchronize security settings.
- Run a Security Analyzer report.
- Manage unified logon.

Understanding User Security

Use the EnterpriseOne Security application (P98OWSEC) to create, test, and change user security for PeopleSoft EnterpriseOne and the logically attached database management systems. The security architecture prevents you from viewing the database or system password and from bypassing PeopleSoft EnterpriseOne applications to view and change data. PeopleSoft EnterpriseOne uses an encryption algorithm to ensure that applications other than PeopleSoft EnterpriseOne security cannot access passwords transmitted across the network.

You can also set up a unified logon server for an PeopleSoft EnterpriseOne server. The unified logon server enables PeopleSoft EnterpriseOne to use the domain logon information to determine user security. In a PeopleSoft EnterpriseOne unified logon scenario, a user needs to enter a user ID and a password only at network logon.

Creating and Revising User Security

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

- Create user security.
- Copy user security.
- Revise user and role security.
- Revise all user security.
- Change a sign-in password.
- Require sign-in security.

Understanding How to Create and Revise User Security

You can create security records one at a time for each of the users, you can set security for a role, or you can set security for all users. You should use this feature to set up user security initially. The User Security application provides a copy function to simplify the creation of security records for individual users.

Note. You should create a model user with security information that you can copy to create other users. Typically, users within a specific role use similar security information.

You should keep user security simple. Managing PeopleSoft EnterpriseOne user IDs and system (database) user IDs can become complicated quickly. The simplest way to set up user security is to have all data sources share the same system user ID and password by leaving the data source field blank when you initially create user security records for users or roles on the Security Revisions form.

When you leave the data source field blank, the P98OWSEC application automatically enters *DEFAULT* in the field. The DEFAULT data source allows you to create one security record for all users. Each time that a user accesses a table through an PeopleSoft EnterpriseOne application, the software searches for a security record for that user and that specific data source where the table resides. If the software does not find a specific record, then it uses the default data source, which is the security record that you created with the DEFAULT data source field.

You use system user IDs to manage user access to databases. Although you should try to maintain as few system user IDs as you can, occasions arise that require you to set up database security in addition to the PeopleSoft EnterpriseOne object and user security for specific users and specific tables. For example, you might need to create system users with additional authority to what the typical system user needs.

See Also

EnterpriseOne Tools 8.94 PeopleBook: Configurable Network Computing Implementation, “Data Sources”

Prerequisites

Before you complete the tasks in this section:

- Set up all user records in the Address Book (P01012) application.
- Create user profiles using the User Profile (P0092) application.

See [Chapter 6, “Working with User Profiles,” page 77](#).

- Attach the proper Address Book record to the user or role profile.
- Review and set the appropriate processing options before using the P98OWSEC application for the first time.

See [Chapter 6, “Working with User Profiles,” Setting Processing Options for User Profile Revisions \(P0092\), page 82](#).

Forms Used to Create and Revise User Security

Form Name	Form ID	Navigation	Usage
Work With User Security	W98OWSECE	Security Maintenance (GH9052), User Security (P98OWSEC)	Access forms to work with user security.
Security Revisions	W98OWSECB	On Work With User Security, click Add.	Create user security.
Copy User Records	W98OWSECN	On Work With User Security, select the user or role and click Copy to copy all security records. To copy a single user security record, select the security record from the detail area, and select Copy Record from the Row menu.	Copy user security.
Security Detail Revisions	W98OWSECI	On Work With User Security, select the appropriate record, and then select Revise Security from the Row menu.	Revise user and role security.
Administration Password Revisions	W98OWSECF	Security Maintenance menu (GH9052), Administrative Password Revisions (P98OWSEC)	Change a sign-in password.
Sign On Security - Required/Not Required	W98OWSECG	On Work With User Security, select Req / Not Req from the Form menu.	Require all machines to use PeopleSoft EnterpriseOne sign-in security

Creating User Security

Access the Work with User Security form.

To create user security:

1. On the Work With User Security form, click Add.

Note. Do not use the GlobalPasswordPolic option in the Form menu. This form contains password settings that only apply for users who are using the User Profile Self-Service (P0092SS) application.

2. On Security Revisions, complete one of these fields:

- User ID

If you enter a user ID that already exists, you can modify data source information for the user. The system disables all other fields and options for the user ID.

- Role

If you enter a role that already exists, you will overwrite the security record for role when you enter information on the form.

Note. When you type information in one of these fields, the system disables the other field. For example, if you type *ROLE1* in the User Class/Role field, the User ID field becomes unavailable for data entry.

3. Complete these fields:

- Data Source

If you leave this field blank, you will set security for all data sources. *DEFAULT* appears in the Data Source field when you tab out of the field.

- System User

- Password

We recommend you complete at least the System User field.

If you create records by role or for all users at one time, the Password field is populated according to the processing option that you select.

4. In the User Status area, select one of these options:

- Enabled

With User Status enabled, security allows the user to sign in. This option is the default setting when you create user security.

- Disabled

With User Status disabled, security prohibits the user from signing in to the software.

Note. If a user commits a security violation, such as exceeding the maximum number of allowed password attempts, the software automatically sets the value for User Status to *Disabled*. The system administrator must access the user security record for the user and set User Status to *Enabled* before the user can sign in. In addition, the system administrator can access Administrative Password Revisions to reset the password of the user, which also restores a user profile to the status of enabled.

5. If you want to set limits on the passwords for users, complete these fields:

- Allowed Password Attempts

Enter the number of invalid password attempts allowed before the system disables access for the user.

- Password Change Frequency

Enter the number of days until the system requires the user to change the password.

- Daily Password Change Limit

Enter the allowed number of times a user can change a password in a day.

- Force Immediate Password Change

Click this option to require the user to change the password on the next sign-in.

6. Click OK to save the current user security information.

User ID

The code that identifies a user profile.

Role	<p>A profile that you use to classify users into groups for system security purposes. You use group profiles to give the members of a group access to specific programs.</p> <p>Some rules for creating a profile for a user class or group are as follows:</p> <ul style="list-style-type: none"> • The name of the user class or group must begin with an asterisk (*) so that it does not conflict with any system profiles. • The User Class/Group field must be blank when you enter a new group profile.
Data Source	The data source to which the user is secured unless a valid system user and system password exists in the record. Blank indicates all data sources.
System User	Identifies the actual user that PeopleSoft EnterpriseOne will use to connect to the database management systems (DBMS) that you have specified as the data source. The system user who you define here must exactly match the user value defined in the DBMS.
Password	<p>Identifies the user password that PeopleSoft EnterpriseOne will use to validate when signing on to PeopleSoft EnterpriseOne. This is the only field that end-users are allowed to change through User Password Revisions.</p> <p>When you set up users for the first time, you should set their PeopleSoft EnterpriseOne password to a value equal to their PeopleSoft EnterpriseOne user ID.</p>
Allowed Password Attempts	The number of sign-on attempts that a user can make before that user profile is disabled.
Password Change Frequency	Identifies the number of days before PeopleSoft EnterpriseOne requires that a user change the PeopleSoft EnterpriseOne password.
Daily Password Change Limit	The number of times per day that a user is allowed to change the password.
Force Immediate Password Change	This option forces a user to change the password on the next sign-in.

Copying User Security

A user profile must already exist for a user before you can create user security records for the user. In addition, when you copy security records to a user, security records must not already exist for the user. If you try to copy user security to a user with existing user security records, you will receive an error message.

Note. You should create a model user with security information that you can copy to create other users. Typically, users within a specific role use similar security information.

Access the Work With User Security form.

To copy user security:

1. On Work With User Security, find the user, and then do one of these:
 - To copy all user security records for a user or role, select the user or role in the tree structure, and click Copy.

- To copy a single user security record for a user or role, select the security record row in the detail area, and select Copy Record from the Row menu.
2. On the Copy User Records form, enter a valid user ID in the To User / Role field and click OK.

Revising User and Role Security

Access the Work With User Security form.

To revise user and role security:

1. On Work With User Security, complete the User ID / Role field.
2. Click Find.
3. Select the appropriate record in the tree structure, and then select Revise Security from the Row menu.
4. On Security Detail Revisions, complete these fields, as necessary:
 - User Status
Under User Status, you can enable or disable a user profile.
 - Password Change Frequency
 - Allowed Password Attempts

Note. For a role, select the appropriate option from the Change box to enable each field.

5. Click OK.

Revising All User Security

Access the Work With User Security form.

To revise all user security:

1. On the Work With User Security form, from the Form menu, select Revise All.
2. On Security Detail Revisions, in the Change box, select any of these options to enable the related field:
 - User Status
 - Frequency
 - Attempts
 - Change Limit
3. Complete any of these fields, and then click OK:
 - User Status
This field allows you to enable or disable user profiles.
 - Password Change Frequency
 - Allowed Password Attempts
 - Force Immediate Password Change
This requires the user to change the password on the next sign-in.

Changing a Sign-in Password

Access the Administration Password Revisions form.

To change a sign-in password (administrators only):

Note. You can also access Administrative Password Revisions from the User Security application. On Work with User Security, find the user, select the user in the tree structure, and then select Password Revisions from the Row menu.

1. On Administration Password Revisions, complete these fields and click OK:

- **User ID**

The user ID is the default value in this field when the user record is highlighted and Password Revision is activated.

- **New Password**

On this form, the system does not restrict the password choices. Any password is valid.

- **New Password - Verify**

- **Force Immediate Password Change**

This requires the user to change the password during the next sign-in.

2. Click OK.

User ID

The code that identifies a user profile.

New Password

Identifies the new value for the user password that PeopleSoft EnterpriseOne uses to validate during the sign-in process. When a user creates a new password, these rules must be followed:

- The new password cannot be the same as the old password.
- The new password cannot be the same as the user ID.
- The new password must be at least six characters in length.

System administrators using Administrative Password Revisions to reset a user's password are not restricted by these rules. Often, standards exist for resetting a forgotten password. For example, a new password reset by a system administrator might need to be the same as the user ID or it may simply be the word *password* each time. Regardless, the new value specified in this field will become effective when the user signs on to PeopleSoft EnterpriseOne for the next time.

New Password - Verify

Identifies a duplicate of the value that you specified in the New Password field.

The value that you enter here must exactly match the value you enter in the New Password field.

Requiring Sign-in Security

Use this feature to require all machines to use PeopleSoft EnterpriseOne sign-in security. This procedure enables mandatory security only for the environment that you are signed onto when you make this change.

Access the Work With User Security form.

To require sign-in security:

1. On Work With User Security, select Req / Not Req from the Form menu.
2. On the Sign On Security - Required/Not Required form, click the lock icon to change the Security Server to *Required* or *Not Required*.

Note. If you set up the security as *Not Required* and have security turned on through the jde.ini file on the enterprise server, users that comment out signon security in their jde.ini files will still not be able to access any data sources without knowing the system user ID and password.

When attempting to access a table in a secured data source, users will receive a database password entry form. If system user IDs and passwords are confidential, no one will be able to access the secured tables.

Reviewing Security History

If you know the specific user or role, you can review the user's or role's security history by using the PeopleSoft EnterpriseOne Security application. You can also search for specific information for all users. For example, to see the users who were deleted on a given day, you can search on event type 06 (*Delete User*) and a specific event date.

Prerequisite

The [SECURITY] section in the server jde.ini must include theHistory=1 setting for the system to record security history.

Forms Used to Review Security History

Form Name	Form ID	Navigation	Usage
Work With User Security	W98OWSECE	Security Maintenance (GH9052), User Security (P98OWSEC)	Access forms to review security history.
Work With Security History	W98OWSECC	On Work With User Security, from the Form menu, select Security History.	Click Find to review the security history records.

Managing Data Sources for User Security

This section provides an overview of data source management for user security and discusses how to:

- Add a data source to a user, a role, or all users.
- Revise a data source for a user, a role, or all users.
- Remove a data source from a user, a role, or all users.

Understanding Data Source Management for User Security

You add data sources to user and role records in user security to authorize users and roles to access PeopleSoft EnterpriseOne databases. You can also revise the system user and system password for existing data sources.

Forms Used to Manage Data Sources for User Security

Form Name	Form ID	Navigation	Usage
Work With User Security	W98OWSECE	Security Maintenance (GH9052), User Security (P98OWSEC)	Access forms to set up user security.
Add Data Source	W98OWSECS	On Work With User Security, from the Form menu, select Add Data Source.	Add a data source to a user, role, or all users.
Data Source Revisions	W98OWSECH	On Work With User Security, select a data source, and then select Revise Data Source from the Row menu.	Revise a data source.
Remove Data Source	W98OWSECK	On Work With Security, select the appropriate record in the tree structure, and then click Delete.	Remove a data source. If you chose a data source for a specific user or role, this form displays the user ID or the role name with the data source name. If you chose only the data source, this form displays only the data source name.

Adding a Data Source to a User, a Role, or All Users

Access the Add Data Source form.

To add a data source to a user, a role, or all users:

- On Add Data Source, complete one of these fields or options:
 - User ID
Complete this field to add a data source to a specific user.
 - Role
Complete this field to add a data source to a specific role.
 - All Users
Select this option to add a data source to all users.
- Complete these additional fields and click OK:
 - Data Source
Leave this field blank to set the data source information for all data sources. When you leave this field blank, the system automatically enters *DEFAULT* in the field.
 - System User

Revising a Data Source for a User, a Role, or All Users

Access the Work With User Security form.

To revise a data source for a user, a role, or all users:

1. On Work With User Security, complete the Data Source field, and then click Find.

Note. You can also enter both a data source and user ID/role. If you select just a data source, the change will affect all users.

2. Select the data source in the tree structure and then, from the Row menu, select Revise Data Source.

The Data Source Revisions form appears. If you chose a specific user or role, this form displays the user ID or the role name and the data source information. If you chose only the data source, this form automatically selects the All Users option with the data source information.

3. Complete the System User field and click OK:

This field is necessary to access databases within the software. Depending on what you chose from the tree on Work With User Security, this information will apply to a specific user, a specific role, or all users.

Removing a Data Source for a User, Role, or All Users

Access the Work With User Security form.

To remove a data source for a user, a role, or all users:

1. On Work With User Security, complete the Data Source field, and then click Find.
2. Select the appropriate record in the tree structure, and then click Delete.

Note. For a user, you can also select a row in the detail area for the user, and then click Delete.

The Remove Data Source form appears. If you chose a data source for a specific user or role, this form displays the user ID or the role name with the data source name. If you chose only the data source, this form displays only the data source name.

Important! If you performed the search by data source without including a specific user or role, when you click OK on Remove Data Source, you remove the data source for *all* users.

3. Click OK to remove the data source.

Enabling and Synchronizing Security Settings

This section provides an overview about enabling and synchronizing security settings and discusses how to:

- Change the workstation jde.ini file for user security.
- Set auxiliary security servers in the workstation jde.ini.
- Change the timeout value due to security server communication error.
- Change the enterprise server jde.ini file for security.
- Set auxiliary security servers in the server jde.ini.
- Verify security processes in the server jde.ini.

Understanding Security Setting Synchronization

You must modify the enterprise server and the workstation jde.ini files to enable and synchronize security settings between the enterprise server and the workstation.

Note. For the PeopleSoft EnterpriseOne workstations, enable security by changing settings in the workstation jde.ini file. You should make these changes on the deployment server-resident jde.ini file that is delivered to the workstation through a package installation.

Changing the Workstation jde.ini File for User Security

Access the jde.ini file.

To change the workstation jde.ini file for security:

1. Locate the jde.ini file that will be sent to the workstation as part of a package installation. This file is located on the deployment server in the release share path:

```
\\xxx\CLIENT\MISC\jde.ini
```

Where xxx is the installed release level of the software (for example, 810).

2. Using a text editor such as Notepad, view the jde.ini file to verify the setting:

```
[SECURITY]
SecurityServer=Enterprise Server
NameDefaultEnvironment=Default Environment
```

This table explains the variable values:

Setting	Value
Security Server	The name of the enterprise server. For workstations to sign on and run batch reports on the enterprise server, this value must be the same for both the workstation and the enterprise server.
DefaultEnvironment	A name that identifies any valid environment. If no value is specified, security is not enabled for that workstation.

Setting Auxiliary Security Servers in the Workstation jde.ini

Within the [SECURITY] section of the workstation jde.ini file, you can set as many as ten auxiliary security servers. This example shows how the jde.ini file might look:

```
[SECURITY]
NumServers=Numeric Value
SecurityServer=Enterprise Server Name (primary)
SecurityServer2=Enterprise Server Name (auxiliary)
SecurityServer3=Enterprise Server Name (auxiliary)
```

This table explains the variable values:

Setting	Value
NumServers	The total number of security servers (primary and auxiliary) that you set under the [SECURITY] section of the jde.ini file. For example, if you set one primary and four auxiliary servers, the NumServers value would be 5. You can set NumServers to any value between one and ten. If you do not include the NumServers setting, the system assumes that you have only one server.
SecurityServer <i>n</i>	<p>The name of an PeopleSoft EnterpriseOne enterprise server. The primary and auxiliary security server names must all correspond to valid enterprise servers. The values must be the same for both the workstation and enterprise servers for workstations to sign on to and run batch reports from the enterprise server.</p> <p>The variable value <i>n</i> can be a number between 1 and 10. This number defines the auxiliary security server.</p>

Changing the Timeout Value Due to Security Server Communication Error

You might need to change a setting in the workstation jde.ini file if you receive an error such as:

```
Failure to Communicate with Security Server.
```

Change this section:

```
[JDENET]
connectTimeout=30
```

Changing the Enterprise Server jde.ini File for Security

To change the enterprise server jde.ini file for security, you should verify the server jde.ini file settings as shown in this task. Use these settings to specify the internal security parameters, valid users and passwords, environments, and data sources.

Locate the enterprise server's jde.ini file.

Using an ASCII editor, such as Notepad, view the jde.ini file to verify these settings:

```
[JDENET_KERNEL_DEF4]
dispatchDLLName=name of host dll
dispatchDLLFunction=JDEK_DispatchSecurity
maxNumberOfProcesses=1
beginningMsgTypeRange=551
endingMsgTypeRange=580
newProcessThresholdRequests=0
[SECURITY]
Security Server=Enterprise Server Name
User=user ID
Password=user password
ServerPswdFile=TRUE/FALSE
DefaultEnvironment=default environment
```

This table explains the variable values:

Setting	Value
dispatchDLLName	<p>Values for enterprise server host platforms are:</p> <p>HP9000, libjdekrnl.sl</p> <p>RS/6000, libjdekrnl.so</p> <p>Windows (Intel), jdekrnl.dll</p> <p>Windows (Compaq AlphaServer), jdekrnl.dll</p> <p>iSeries, JDEKRNL</p> <p>For UNIX platforms, values are case-sensitive.</p>
SecurityServer	The name of the enterprise server. This value must be the same for both the workstation and the enterprise server for workstations to run batch reports on the enterprise server.
User	The ID of a user with access to the F98OWSEC. This is the ID used to connect to the DBMS; therefore, this value must match that of the target DBMS.
Password	The password for the user ID with access to the F98OWSEC. This is the password used to connect to the DBMS; therefore, this value must match that of the target DBMS.
ServerPswdFile	<p>This parameter is valid for servers operating under UNIX operating systems.</p> <p>The setting of this parameter determines whether the system uses special password handling for batch reports running on the server.</p> <p>Set the value to TRUE to instruct the system to enable special handling of passwords.</p> <p>Set the value to FALSE to disable special handling.</p> <p>When the system runs a batch report on the server, it runs the report using a string of line commands and parameters that includes the user password. Under UNIX operating systems, it is possible to use the process status command (ps command) to query the status of a job and view the parameters that were used to start the process.</p> <p>As a security measure, you can enable special handling by the software. When enabled, the software does not include the user password in the parameter list for a batch process. Instead, it includes the name of a file that contains the user password. This file is deleted as soon as the batch report reads the password.</p>
DefaultEnvironment	The name of a valid environment for accessing the security table (or example, PD810).

Setting Auxiliary Security Servers in the Server jde.ini

Within the [SECURITY] section of the server jde.ini file, you can set one to ten auxiliary security servers. You set multiple auxiliary security servers to establish levels of default servers. For example, if a machine cannot access a given security server, the machine tries the next security server that is defined in the [SECURITY] section. The settings for the auxiliary security servers might look like this example:

```
[SECURITY]
NumServers=Numeric Value
```

```

SecurityServer=Enterprise Server Name (primary)
SecurityServer2=Enterprise Server Name (auxiliary)
SecurityServer3=Enterprise Server Name (auxiliary)

```

This table explains the variable values:

Setting	Value
NumServers	The total number of security servers (primary and auxiliary) that you set under the [SECURITY] section of the jde.ini file. For example, if you set one primary and four auxiliary servers, the NumServers value would be 5. You can set NumServers to any value between one and ten. If you do not include the NumServers setting, the system assumes that you have only one server.
SecurityServerx	<p>The name of an enterprise server. The primary and auxiliary security server names must all be valid enterprise servers. The values must be the same for both the workstation and enterprise servers for workstations to log onto and run batch reports from the enterprise server.</p> <p>The variable value <i>x</i> can be any number between one and ten. This number defines the auxiliary security server.</p>

Verifying Security Processes in the Server jde.ini

You should define only one process for the security network. You can set multiple processes, but they are probably not necessary. Under the [JDENET_KERNEL_DEF4] section of the server jde.ini file, verify that the parameter is set:

```

[JDENET_KERNEL_DEF4]
maxNumberOfProcesses=1

```

Running a Security Analyzer Report

This section provides an overview of running a Security Analyzer Report and discusses how to:

- Run the Security Analyzer by Data Source Report (R98OWSECA).
- Run the Security Analyzer by User or Group Report (R98OWSECB).

Understanding the Security Analyzer Report

This process generates two separate reports that provide you with an analysis of PeopleSoft EnterpriseOne security. The first report is the Security Analyzer by Data Source (R98OWSECA) and is organized and sorted by data source. A blank data source means that security for the System User ID is applicable to all data sources. The Security Analyzer by Data Source report is based on data that it reads from the F98OWSEC table.

The second report is the Security Analyzer by User or Group (R98OWSECB) and is organized by user or role. The Security Analyzer by User or Role report is also based on data that it reads from the F98OWSEC table.

Form Used to Run a Security Analyzer Report

Form Name	Form ID	Navigation	Usage
Work With Batch Versions - Available Versions	W98305A	Report Management (GH9111), Batch Versions (P98305)	Run the Security Analyzer by Data Source (R98OWSECA) and Security Analyzer by User or Group (R98OWSECB) reports.

Running the Security Analyzer by Data Source Report (R98OWSECA)

This report presents security analysis information for each data source, each user ID, and each role. The report is sorted by data source and then by user ID. The columnar data appears:

- Data Source
Identifies the data source to which the user is secured. Blank indicates all data sources.
- User ID
- User / Role
An identification code for a user profile.
- System User ID
Identifies the actual user that PeopleSoft EnterpriseOne uses to connect to the database management system (DBMS) that you specified as the data source. The system user shown here must match the user value that is defined in the DBMS.
- Change Frequency
Indicates the number of days before the system requires that a user change the password. This data can be set by individual user ID or by role.
- Source Password Changed
Indicates the date when a user's password was last changed.
- Invalid Signons
Indicates the number of invalid sign-in attempts by a user. If the retry count value exceeds the number of allowed attempts, the user profile is disabled.
- Allowed Attempts
Indicates the number of signon attempts that a user can make before that user profile is disabled.
- User Status
Indicates whether the user can sign in to PeopleSoft EnterpriseOne. Values are 01 (enabled) and 02 (disabled).
- Status
Displays the status of the User Status field.

Access the Work With Batch Versions - Available Versions form.

To run the Security Analyzer by Data Source Report (R98OWSECA):

1. On the Work With Batch Versions - Available Versions form, select a version and then click Select.

The default version is XJDE0001. It creates a report for all user IDs for all data sources.

2. On the Version Prompting form, click Submit.
3. On Report Output Destination, select any of these options:
 - On Screen
 - To Printer
 - Export to CSV
4. If desired, select the OSA Interface Name option and enter a name in the box that appears.
5. Click OK.

Running the Security Analyzer by User or Group Report (R98OWSECB)

The Security Analyzer by User or Group Report (R98OWSECB) report presents security analysis information for each user ID, each group, and each data source. The report is sorted either by user ID or user group, depending on which processing option you select. The columnar data is displayed on the report:

- User ID
- Role
- Password Change Frequency

Indicates the number of days before a user must change the password. This data can be set by individual user ID or by group.

- Data Source

Identifies the data source to which the user is secured. A blank indicates all data sources.

- System User

Identifies the actual user that the software uses to connect to the database management system (DBMS) that you specified as the data source. The system user that is defined here must match the user value that is defined in the DBMS.

Access the Work With Batch Versions - Available Versions form.

To run the Security Analyzer by User or Group Report (R98OWSECB):

1. On the Work With Batch Versions - Available Versions form, select a version and click Select.
 The default version is XJDE0001. It creates a report for all user IDs for all data sources.
 By default, the XJDE0001 version has the processing option for this report set to 1. This option generates a report by user ID.
 To generate a report by role, you can prompt for processing options and then, on the User Setup tab, change the value to 2.
2. On the Version Prompting form, click Submit.
3. Complete the processing options as necessary, and then click OK.
4. On Report Output Destination, select any of these options:
 - On Screen
 - To Printer

- Export to CSV
5. If desired, select the OSE Interface Name option and type a name in the field that appears.
 6. Click OK.

Managing Unified Logon

This section provides an overview of unified logon and discusses how to:

- Modify the jde.ini setting to enable or disable unified logon.
- Set up a service for unified logon.
- Remove a service for unified logon.

Understanding Unified Logon

For configurations that use a Windows enterprise server, to set up unified logon, you need to modify only the [SECURITY] section of the jde.ini file. When a user signs on, these settings alert the software to use unified logon.

When the enterprise server is on a non-Windows platform, you need to set up a Windows service for unified logon. This service identifies the unified logon server for PeopleSoft EnterpriseOne. You also need to set the unified logon settings in the [SECURITY] section of the jde.ini file.

Important! When you use unified logon, you need to use the same user ID for the Windows domain and PeopleSoft EnterpriseOne so that the records for each are synchronized. For example, if the user ID for a user in the Windows domain is USER1, the user ID for PeopleSoft EnterpriseOne must also be USER1. If the user IDs are different, unified logon does not work for the user.

Modifying the jde.ini Setting to Enable or Disable Unified Logon

Locate the jde.ini files on the server and on the workstation.

To modify the jde.ini setting to enable or disable unified logon:

1. In the server jde.ini file, add these settings in the [SECURITY] section:

```
[SECURITY]
SecurityMode=0, 1 or 2
```

Value	Description
0	Accepts only users set up for standard sign-in security.
1	Accepts only users set up for unified logon.
2	Accepts users set up for both unified logon and standard sign-in security.

2. In the workstation jde.ini file, add these settings in the [SECURITY] section:

```
[SECURITY]
UnifiedLogon=0 or 1
```

Value	Description
0	Disables unified logon for the workstation. This setting is the default value.
1	Sets unified logon for the workstation.
server_name	Enter the name of the server on which the unified logon server data resides.

Setting Up a Service for Unified Logon

If the enterprise server is not a Windows server, you should set up services for unified logon on the deployment server. The deployment server is always a Windows server.

To set up a service for unified logon:

1. On the deployment server, in Windows Explorer, access the \Unified Logon directory and run the file UniLogonSetup.exe.

The Unified Logon Server Setup form appears. On this form, you define the Windows service for unified logon servers. You can also remove these services on this form.

2. Complete these fields:

- Unified Logon Service Name

Enter the name for the unified logon server.

- EnterpriseOne Port Number

The port number for the unified logon server should match the PeopleSoft EnterpriseOne port number of the server for which you want to set up unified logon.

- Service Executable Filename

Enter the directory path for the unified logon service program.

- Log Filename

Enter the name of the unified logon log file, including the full directory path.

The default user list contains all authenticated network users.

3. To create a custom user list, enter the users or the groups in the Users or User Groups box to add the user information to the unified logon user list.

Note. Generally, the default Windows list of authenticated network users lists users by group.

4. Click the Install Service button to save the service information for the unified logon server.

Removing a Service for Unified Logon

To remove a service for unified logon:

1. Run UniLogonSetup.exe.

The Unified Logon Server Setup form appears.

2. From the Unified Logon Service Name drop-down menu, select a unified logon server, and then click the Uninstall Service button.

CHAPTER 13

Setting Up Solution Explorer Security

This chapter provides an overview of Solution Explorer security and the default security settings and discusses how to configure Solution Explorer security.

Understanding Solution Explorer Security

Use the Security Workbench application (P00950) to set up security for PeopleSoft Solution Explorer. Setting up security correctly ensures that users in the system will have permission to perform only those actions that are essential to their jobs. In addition to setting up security for the PeopleSoft Solution Explorer, you can set security for these features:

- Menu Design
- Menu Filtering
- Favorites
- Fast Path
- Documentation
- OMW Logging

This table summarizes the security settings available for many of the PeopleSoft Solution Explorer features and the description of each:

Security Setting	Description
Secured	Restricts the user from accessing the feature.
View	Allows the user read-only access to the feature, but with no modification capability.
Change	Gives the user full access to the feature with no restrictions on changing, adding, or deleting data.

In PeopleSoft Solution Explorer, you can check the permissions for each feature for any user in the system. You view the settings by signing onto PeopleSoft EnterpriseOne as the user whose settings you want to view, and then click the security button in the status bar of the PeopleSoft Solution Explorer, which launches the PeopleSoft Solution Explorer Security form. Keep in mind that you cannot change the security settings on this form.

Default Security Settings

The Work With Solution Explorer Security Revisions form contains security presets that represent default security settings for different types of users in the system. These user types correspond to novice (Preset One), intermediate (Preset Two), and expert (Preset Three) users. If you click one of these preset buttons, PeopleSoft Solution Explorer changes the Security Revisions default settings for each feature.

Novice users require the most restrictive security settings; expert users require the least restrictive settings. Although you can fine-tune these default settings for a particular individual, using the default settings can free you from the task of manually choosing security setting options for each individual in the system because you can apply them to groups as well as to individual users.

Forms Used to Set Up Solution Explorer Security

Form Name	Form ID	Navigation	Usage
Solution Explorer Security	NA	From any view in PeopleSoft Solution Explorer, double-click the Security button (the lock icon) in the status bar.	Check the permissions for each PeopleSoft Solution Explorer feature.
Work With User/Role Security	W00950A	In PeopleSoft Solution Explorer, enter <i>P00950</i> in the Fast Path and press Enter.	Access the form to set up PeopleSoft Solution Explorer security.
Work with Solution Explorer Security Revisions	W00950H	On Work With User/Role Security, from the Form menu, select Setup Security, and then select Solution Explorer.	Specify security setting options for a user or a group of users.

Configuring Solution Explorer Security

Access the Work with Solution Explorer Security Revisions form.

To configure Solution Explorer security:

1. Enter the user or role ID for which you want to configure security in the User / Role field.
2. Specify security setting options for each feature.
3. If you want to automatically apply settings to a group or to an individual user, select one of these options from the Form menu:
 - Preset One
 - Preset Two
 - Preset Three

Based on the preset button that you clicked, PeopleSoft Solution Explorer automatically selects the default security options.

CHAPTER 14

Employing LDAP in PeopleSoft EnterpriseOne

This chapter provides an overview of Lightweight Data Access Protocol (LDAP) support for PeopleSoft EnterpriseOne and discusses:

- LDAP and PeopleSoft EnterpriseOne relationships.
- Implementing LDAP support in PeopleSoft EnterpriseOne.
- User profiles in LDAP-enabled PeopleSoft EnterpriseOne.
- LDAP-enabled PeopleSoft EnterpriseOne application changes.
- LDAP server-side administration.
- PeopleSoft EnterpriseOne server-side administration.
- Using LDAP bulk synchronization (R9200040).
- Using LDAP over SSL.

Understanding LDAP Support for PeopleSoft EnterpriseOne

LDAP is a protocol that enables system administrators to manage user profiles, such as user IDs and passwords, across multiple application systems. You can enable PeopleSoft EnterpriseOne to use LDAP to manage user profiles and user-role relationships. You can administer an LDAP user profile through an LDAP version 3 compliant directory server. System administrators and end users use a third-party tool to access the LDAP server.

LDAP provides the following benefits:

- Central administration and repository for user profiles.

System administrators can easily maintain user profiles in a single location that serves multiple end user applications, including PeopleSoft EnterpriseOne applications.

- Reduced complexity.

System administrators are not required to use several applications to maintain user profiles. In addition, users are not required to maintain multiple passwords across multiple systems.

LDAP does not support certain user profile information. Such information remains in the domain of the PeopleSoft EnterpriseOne server and must be maintained by the PeopleSoft EnterpriseOne system administrator. Therefore, two distinct and separate user profiles may exist:

- LDAP user profile

This profile includes the user ID, password, and user-role relationship.

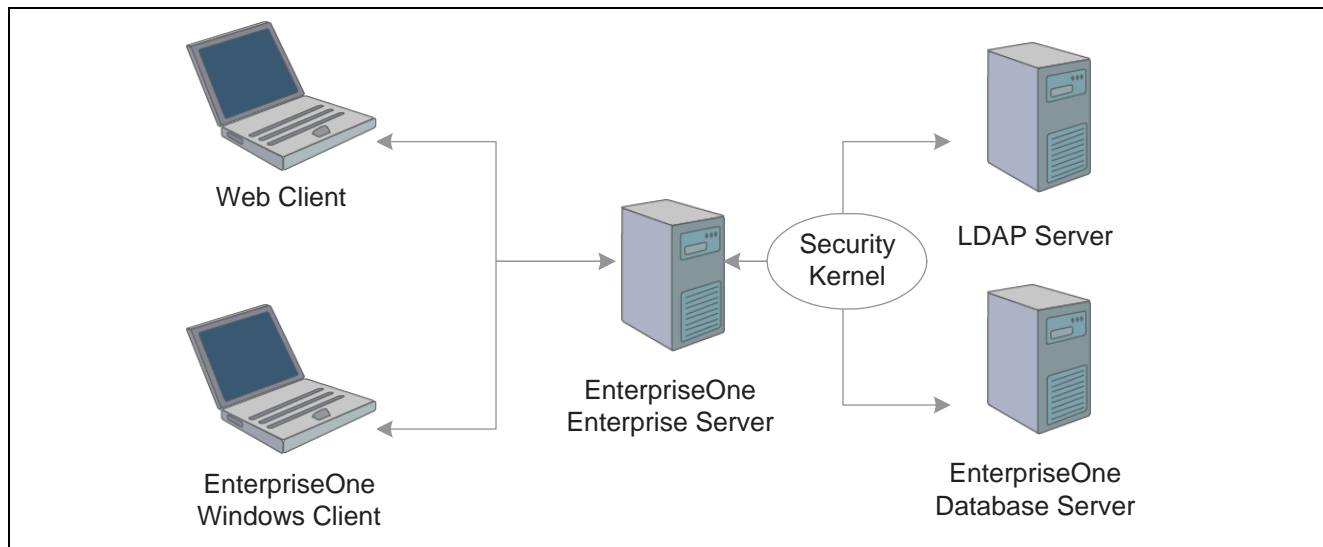
- PeopleSoft EnterpriseOne user profile

The information contained in this profile is stored in the PeopleSoft EnterpriseOne database in the F0092 table. Examples of such information include the date separator, the decimal separator, and so on.

Note. LDAP support does not address single signon functionality that may or may not exist through other PeopleSoft EnterpriseOne functionality.

When LDAP is enabled, all systems (including PeopleSoft EnterpriseOne) are directed to perform user authentication through the LDAP server.

The following illustration shows how LDAP and PeopleSoft EnterpriseOne handle authentication:



LDAP and EnterpriseOne authentication

In this illustration, the EnterpriseOne enterprise server security kernel performs authentication against the LDAP server when LDAP is enabled in the SECURITY section of the jde.ini file of the EnterpriseOne enterprise server. Otherwise, when LDAP is disabled, the security kernel authenticates the user against the EnterpriseOne enterprise server database.

LDAP and PeopleSoft EnterpriseOne Relationships

This section provides an overview of LDAP and PeopleSoft EnterpriseOne relationships and discusses:

- User data managed by LDAP.
- User data managed by PeopleSoft EnterpriseOne.

Understanding LDAP and PeopleSoft EnterpriseOne Relationships

The LDAP system administrator must understand the logical and database-dependent relationships between LDAP and PeopleSoft EnterpriseOne. The system administrator directly or indirectly controls the logical flow of events and where specific data resides, based on the setting of system variables in the PeopleSoft EnterpriseOne enterprise server initialization (jde.ini) file and settings specified in the P95928 application (LDAP Server Configuration Workbench).

The security kernel on the PeopleSoft EnterpriseOne enterprise server is responsible for ensuring the integrity of the security within PeopleSoft EnterpriseOne. If this kernel is not running correctly or cannot locate requisite data, users cannot sign in to PeopleSoft EnterpriseOne. However, when the security kernel is properly configured, the system verifies the user credentials from data within the user profiles. In this case, the following two high-level scenarios are configurable in PeopleSoft EnterpriseOne:

- You can enable LDAP support in the PeopleSoft EnterpriseOne jde.ini file.
- You can set PeopleSoft EnterpriseOne to use user-role relationship data as defined by either PeopleSoft EnterpriseOne or LDAP through the LDAP Server Configuration Workbench application (P95928).

User Data Managed by LDAP

If you configure PeopleSoft EnterpriseOne to use LDAP, the EnterpriseOne security kernel uses the following data stored in the LDAP server:

- User ID
- User password

In addition, if you configure PeopleSoft EnterpriseOne to use LDAP for user-role relationships, the EnterpriseOne security kernel uses the relevant data stored in the LDAP server.

User Data Managed by PeopleSoft EnterpriseOne

The security kernel in PeopleSoft EnterpriseOne requires specific attributes to be defined for all users. These attributes generally include:

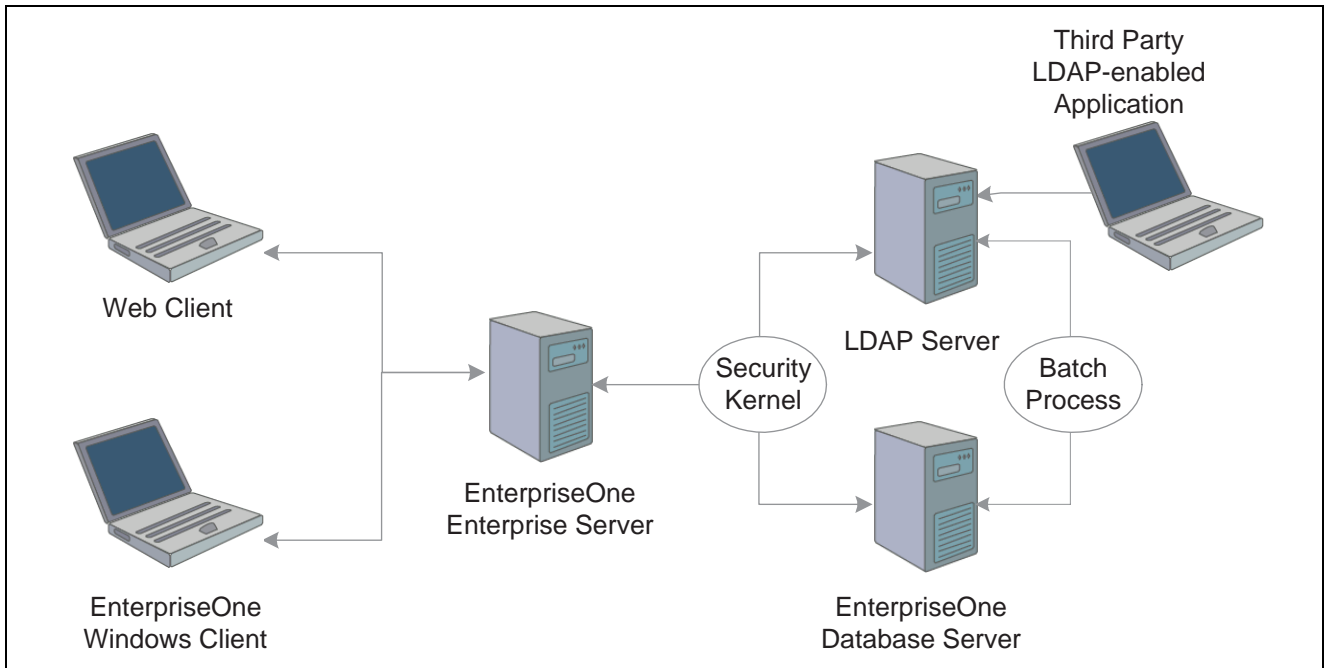
- User ID
- User password
- User-role relationship
- EnterpriseOne proxy user
- Definition of role
- EnterpriseOne user profile settings

The following table explains how this data is managed by LDAP and PeopleSoft EnterpriseOne, as well as how the security kernel uses this information.

Data Category	LDAP	EnterpriseOne	Comment
EnterpriseOne User ID	Yes	Yes F0092	If you enable LDAP in EnterpriseOne, the security kernel validates the user from the LDAP database. If the user ID exists in only one location (either LDAP or EnterpriseOne), the security kernel synchronizes only when the user exists in LDAP and not in EnterpriseOne.
EnterpriseOne User Password	Yes	Yes F98OWSEC	If LDAP is enabled, the user password is always stored in LDAP. If LDAP is not enabled, the user password is stored in the F98OWSEC table in EnterpriseOne.

Data Category	LDAP	EnterpriseOne	Comment
User-Role Relationship	Yes	Yes F95921	<p>If the user-role relationship is defined to execute through EnterpriseOne, the data is stored in the EnterpriseOne database in the F95921 table.</p> <p>If the user-role relationship is defined to execute through LDAP, the user-role relationship is synchronized between systems when the user signs in.</p>
EnterpriseOne Proxy User	No	Yes F98OWSEC	<p>Not managed in LDAP.</p> <p>EnterpriseOne requires each user to have a proxy user specified for access to the EnterpriseOne database. The database user and the associated database password are set by the EnterpriseOne system administrator in the EnterpriseOne security table, F98OWSEC.</p> <p>If there are no valid proxy user settings, the EnterpriseOne security kernel will not validate the user.</p>
Definition of Role	Yes	Yes F0092	The user-role relationship is synchronized from LDAP to the EnterpriseOne database for roles defined in the EnterpriseOne database. However, the system does not synchronize role definitions from LDAP to the EnterpriseOne database.
EnterpriseOne User Profile Settings	No	Yes F00921 and F0092	<p>Not managed in LDAP.</p> <p>EnterpriseOne requires additional user profile attributes that are not generally defined through equivalent attributes in LDAP. Therefore, you can manually set these attributes. You can also specify these values in the default user profile settings for LDAP so that these settings are included for each user that is synchronized from LDAP to PeopleSoft EnterpriseOne.</p> <p>These attributes include:</p> <ul style="list-style-type: none"> • Address Book Number • Decimal Separator • Time Zone • Currency • Date Format

The following illustration shows the user ID and user-role relationship synchronization in LDAP-enabled EnterpriseOne:



User ID and user-role relationship synchronization

This illustration shows the configuration for using an LDAP vendor administration application to add, modify, and delete LDAP user information. In addition, the illustration shows how the system uses the following methods to synchronize user IDs and user-role relationships:

- At user sign-in, the EnterpriseOne security kernel synchronizes the user ID and user-role relationship from LDAP to the EnterpriseOne database.
- EnterpriseOne uses the R9200040 batch process to populate and synchronize user IDs and user-role relationships from LDAP to the EnterpriseOne database.

Implementing LDAP Support in PeopleSoft EnterpriseOne

This section provides an overview of implementing LDAP support in PeopleSoft EnterpriseOne and discusses how to:

- Enable LDAP authentication mode.
- Configure the LDAP server settings.
- Create an LDAP configuration.
- Configure the LDAP to PeopleSoft EnterpriseOne enterprise server mappings.
- Change the LDAP configuration status.

LDAP Support Implementation Overview

You must follow these high-level steps in the specified order to properly configure the PeopleSoft EnterpriseOne enterprise server to support LDAP:

1. Disable LDAP authentication by ensuring that the [LDAP] section of the jde.ini file on the PeopleSoft EnterpriseOne enterprise server contains the following setting:

```
LDAPAuthentication=false
```

2. Use the LDAP Server Configuration Workbench application (P95928) to create an LDAP configuration, configure the LDAP server settings, and configure the LDAP to PeopleSoft EnterpriseOne enterprise server mappings.
3. Use the Configure LDAP Defaults form (W0092M) to enter the required LDAP default user profile settings.

See [Chapter 14, “Employing LDAP in PeopleSoft EnterpriseOne,” LDAP Default User Profile Settings, page 199](#).

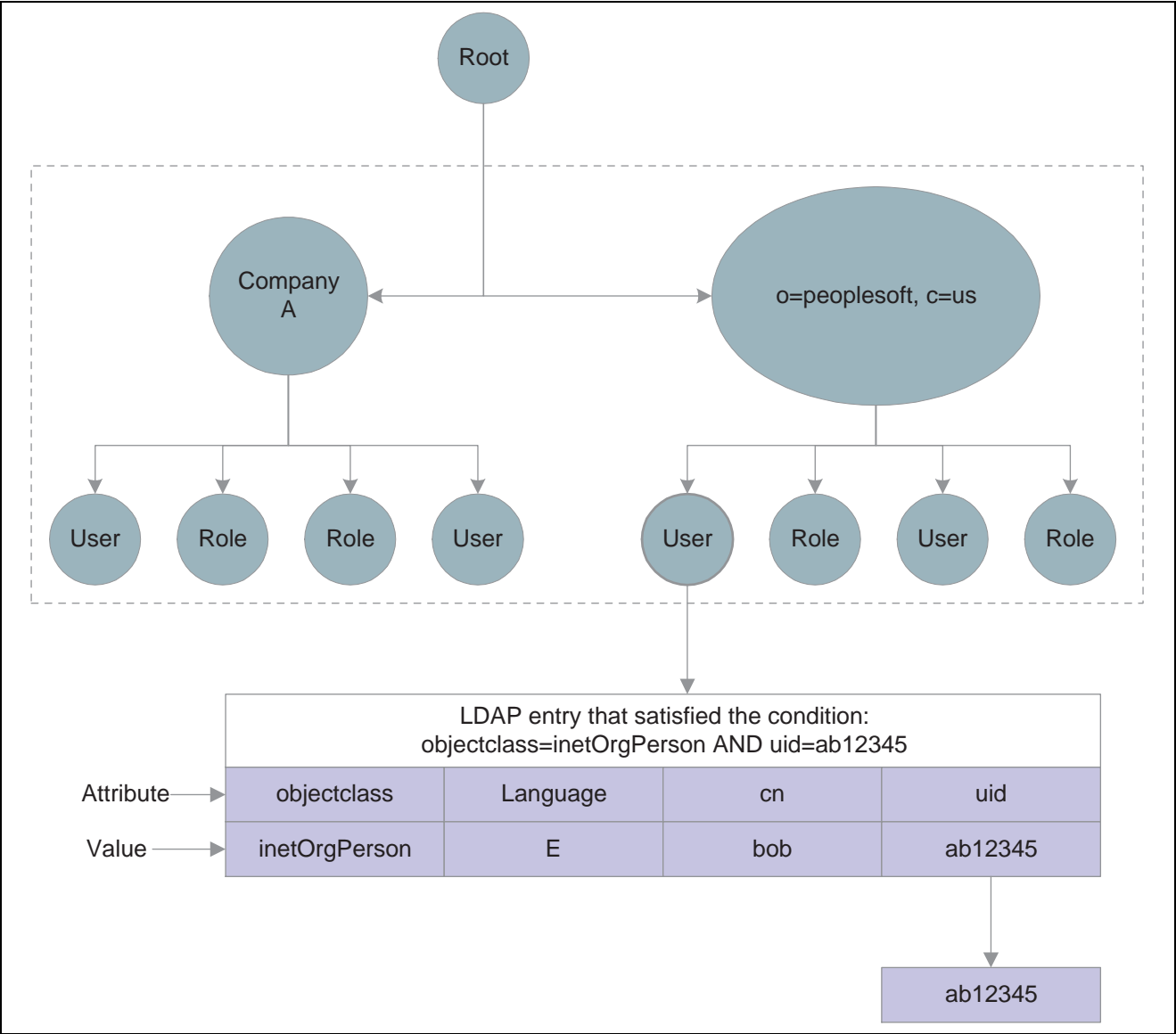
4. Change the LDAP configuration status.
5. Enable LDAP authentication by reversing the setting in step 1:

```
LDAPAuthentication=true
```

6. Restart the PeopleSoft EnterpriseOne enterprise server.

Understanding How PeopleSoft EnterpriseOne Uses LDAP Server Settings

The following diagram shows how PeopleSoft EnterpriseOne uses the LDAP server settings to search for user profiles in the LDAP server:



User ID and user-role search hierarchy in the LDAP server

In this diagram, the PeopleSoft EnterpriseOne application requests a search of the Directory Information Tree for a PeopleSoft user in the United States with an ab12345 user ID. The user can only be found if the following attributes contain valid values:

Attribute	Value
USRSRCHBAS (User Search Base)	o=peoplesoft, c=us
USRSRCHSCP (User Search Scope)	subtree
USRSRCHFLT (User Search Filter)	objectclass=inetOrgperson
USRSRCHATR (User Search Attribute)	uid
E1USRIDATR (EnterpriseOne User ID Attribute)	uid

1. PeopleSoft EnterpriseOne starts the search using the criteria specified in the User Search Base attribute.
2. PeopleSoft EnterpriseOne uses the value in the User Search Scope attribute to determine the scope of the search.
3. PeopleSoft EnterpriseOne uses the following Search Filter parameter to search for the user in LDAP:
`(&((User Search Filter value), ((User Search Attribute value)= "ab12345")))`
4. PeopleSoft EnterpriseOne retrieves the user ID from the EnterpriseOne User ID Attribute.

Enabling LDAP Authentication Mode

The following table describes the LDAP authentication mode setting and values in the PeopleSoft EnterpriseOne enterprise server jde.ini file. When authentication mode is enabled, the system uses LDAP for security authentication. Authentication mode is set in the [SECURITY] section of the jde.ini file.

[Security]

Name	Description
LDAPAuthentication	Set this flag to specify whether LDAP is enabled for security authentication. Values are true (for enabled) and false (for disabled, which is the default).

Creating an LDAP Configuration

Use the LDAP Server Configuration Workbench application (P95928) to create an LDAP configuration. PeopleSoft EnterpriseOne provides two versions of this application. You can use VERSION1 to create a template for creating an LDAP configuration. Create the template by adding specific attributes to the LDAP configuration that can be defined later. This section uses VERSION2 of the application to show all possible attributes that can be mapped in the LDAP configuration.

Note. PeopleSoft EnterpriseOne also provides default templates that you can use to create an LDAP configuration.

From the Application Development menu (GH902), select Object Management, Interactive and Batch Versions, and then double-click Interactive Versions.

To create an LDAP configuration record:

1. On Interactive Versions, enter P95928 in the Interactive Version field and click Find.
2. On Work With Interactive Version, select VERSION2 and then select Run from the Row menu.
3. On Available LDAP Configurations, click Add to add a new configuration record.
4. On LDAP Server Information, complete these fields and then click OK:

Server Configuration Name	Enter a unique name for the server configuration, and then tab to the next field and enter a description.
Enterprise Server Location	The location of the enterprise server.
Enterprise Server Port	The port used to connect to the Enterprise server.
LDAP Server Location	The location (machine name or IP address) of the LDAP server on the network.
LDAP Server Port	The port used to connect to the LDAP server.

LDAP Server Type	Click the Visual Assist button to select the type of LDAP server: Microsoft, IBM, or Domino.
LDAP Admin ID	The administrator's ID for the LDAP server.
LDAP Admin Password	The administrator's password for the LDAP server.
SSL Enabled LDAP Server	Click this option if you want to set up Secure Socket Layer (SSL) communication between PeopleSoft EnterpriseOne security kernel and the LDAP server.

Note. This requires the LDAP server to be configured for SSL.

See [Chapter 14, "Employing LDAP in PeopleSoft EnterpriseOne," Using LDAP Over SSL, page 207.](#)

Role Enabled in LDAP	Click this option if you are managing user-role relationships in LDAP.
-----------------------------	--

Configuring the LDAP Server Settings

Use the LDAP Server Configuration Workbench application (P95928) to configure the LDAP server settings. These settings are in compliance with the standard syntax specified by the LDAP Data Interchange Format (LDIF).

Access the Available LDAP Configurations form.

To configure the LDAP server settings:

1. On Available LDAP Configurations, select a configuration record and then select Values from the Row menu.
2. On LDAP Server Attribute Values, click the search button in the *Enterprise Server Attribute Name* column to select the attributes to include in the LDAP server settings.

After choosing the attributes, you must enter the appropriate LDAP value for the attribute in the LDAP Server Attribute Value column.

3. To configure the standard PeopleSoft EnterpriseOne settings for LDAP server, enter values for the following attributes:

USRSRCHBAS	User search base. This specifies that the system searches for user information at the root of the directory information tree. Use this value to specify the "container" in which to begin the search. For example, USRSRCHBAS=o=PeopleSoft,c=us
USRSRCHFLT	User search filter. This specifies that a search is performed at the base level for the user ID in the LDAP server using the specified criteria. For example, USRSRCHFLT=objectclass=inetOrgPerson If you do not specify this value, no search filtering occurs.
USRSRCHSCP	User search scope. This specifies the level, or scope, at which the system searches for user information. Valid values are: <ul style="list-style-type: none"> • <i>base</i> The query searches only the value you specified in the USRSRCHBAS setting. • <i>subtree</i>

This is the default value. The query searches the value in the Search Base field and all entries beneath it.

- *onelevel*

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

ROLSRCHBAS

Role search base (use only if roles are enabled in LDAP). This specifies that a search is performed at the base level for the UserIDAttri in the LDAP database. For example, `ROLSRCHBAS=o=PeopleSoft,c=us`

ROLSRCHFLT

Role search filter (use only if roles are enabled in LDAP). This specifies that a search is performed at the base level for the role in the LDAP database using the specified criteria. For example, `ROLSRCHFLT=objectclass=groupOfNames`

If you do not specify this value, no search filtering occurs.

ROLSRCHSCP

Role search scope (use only if roles are enabled in LDAP). This specifies the level, or scope, at which the system searches for role information. Valid values are:

- *base*

The query searches only the value you specified in the `ROLSRCHBAS` setting.

- *subtree*

This is the default value. The query searches the value in the Search Base field and all entries beneath it.

- *onelevel*

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

4. When using Secure Socket Layer (SSL) with LDAP server, enter values for the following attributes:

SSLPORT

SSL Port for the LDAP server. Specifies the SSL port on the LDAP server.

CERTDBPATH

Dir path for cert7.db (SSL)

For Windows and UNIX: This specifies the directory path to the cert7.db file (SSL). This file should generally be located in the system\bin32 directory on the PeopleSoft EnterpriseOne enterprise server.

For iSeries: This specifies the directory path and file name for the cert.kdb file on the iSeries-based EnterpriseOne enterprise server machine, for example `/QIBM/USERDATA/ICSS/CERT/SERVER/CERT.KDB`. You should use the Digital Certificate Manager (DCM) to verify the location of the certificate for your installation.

CERTDBCLBL

Do not use this attribute. This is for future use only.

CERTDBPSWD

For iSeries only.

This is the password to the key database. This specifies the password to the key database (files with a “kdb” extension). The key database is used to store a uniquely identified name, or label, associated with the client private key/certificate pair.

SSLTIMEOUT	For iSeries only. This specifies the time-out value for the SSL connection.
5. When using User Self Service (P0092SS) with LDAP-enabled PeopleSoft EnterpriseOne, enter values for the following attributes:	
USRACNTCTL	User Account Control. Specifies the authority attached when creating a user in Active Directory, for example USRACNTCTL=512 creates an enabled user in Active Directory only.
USRADDLOC	User Add Location. Specifies the location in LDAP where users will be added, for example USRADDLOC=0=peoplesoft.
USRCLSHRCY	User Class Hierarchy. Specifies the class hierarchy needed to create a user in LDAP, for example USRCLSHRCY=top, person, organizationalPerson, inetOrgPerson.
ROLADDLOC	Role Add Location (use only if roles are enabled in LDAP). Specifies the location in LDAP that contains the user-role relationship, for example ROLADDLOC=0=peoplesoft.
ROLCLSHRCY	Do not use this attribute. This is for future use only.

Configuring LDAP to PeopleSoft EnterpriseOne Enterprise Server Mappings

Use the LDAP Server Configuration Workbench application (P95928) to configure the LDAP to PeopleSoft EnterpriseOne enterprise server mappings. You can map attributes for users or for user-role relationships, depending upon your configuration.

In addition, if you are entering mappings for user-role relationships, you must also ensure that the LDAP configuration record is enabled for roles.

Access the Available LDAP Configurations form.

To configure LDAP to PeopleSoft EnterpriseOne enterprise server mappings:

1. On Available LDAP Configurations, select a configuration record and then select Mappings from the Row menu.
2. On LDAP Server Mappings, click the search button in the Enterprise Server Attribute Name column to select the attributes to include in the mappings.

After selecting the attributes, you must enter the appropriate LDAP value for the attribute in the LDAP Server Actual Attribute column.

3. To configure the LDAP to PeopleSoft EnterpriseOne enterprise server mappings for a standard setup, enter values for the following attributes:

E1USRIDATR	EnterpriseOne User ID Attribute. Specifies the user ID attribute in LDAP that is used for PeopleSoft EnterpriseOne users. The system uses this attribute when creating users in LDAP during PeopleSoft EnterpriseOne sign-in, for example E1USRIDATR=cn.
USRSRCHATR	User ID Search Attribute. Specifies that the search criteria for the sign-on user ID. This is the value that maps the sign-on user ID in LDAP to the sign-in user ID in PeopleSoft EnterpriseOne, for example USRSRCHATR=cn.

The USRSRCHATR and E1USRIDATR attributes should be mapped to the same value.

EUSRIDATR

Enterprise User ID Attribute. Specifies the User ID attribute in LDAP that is used for Enterprise users. The system uses this attribute to search for Enterprise users for single signon between Enterprise Portal and PeopleSoft EnterpriseOne, for example EUSRIDATR = cn.

ROLNAMEATR

Role Name Attribute (use only if roles are enabled in LDAP). This value maps the role in LDAP to the role in PeopleSoft EnterpriseOne, for example ROLNAMEATR=cn

ROLSRCHATR

Role Search Attribute (use only if roles are enabled in LDAP). Specifies the search attribute for the role in the LDAP server. The system uses this attribute to search LDAP for a list of roles for a user, for example ROLSCHATR=member.

LANGUAGATR

Language Attribute. This specifies the language attribute used within LDAP, for example LANGUAGATR=preferredLanguage

4. When using User Self Service (P0092SS) with LDAP server, enter values for the following attributes:

CMNNAME

Common Name. Specifies the Common Name for a user in LDAP. The system uses this attribute when creating users in LDAP, for example CMNNAME=cn

GIVENNAME

Specifies the Given Name for a user in LDAP it is used when creating users in LDAP especially in Active Directory, for example GIVENNAME=givenName.

SURNAME

Specifies the SUR Name for a user in LDAP. This attribute is used when creating users in LDAP, for example SURNAME=sn.

PASSWORD

Specifies the password associated with the account that you specify with the ConnectDN (distinguished name) of the LDAP server.

OBJCLASS

Object Class. Specifies the Object Class attribute for a user in LDAP it is used when creating users in LDAP, for example OBJCLASS=objectCLASS.

ACNTCTLATR

Account Control Attribute. Specifies the attribute used in Active Directory for user authority in Active Directory, for example ACNTCTLATR=userAccountControl. If the attribute USRACNTCTL=512 is used in conjunction with ACNTCTLATR, the PeopleSoft EnterpriseOne API will create an enabled user in Active Directory only.

ACTNAMEATR

Account Name Attribute. Specifies the attribute used only in Active Directory for creating a signon user account, for example ACNTCTLATR=sAMAccountName.

Changing the LDAP Configuration Status

After you add an LDAP configuration, its default status is non-active. You must change the status to active in order to enable the configuration.

Note. You can only have one active LDAP configuration per port.

Access the Available LDAP Configurations form.

To change the LDAP configuration status:

On the Available LDAP Configurations form, select a configuration record and then select Change Status from the Row menu.

The system changes the status in the Status column to AV (active) or NA (not active).

LDAP Default User Profile Settings

This section provides an overview of the LDAP default user profile settings and discusses how to:

- Review the current LDAP default settings.
- Modify the default user profile settings for LDAP.
- Modify the default role relationships for LDAP.
- Modify the default user security settings for LDAP.

Understanding LDAP Default User Profile Settings

The Configuring LDAP Defaults form (W0092M) enables the system administrator to enter and review the default LDAP user profile settings that are in the PeopleSoft EnterpriseOne database. The system requires the default settings for user profile synchronization.

Note. You must set the default LDAP user profile settings before enabling LDAP authentication in the jde.ini file of the PeopleSoft EnterpriseOne security server.

The Configuring LDAP Defaults form shows whether the following items exist for the default user:

- User profile
- Role relationships
- Data source/system user

Important! Changes made in this application can affect almost all PeopleSoft EnterpriseOne users when synchronizing data from LDAP to the PeopleSoft EnterpriseOne database.

Reviewing the Current LDAP Default Settings

All user values are assigned per user ID the first time, and the first time only, that a user signs in. During this initial sign-in, the values are synchronized from LDAP to the PeopleSoft EnterpriseOne database. The default role relationship is synchronized only if roles are managed by PeopleSoft EnterpriseOne.

To access the Configure LDAP Defaults form, from the Security Maintenance menu (GH9011), select User Management and Advanced Technical Operations, and then double-click Configure LDAP Defaults.

To review the current LDAP default settings:

LDAP Authentication	Indicates whether LDAP authentication is enabled or disabled.
----------------------------	---

Role Management	<p>Indicates whether roles are managed by LDAP. You can enable PeopleSoft EnterpriseOne to manage roles in LDAP through the P95928 application.</p> <p>See Chapter 14, “Employing LDAP in PeopleSoft EnterpriseOne,” Creating an LDAP Configuration, page 194.</p>
User Profile	<p>Indicates whether a default user profile exists within the PeopleSoft EnterpriseOne database. Click this link to modify the default user profile settings.</p> <p>See Chapter 14, “Employing LDAP in PeopleSoft EnterpriseOne,” Modifying the Default User Profile Settings for LDAP, page 200.</p>
Role Relationships	<p>Indicates whether a default role relationship exists. If LDAP authentication is enabled, and if user-role relationships are set to be managed by LDAP, then this option is disabled. This means that the system does not use the default user-role relationship when synchronizing users from LDAP to the PeopleSoft EnterpriseOne database.</p> <p>Click this link to revise the default role relationship.</p> <p>See Chapter 14, “Employing LDAP in PeopleSoft EnterpriseOne,” Modifying the Default Role Relationships for LDAP, page 200.</p>
Data Source/System User	<p>Indicates whether a default data source or system user exists. Click this link to add or change the data source or system user.</p> <p>See Chapter 14, “Employing LDAP in PeopleSoft EnterpriseOne,” Modifying the Default User Security Settings for LDAP, page 201.</p>

Modifying the Default User Profile Settings for LDAP

The default user profile settings are written to the F0092 table. These values are synchronized between LDAP and PeopleSoft EnterpriseOne by the LDAP synchronization mechanisms (security kernel and batch reports).

Access the Configure LDAP Defaults form:

To modify the default user profile settings for LDAP:

1. On Configure LDAP Defaults, click the User Profile link in the Configure Defaults area.
2. On User Profile Revisions, complete the fields to modify the default user profile settings:

Note. The User ID field always contains the default user ID for the LDAP system. This field is disabled and cannot be modified by the system administrator.

Modifying the Default Role Relationships for LDAP

The Configuring LDAP Default form enables you to add roles to the default user.

Note. These values are only synchronized between PeopleSoft EnterpriseOne and LDAP if the role is being managed by PeopleSoft EnterpriseOne.

Access the Configure LDAP Defaults form.

To modify role relationships for LDAP:

1. On Configure LDAP Defaults, click the Role Relationships option in the Configure Defaults area.

Note. If LDAP authentication is enabled and user-role relationships are being managed by LDAP, then this option is disabled. This means that user-role relationship functionality from within PeopleSoft EnterpriseOne is disabled.

2. On Work With Role Relationships, you can highlight a role in either the Assigned Roles or Available Roles menus, and then click the appropriate directional arrow button to add or remove the role for the default user.

Note. The User ID field always contains the default user ID for the LDAP system. This field is disabled and cannot be modified by the system administrator.

Modifying the Default User Security Settings for LDAP

Use the Configuring LDAP Defaults form to add or modify the data source or system user settings.

Access the Configure LDAP Defaults form.

To add or modify user security settings for LDAP:

1. On Configure LDAP Defaults, click the Data Source/System User option in the Configure Defaults area. If the default data source or system user does not exist, the Security Revisions form appears.
2. On Security Revisions, complete the System User field to add or change the data source or system user:

Note. The User ID field always contains the default user ID for the LDAP system. This field is disabled and cannot be modified by the system administrator.

If the default data source is defined, the Work With User Security form appears.

3. To assign a different system user to the data source, on Work With User Security, select the security record and then click Select. On Data Source Revisions, click the search button in the System User field to assign a different system user.
4. To add an additional data source, on Work With User Security, click Add. On Security Revisions, complete the fields as appropriate.

LDAP-Enabled PeopleSoft EnterpriseOne Application Changes

This section provides an overview of the application changes when LDAP is enabled for PeopleSoft EnterpriseOne and discusses the following topics:

- User password changes.
- User Profiles application changes.
- Security Revisions application changes.
- User-Role Relationships Preferences application changes.
- Scheduler application changes.
- User Profile Self-Service application changes.

Understanding Application Changes in LDAP-Enabled PeopleSoft EnterpriseOne

When LDAP is enabled, some of the user profile tasks that you normally perform in PeopleSoft EnterpriseOne, such as adding and deleting users, are disabled. This ensures that users are only managed through LDAP. You must use LDAP to modify these records, not PeopleSoft EnterpriseOne. This section summarizes the changes to the existing PeopleSoft EnterpriseOne menus and applications that result from using LDAP to manage user profile information.

User Password Changes

In PeopleSoft EnterpriseOne, users can change their passwords using the User Default Revisions program. However, when LDAP is enabled, users must contact a system administrator for password changes. If a user attempts to choose the Change Password option in User Default Revisions, the system displays the following error:

Error: LDAP authentication is enabled.

Solution: Users must contact a security administrator to have their passwords changed.

User Profile Revisions Application Changes

The following functions for managing user information in User Profile Revisions (P0092) are disabled:

- Add
- Copy
- Delete

This ensures that users can only be managed through LDAP.

Security Revisions Application Changes

When LDAP is enabled, Security Revisions (P98OWSEC) only allows the system administrator to add or change specific security settings for specified users. This section discusses the features that you can use in this application when LDAP is enabled.

Security Detail Revisions (Single User)

When an existing user is selected for security revisions, the User ID field contains the selected user ID.

On Security Detail Revisions, you can enable the User Status and Allowed Password Attempts fields by clicking on the following corresponding options:

- User Status
- Attempts

Security Detail Revisions (All Users)

When the system administrator clicks the Revise All button from the Form exit in Work With User / Role Profiles, the Security Detail Revisions form appears.

On Security Detail Revisions, you can enable the User Status and Allowed Password Attempts fields for all users by clicking on the following corresponding options:

- User Status

- Attempts

Administration Password Revisions

When the system administrator selects an existing user for Administration Password Revisions using the Admin Password Rev form exit, all fields are disabled.

User-Role Relationships Preferences Application Changes

When LDAP is enabled, the User-Role Relationship Preferences (P95921) application has been modified to enable or disable necessary functionality, depending on whether roles are managed in LDAP. When roles are managed in LDAP, you cannot use PeopleSoft EnterpriseOne to add or delete a role for an individual user. However, you can add roles to the default user for LDAP, which is _LDAPDEFLT. Additionally, you can modify the role expiration date.

If you attempt to add a role to an individual user in PeopleSoft EnterpriseOne, the system displays the following error:

Error: Role Relationship is managed by LDAP.

Similarly, if you attempt to delegate, remove, or add a role for an individual user, the system will display the same error.

Note. When LDAP is enabled and roles are managed in LDAP, you can use a third-party vendor LDAP administration application to add, delete, or modify role relationships for any user.

Scheduler Application Changes

The Scheduler (P91300) application has been modified to allow necessary functionality.

Schedule Job Master

The Schedule Job Master application (P91300) displays a password column which is written to the F91300 table. The password stored in this column provides the password that the Scheduler application uses to connect to the PeopleSoft EnterpriseOne database. The column is only stored for program use and the actual database record contains an encrypted blob that cannot be viewed or decrypted by the system administrator. However, you can enter the password in the Scheduling Advance Options form.

Scheduling Advanced Options

The system administrator must manually enter a password for the Scheduler application.

Scheduled Password	<p>The system administrator must assign a password for the Scheduler program to use when connecting to the PeopleSoft EnterpriseOne database.</p> <p>The Scheduler kernel validates the user ID and password stored in F91300. The job cannot be launched if the validation fails. Therefore, if the user changes their password after the job is scheduled, the job cannot be launched. In such cases, the user must use P91300 to revise the job.</p>
--------------------	---

User Profile Self-Service Application Changes

When LDAP is enabled, the User Profile Self-Service (P0092SS) application has been modified so that you can add user IDs, passwords, and user-role relationships in LDAP.

You can find additional information in the PeopleSoft EnterpriseOne self service application guides.

LDAP Server-Side Administration

This section assumes that PeopleSoft EnterpriseOne is using the LDAP server for user profile administration. Using a third-party tool to access the LDAP server, the system administrator can manually add, modify, or delete attributes of user profiles, as shown in the following table:

User Profile Attribute	Action	Notes
User ID and Password Values	Add Modify Delete	<p>The user ID and password values must be alphanumeric and cannot exceed 10 characters in length. Unicode is supported.</p> <p>At sign-in, logic on the PeopleSoft EnterpriseOne server automatically performs one-way, real-time synchronization of user IDs with the LDAP server.</p> <p>System administrators can run a separate batch program on the PeopleSoft EnterpriseOne enterprise server to initially migrate user IDs from LDAP to the PeopleSoft EnterpriseOne database.</p> <p>See Chapter 14, “Employing LDAP in PeopleSoft EnterpriseOne,” Modifying the Default User Security Settings for LDAP, page 201.</p>
User-Role Relationship	Add Modify Delete	<p>At sign-in, logic on the PeopleSoft EnterpriseOne server will automatically perform one-way real-time synchronization of these values with the LDAP server.</p> <p>System administrators can run a separate batch program on the PeopleSoft EnterpriseOne server to initially migrate this data from LDAP to the PeopleSoft EnterpriseOne database.</p> <p>Only valid PeopleSoft EnterpriseOne user-role relationships will be synchronized from LDAP to the PeopleSoft EnterpriseOne database.</p> <p>See Chapter 14, “Employing LDAP in PeopleSoft EnterpriseOne,” PeopleSoft EnterpriseOne Server-Side Administration, page 205.</p>
Role Definitions	Add Modify Delete	<p>The system administrator must manually set up role definitions in LDAP and PeopleSoft EnterpriseOne because there is no automated method to synchronize this data.</p>

PeopleSoft EnterpriseOne Server-Side Administration

System administrators must perform certain tasks or functions that fall into the following categories:

- Tasks that are not supported by LDAP.
- Tasks that are not synchronized automatically.
- Tasks that are not synchronized through a batch process.

You can use the User Security application (P98OWSEC) to perform these tasks on the PeopleSoft EnterpriseOne server.

EnterpriseOne Server Function	Action	Notes
Configure EnterpriseOne Server to use LDAP	Enable Disable	System administrators must configure jde.ini to enable or disable LDAP functionality.
Proxy User ID and Password	Add Modify Delete	Required to set proxy values not supported by LDAP. Proxy information is used to connect to the database. It includes database proxy user name, proxy user password, and data source name (proxy key).
User-Role Relationship	Add Modify Delete	Required if user-role relationships are managed in PeopleSoft EnterpriseOne.
User-Role Relationship Attributes	Add Modify Delete	Required to set attributes not supported by LDAP, such as *ALL and Expiration Dates, when you manage role relationships in LDAP.
User Status	Modify	Allowed statuses include: <ul style="list-style-type: none"> • Enabled • Disabled There is no automatic or batch synchronization between LDAP and PeopleSoft EnterpriseOne.
Allow Login for EnterpriseOne User	Enable Disable	When enabled, a PeopleSoft EnterpriseOne user is allowed to enter profile information on the LDAP server which performs validation, and if successful, enables the user to access PeopleSoft EnterpriseOne applications.

EnterpriseOne Server Function	Action	Notes
Maximum Number of Login Attempts	Modify	The number of sign-on attempts a user can make before that user profile is disabled.
Role Definition	Modify	You must always define the role definition in PeopleSoft EnterpriseOne, regardless of any LDAP considerations.

Using LDAP Bulk Synchronization (R9200040)

The LDAP directory server contains user profile data for multiple users. This data must also exist in the PeopleSoft EnterpriseOne database server. The LDAP Bulk Synchronization report (R9200040) enables the system administrator to perform bulk synchronization of database records between the LDAP directory server and the PeopleSoft EnterpriseOne directory server. In a typical scenario, this data will not exist on the LDAP server. Therefore, this report is beneficial to the system administrator because it automatically populates default data that is required for PeopleSoft EnterpriseOne functionality.

Note. Data is only written to the PeopleSoft EnterpriseOne database tables if the corresponding data exists on the LDAP directory server.

Running the report synchronizes user data obtained from the LDAP directory server with the following PeopleSoft EnterpriseOne database tables:

Table	Description
F0092	Library List User
F00921	User Display Preferences
F98OWSEC	Security settings
F95921	Role Relationship
F0093	Library List Control
F00922	User Display Preferences Tag File
F00924	User Install Package
F00926	Anonymous User Access Table
F9005	Variant Description - Control Tables
F9006	Variant Detail - Control Tables
F00927	E1 Users PIM Information

Example: LDAP Bulk Synchronization (R9200040)

The following example shows the PDF output of the LDAP Bulk Synchronization (R9200040) report. Note that if the data on the LDAP server is already the same as the corresponding data on the PeopleSoft EnterpriseOne database server, the report lists the affected tables and shows a zero record synchronization, which indicates the data exists, but is identical.

Worldwide Company				
Synchronize the LDAP and EnterpriseOne Database				
<u>Table Name</u>	<u>Records Added</u>	<u>Records Deleted</u>	<u>Records Failed</u>	<u>Synchronization Status</u>
F0092	17	219	0	Successful
F00921	17	219	0	Successful
F98OWSEC	34	148	0	Successful
F95921	43	272	0	Successful
F9312	0	0	0	Successful
F0093	0	133	0	Successful
F00922	0	13	0	Successful
F00924	0	3	0	Successful

LDAP Bulk Synchronization report output

Using LDAP Over SSL

This section provides an overview on how to enable LDAP authentication over Secure Socket Layer (SSL). You can establish a secure LDAP connection between the PeopleSoft EnterpriseOne server and the LDAP server.

Enabling LDAP Authentication Over SSL for Windows and UNIX

The PeopleSoft EnterpriseOne server uses Netscape's certificate database, cert7.db. You can obtain a cert7.db using the PKCS Utilities distributed by Netscape. Refer to Netscape's documentation for more information on obtaining and using the PKCS Utilities.

To establish the secure connection between the PeopleSoft EnterpriseOne application server and the LDAP server you will need the following:

- Cert7.db certificate database from Netscape.
- A server certificate for the LDAP server.
- The trusted root certificate from the certificate authority (CA) that issues the server certificate.

To enable LDAP authentication over SSL:

1. Follow the documentation for your directory server to add the server certificate to the directory server.
2. Using Netscape's PKCS Utilities, add the CA's trusted root certificate to the cert7.db certificate database.
3. Enable SSL for the LDAP configuration using the LDAP Server Configuration Workbench application.
4. Specify the SSL parameters.

See [Chapter 14, "Employing LDAP in PeopleSoft EnterpriseOne," Configuring the LDAP Server Settings, page 195.](#)

5. Restart the PeopleSoft EnterpriseOne server.

Enabling LDAP Authentication Over SSL for iSeries

The EnterpriseOne server uses IBM certificate database (.kdb) to store certificates on iSeries. You can create a certificate database on iSeries using Digital Certificate Manager.

Establishing the secure connection between the PeopleSoft EnterpriseOne application server and the LDAP server requires the following:

- IBM Certificate store (.kdb) certificate database.
- A server certificate for the LDAP server.
- The trusted root certificate from the certificate authority (CA) that issues the server certificate.

To enable LDAP authentication over SSL:

1. Follow the documentation for your directory server to add the server certificate to the directory server.
2. Use Digital Certificate Manager to add and export the CA's trusted root certificate to the certificate database (.kdb file).
3. Enable the SSL for the LDAP configuration using the LDAP Server Configuration Workbench application.
4. Specify the SSL parameters.

See [Chapter 14, "Employing LDAP in PeopleSoft EnterpriseOne," Configuring the LDAP Server Settings, page 195.](#)

5. Restart the EnterpriseOne server.

CHAPTER 15

Understanding PeopleSoft EnterpriseOne Single Signon

This chapter provides an overview of PeopleSoft EnterpriseOne single signon and discusses:

- PeopleSoft authenticate token.
- Understanding nodes.
- How a node validates an authenticate token.
- How single signon works.

PeopleSoft EnterpriseOne Single Signon Overview

PeopleSoft EnterpriseOne single signon enables users that are signed in to either Enterprise Portal or PeopleSoft EnterpriseOne Collaborative Portal to access PeopleSoft EnterpriseOne applications without re-entering a user ID and password. Single signon provides the following benefits:

- Allows users to navigate between Enterprise Portal and PeopleSoft EnterpriseOne applications seamlessly.
- Increases the security for the PeopleSoft EnterpriseOne system since passwords are no longer passing between different sub-systems in PeopleSoft EnterpriseOne.

Note. PeopleSoft EnterpriseOne does not support single signon between PeopleSoft EnterpriseOne applications and third-party applications.

PeopleSoft Authenticate Token

PeopleSoft EnterpriseOne uses an authenticate token to achieve single signon. The authenticate token contains criteria that grants access to a PeopleSoft EnterpriseOne application from Enterprise Portal or PeopleSoft EnterpriseOne Collaborative Portal.

When a user signs on to either system, an authenticate token is generated after successful authentication. When the user accesses an EnterpriseOne application, the system uses the generated token to validate the user against the EnterpriseOne security server. As a result, the user does not have to manually sign on to the system again.

For security purposes, all authenticate tokens expire after a certain period of time and contain a digital signature that ensures the token cannot be tampered with.

An authenticate token contains the following properties:

UserID	The user ID of the user to which the server issued the token. When the browser submits this token for single signon, this is the user that the application server signs in to the system.
Language Code	The language code of a user. When the system uses a token for single signon, it sets the language code for the session based on this value.
Date and Time Issued	The date and time the token was first issued. The system uses this field to enforce a timeout interval for the single signon token. Any application server that accepts tokens for signon compares this value against the amount of time set in the application server to accept tokens. The value is in Greenwich Mean Time (GMT) so it does not matter which time zone the application server is in.
<hr/> Note. The system date and time is used to validate the expiration of a token. Changing these values on the server may expose a potential security risk. <hr/>	
Issuing Node Name	The name of the system that issued the token.
Signature	<p>A digital signature that the application server (node) uses to validate the token for single signon by ensuring that the token has not been tampered with since it was originally issued. The system issuing the token generates the signature by concatenating the contents of the token (all the fields that appear in this table) with the message node password for the local node. Then the system hashes the resulting string using the SHA1 hash algorithm. For example ("+" means concatenation),</p> <p>signature = SHA1_Hash (UserID + Lang + Date Time issued + Issuing Node Name+ Issuing Node Password)</p> <p>There is only one way to derive the 160 bits of data that make up the signature, and that is by hashing exactly the same User ID, Language, Date Time, Issuing System, and node password.</p>

Understanding Nodes

A node is a machine that can generate or validate an authenticate token. The node contains properties that you set to control security and specify parameters for which tokens the node will accept. The system stores the node properties in the database or the jde.ini files, depending on your particular setup.

Each node contains the following properties:

Node name	A logical name associated with this node. The length of the node name cannot exceed 15 characters.
Node password	Each node has a password which is known only by the system administrator. It serves as a key to ensure that the token does not get tampered with after it is generated.
Physical machine name	The physical machine name in which the node resides.
Trusted nodes list	This property contains the list of nodes that can be trusted by this node. For security purposes, only tokens that are generated by predefined machines can be accepted. These predefined machines are called trusted nodes.

The trusted node is one way, for example if you set up node A to trust node B, it does not mean that node B trusts node A.

Token lifetime properties

When validating a token, the node checks the time the token was issued against the amount of time that you set in the token lifetime properties. For example, if you set the token lifetime for six hours, and the node receives a token that was originally issued seven hours prior, the node will not accept the token. You can use the following two properties to specify the token lifetime:

- Regular token lifetime

This property specifies the expiration time for a regular token. A regular token gives a user the authority to run a regular short-run process, such as a business function. The default value for this property is 12 hours.

- Extended token lifetime

This property specifies the expiration time for an extended token. An extended token gives a user the authority to run a long-run process, such as a UBE, after it is issued. The default value for this property is 30 days.

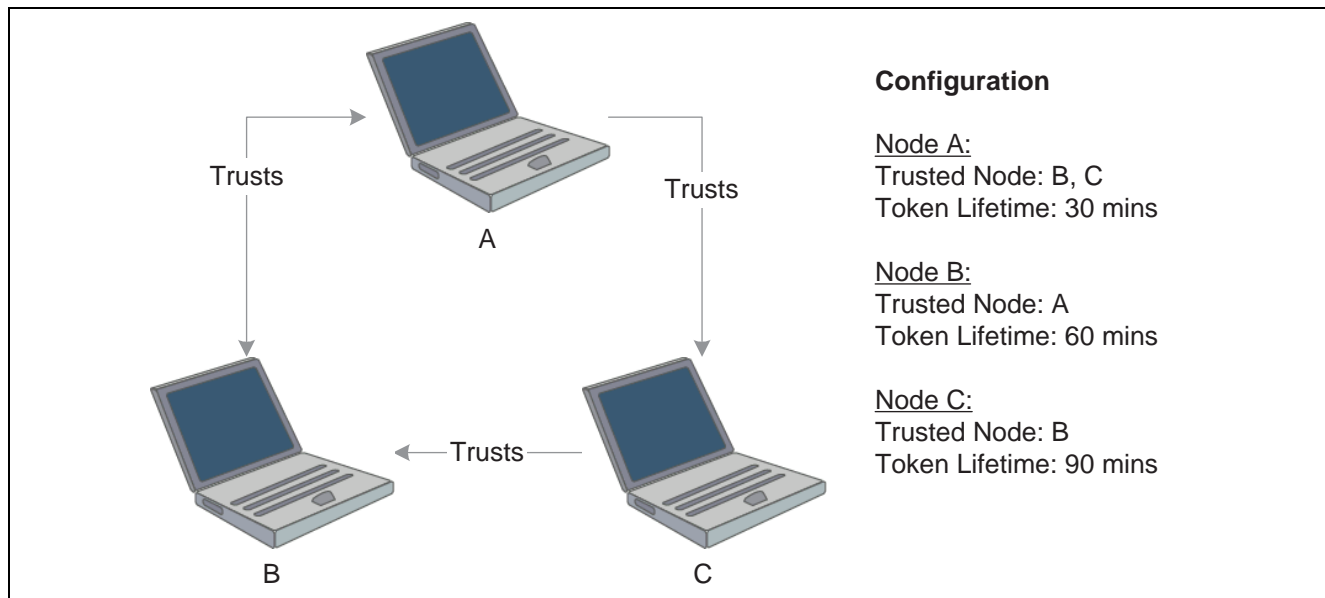
Note. On the iSeries platform, GMT time calculation does not take into account daylight savings time. Consequently, there can be a one hour difference in GMT time calculation between tokens generated on iSeries and Windows platforms. If you set the token timeout values as 12 hours (the default) or longer, you will notice this issue in sessions running for longer than 11 hours. If you set the token timeout values as less than one hour, then the tokens generated on Windows will automatically expire on iSeries. To resolve this issue, on the iSeries server, you should change the QUTCOffset value manually whenever there is a change in daylight savings time to ensure proper calculation of GMT time.

How a Node Validates an Authenticate Token

The node validates an authenticate token by checking the following:

- Whether the token signature has been changed.
- Whether the token is expired.
- Whether the token is generated by a trusted node.

The following illustration is an example of token validation in a multiple node setup:



Token validation in a multiple node setup

According to this configuration, the following tokens are validated by a node:

- Node A validates tokens generated by node B and node C if received less than 30 minutes from generation.
- Node B validates tokens generated by node A if received less than 60 minutes from generation.
- Node C validates tokens generated by node B if received less than 90 minutes from generation.

The following tokens are not validated by a node:

- Node B cannot accept a token generated by node C, even though node C trusts node B.
- A node will not accept a token if the time between its generation and reception by the node is greater than the token lifetime set for that node. For example, node A cannot accept a token from node B if the token was generated more than 30 minutes prior to being received by node A.

Note. No node will accept a token if its signature has been changed. The system verifies this by comparing the token signature and the hash value of the token body.

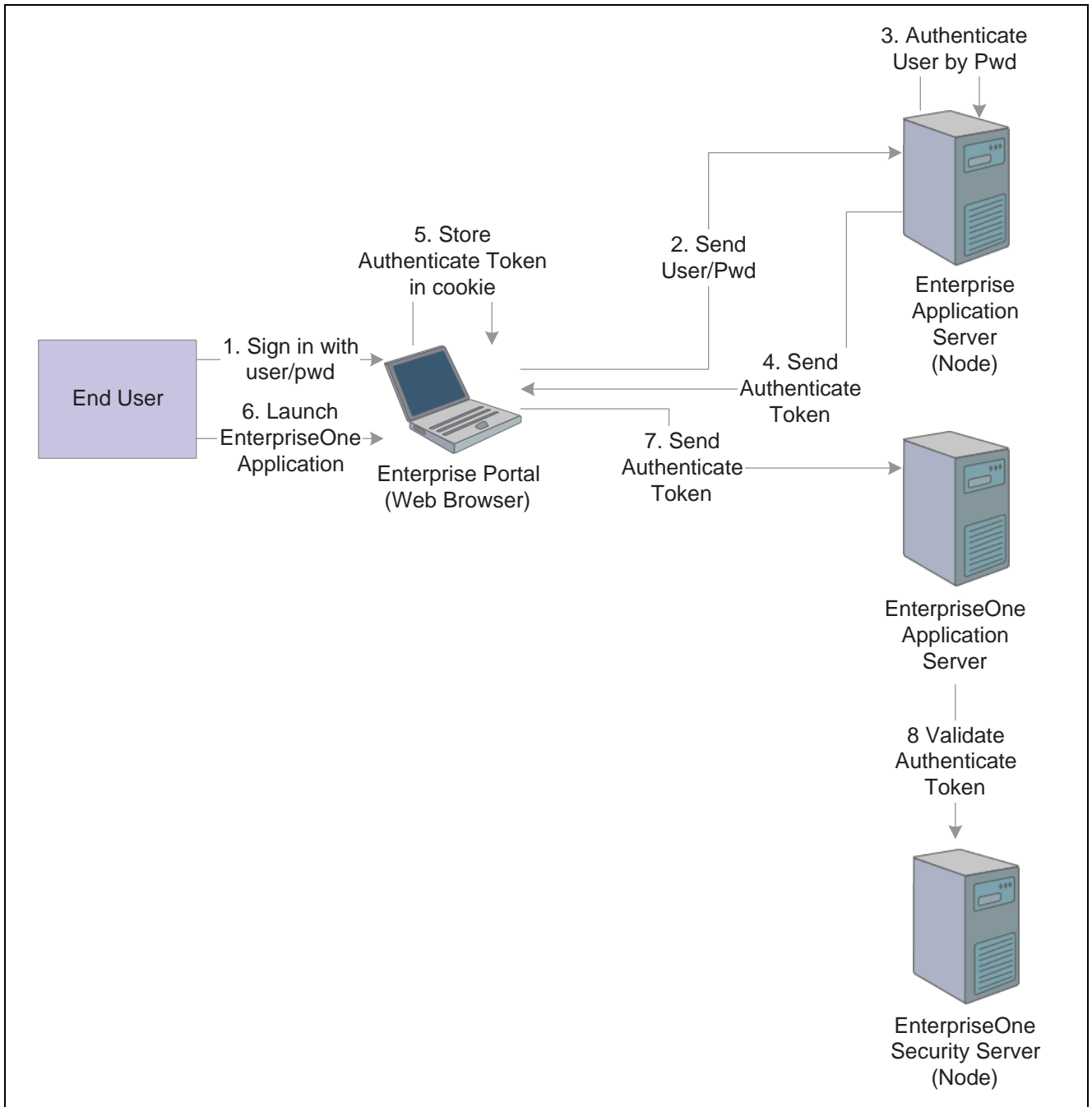
How Single Signon Works

This section discusses how single signon works in the following scenarios:

- Launching an PeopleSoft EnterpriseOne application from Enterprise Portal.
- Launching an PeopleSoft EnterpriseOne application from PeopleSoft EnterpriseOne Collaborative Portal.

Launching an PeopleSoft EnterpriseOne Application from Enterprise Portal

The following illustration and steps explain how single signon works when an end user signs in to Enterprise Portal and launches an PeopleSoft EnterpriseOne application:



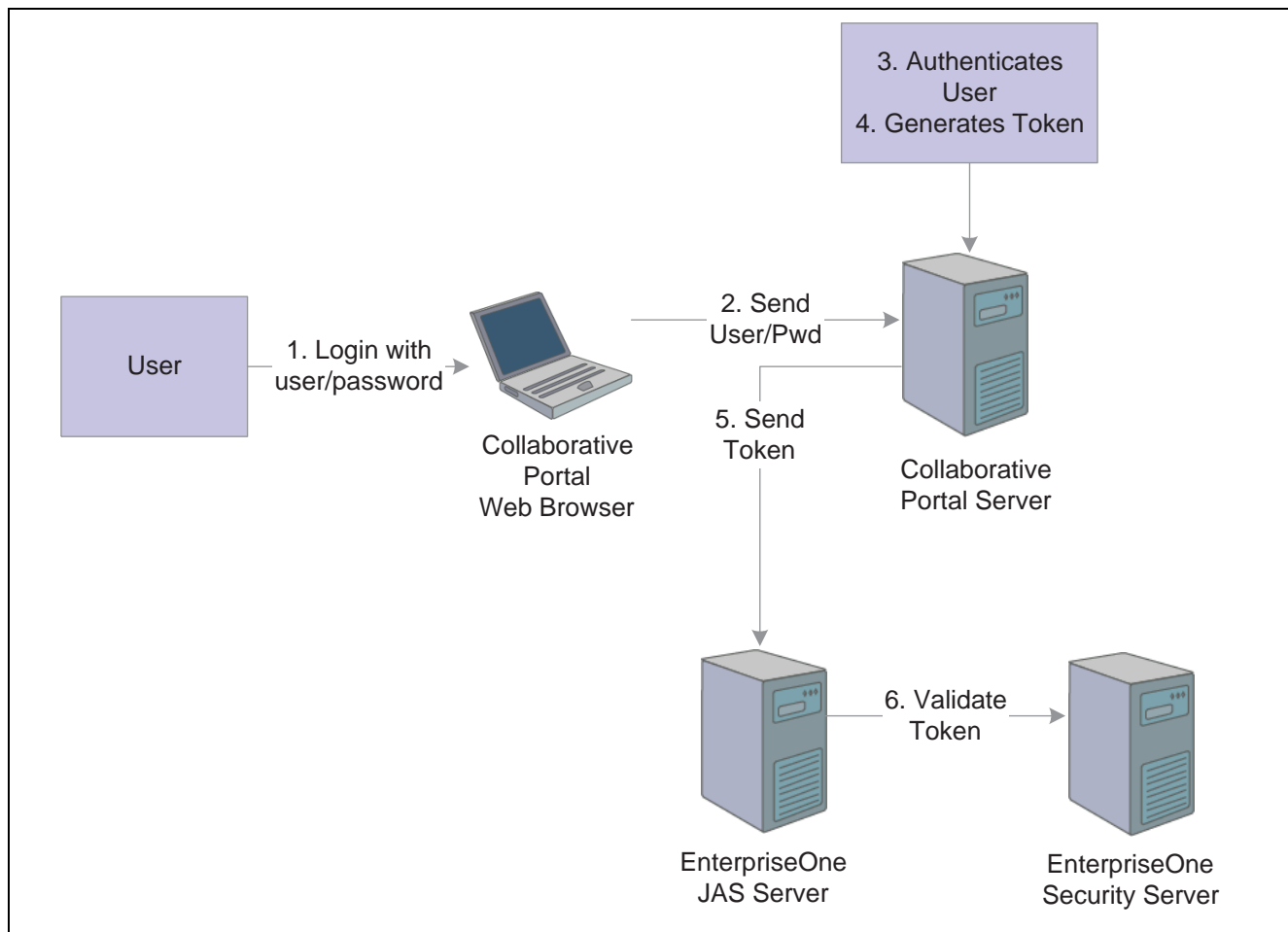
Single signon between Enterprise Portal and PeopleSoft EnterpriseOne applications

1. The user signs in to Enterprise Portal in a Web browser using an Enterprise user ID and password.
2. The Web browser sends the user ID and password to the Enterprise application server (node).
3. The Enterprise application server authenticates the user credentials and generates an authenticate token.
4. The Enterprise application server delivers a cookie containing an authenticate token to the Web browser.
5. The Web browser stores the cookie on the local machine.
6. The end user tries to launch an PeopleSoft EnterpriseOne application through Enterprise Portal.
7. The Enterprise Portal sends the authenticate token to the PeopleSoft EnterpriseOne application server.

8. The PeopleSoft EnterpriseOne application server validates the token (through the PeopleSoft EnterpriseOne security server).

Launching an PeopleSoft EnterpriseOne Application from PeopleSoft EnterpriseOne Collaborative Portal

The following illustration and steps explain how single signon works when an end user signs in to PeopleSoft EnterpriseOne Collaborative Portal and launches a PeopleSoft EnterpriseOne application:



Single Signon Between PeopleSoft EnterpriseOne Collaborative Portal and PeopleSoft EnterpriseOne applications

1. The user signs in to PeopleSoft EnterpriseOne Collaborative Portal through a web browser using an PeopleSoft EnterpriseOne user ID and password.
2. The system sends the user ID and password to the Collaborative Portal.
3. Collaborative Portal authenticates the user ID and password against either LDAP, PeopleSoft EnterpriseOne tables, or WebSphere security.
4. A token is generated for the user ID.
5. When single signon is required for PeopleSoft EnterpriseOne, the token is sent to either a JAS Server or an PeopleSoft EnterpriseOne application server.
6. The PeopleSoft EnterpriseOne security server validates the token and grants access to the PeopleSoft EnterpriseOne application.

CHAPTER 16

Setting Up EnterpriseOne Single Signon

This chapter provides an overview of the settings for the single signon configuration and discusses how to:

- Set up a node configuration.
- Set up a token lifetime configuration record.
- Set up a trusted node configuration.
- Configure single signon for a pre-EnterpriseOne 8.11 release.
- Configure single signon without a security server.
- Configure single signon for Collaborative Portal.
- Configure single signon for portlets.
- Configure single signon between Enterprise Portal and EnterpriseOne.

Default Settings for Single Signon Node Configuration

By default, when there is no configuration table specifications in the system and no configurations in the jde.ini file, a security server uses the following settings for node information:

Logical Node Name	_GLOBALNODE
Physical machine name	N/A (the default settings are all the same independent of the physical machine that it is residue in)
Regular token timeout	12 hours
Extended token timeout	30 days
Trusted node	_GLOBALNODE

As a result, the EnterpriseOne system will generate a token with node name _GLOBALNODE, and it will only accept a token with node name _GLOBALNODE.

Note. Using default settings may expose a potential security risk. Thus, it is highly recommend to overwrite the single signon settings using the single signon configuration applications discussed in this section.

Setting Up a Node Configuration

This section provides an overview of the single signon configurations and discusses how to:

- Add a node configuration.

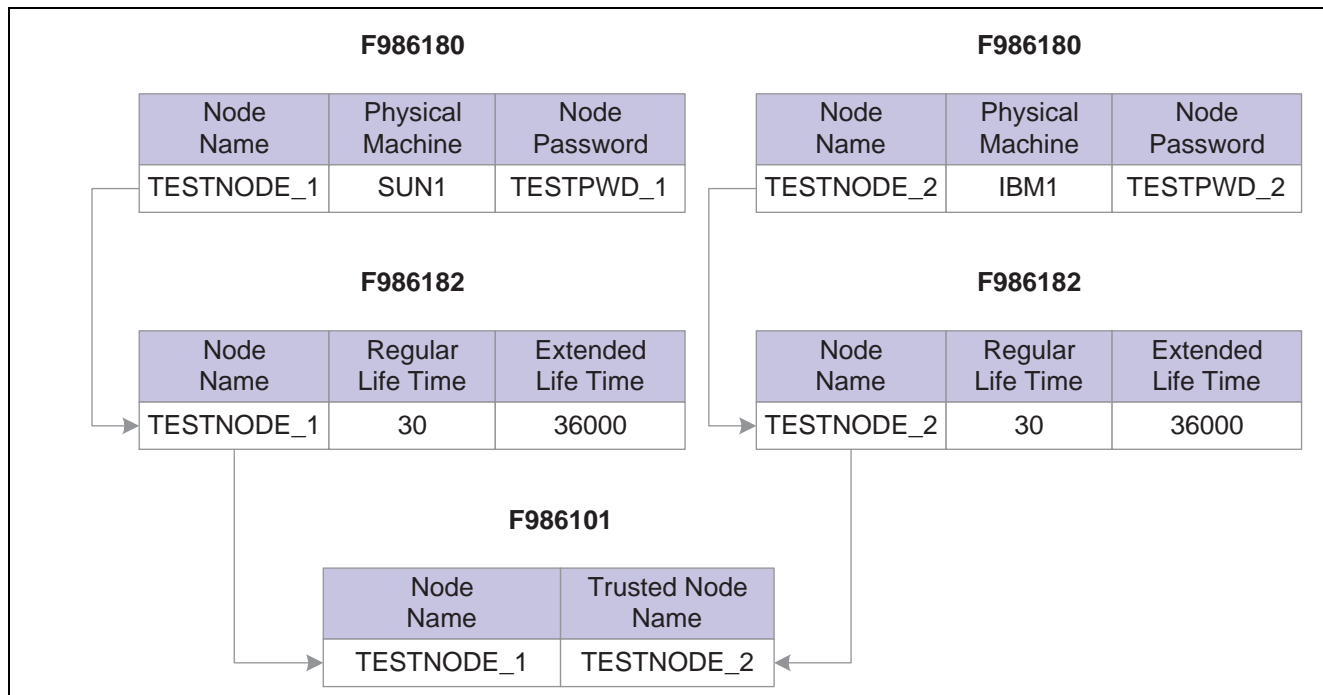
- Revise a node configuration
- Change the status of a node.
- Delete a node configuration.

Understanding Single Signon Configurations and Their Relationships

In EnterpriseOne 8.11, the node configurations are stored in a database. The node lifetime configuration is the configuration for the existing node, and the nodes in the trusted node configuration must have an existing node that has the lifetime configurations. The node properties are stored in the following three database tables:

- Node Configuration Table (F986180). This table contains the information of a node in the single signon environment, such as the node name, description, machine name, node status (active/inactive), and the password.
- Node Lifetime Configuration Table (F986182): This table contains the lifetime information for an existing node. The node lifetime configuration information, such as the node name, regular token lifetime, and extended token lifetime.
- Trusted Node Configuration Table (F986181): This table contains the trust relationship between two nodes.

The following diagram shows the relationship among these tables:



Single signon table relationships

This configuration requires that you configure the single signon settings in the following order:

1. Set up node information.
2. Set up node lifetime.
3. Establish the trust between nodes.

You should delete the single signon settings in the following order:

1. Delete the trusted node relationship.
2. Delete the lifetime.
3. Delete the node information.

Alternatively, you can delete the node information directly by deleting the node record in the F986180 table. The system will automatically delete the record's corresponding entries in the Node Lifetime (F986181) and Trusted Node (F986182) tables.

Adding a Node Configuration

Access the SSO Environment Configuration Tools form. In Solution Explorer, select System Administration Tools (GH9011), User Management, User Management Advanced and Technical Operations, and then double-click SSO Environment Configuration Tools.

To add a node configuration:

1. On SSO Environment Configuration Tools, click the Single Signon Node Configuration link.
2. On Work With Node Configuration, click Add.
3. On SSO Node Configuration Revisions, complete these fields:

Node Name	Enter a logical name associated with this node. The length of the node name cannot exceed 15 characters.
Node Description	Enter a description of the node.
Machine Name	Enter the physical machine name where the node resides.
Node Status	Choose whether the node is active or inactive.
Node Password	Enter a password for the node. The password ensures that tokens that are generated from the node do not get tampered with.
Verify Node Password	Re-enter the password.

Revising a Node Configuration

Access the Work With Node Configuration form.

To revise a node configuration:

1. On Work With Node Configuration, select a node and then click Select.
2. On SSO Node Configuration Revision, modify the appropriate fields.

Changing the Status of a Node

Access the Work With Node Configuration form.

Work With Node Configuration form.

To change the status of a node:

On Work With Node Configuration, select the node and then from the Row menu, choose Active/Inactive to change the status of the node.

Deleting a Node Configuration

Deleting an existing node configuration results in the removal of its lifetime configuration and trusted node configuration records in F986181 and F986182 respectively.

Access the Work With Node Configuration form.

To delete a node configuration:

1. On Work With Node Configuration, select the node that you want to delete and click Delete.
A warning message appears informing you of the corresponding records that are deleted when you delete a node configuration.
2. Click OK to delete the node configuration.

Setting Up a Token Lifetime Configuration Record

This section discusses how to:

- Add a token lifetime configuration record.
- Delete a token lifetime configuration record.

Adding a Token Lifetime Configuration Record

A node that has a token lifetime configuration always generates a pair of lifetime configuration records—one for the regular token and one for the extended token. The trusted node configuration depends on the token lifetime configuration. You can add a pair of new token lifetime configuration records for an existing node.

Access the SSO Environment Configuration Tools form. In PeopleSoft Solution Explorer, select System Administration Tools (GH9011), User Management, User Management Advanced and Technical Operations, and then double-click SSO Environment Configuration Tools.

To add a token lifetime configuration record:

1. On SSO Environment Configuration Tools, click the Single Signon Token Lifetime Configuration link.
2. On Work With Token Lifetime Configuration, click Add.
3. On Token Lifetime Configuration Revision, complete these fields:

Regular Token Lifetime	Specify the expiration time for a regular token. The default value for a node is 720 minutes (12 hours).
Extended Token Lifetime	Specify the expiration time for an extended token. The default value is 4320 minutes (three days). However, the recommended value for this setting is 43,200 minutes (30 days).

Deleting a Token Lifetime Configuration Record

If one token lifetime configuration record is deleted, then another token lifetime configuration for the same node and the trusted node configurations that have this node in it will be deleted as well.

Access the Work With Token Lifetime Configuration form.

To delete a token lifetime configuration record:

On Work With Token Lifetime Configuration, select a node and then click the Delete button.

Note. A dialog box appears warning you that if you delete this record, the system will delete the extended and regular token lifetime configuration records and the trusted node configuration records of this node.

Setting Up a Trusted Node Configuration

This section discusses how to:

- Add a trusted node configuration.
- Delete a trusted node configuration.

Adding a Trusted Node Configuration

The nodes that you add to a new trusted node configuration must already be defined and have token lifetime configuration records.

Access the SSO Environment Configuration Tools form. In PeopleSoft Solution Explorer, select System Administration Tools (GH9011), User Management, User Management Advanced and Technical Operations, and then double-click SSO Environment Configuration Tools.

To add a trusted node configuration:

1. On SSO Environment Configuration Tools, click the Single Signon Trusted Node Configuration link.
2. On Work With Trusted Node Configuration, click Find, select a record, and then click Add.
3. On Trusted Node Configuration Revision, enter a node in the Node Name field and then click OK.

Deleting a Trusted Node Configuration

Access the Work With Trusted Node Configuration form.

To delete a trusted node configuration:

On Work With Trusted Node Configuration, select a record and then click Delete.

Configuring Single Signon for a Pre-EnterpriseOne 8.11 Release

This section provides an overview of single signon for a pre-EnterpriseOne 8.11 release and discusses:

- jde.ini file node setting modifications for single signon.
- Sample jde.ini node settings for single signon.

Understanding Single Signon for a Pre-EnterpriseOne 8.11

EnterpriseOne 8.11 stores single signon node configuration information in new tables (F986180, F986181 and F986182). These tables are not available in pre-8.11 releases (such as release 8.94). However, you can still configure single signon for the pre-release through single signon node settings in the jde.ini file.

jde.ini file Node Setting Modifications for Single Signon

PeopleSoft EnterpriseOne comes with standard default settings for single signon. If you do not want to accept the default settings, you can overwrite the default single signon node settings by configuring the jde.ini file.

See [Chapter 16, “Setting Up EnterpriseOne Single Signon,” Default Settings for Single Signon Node Configuration, page 215.](#)

Access the jde.ini file to modify the single signon node settings.

In the [TRUSTED NODE] section of the jde.ini file, add the appropriate values to the following settings:

numTrustedNodes	Enter the number of trusted nodes.
RegularLifeTime	Enter the expiration time (in minutes) for a regular token.
ExtendedLifeTime	Enter the expiration time (in minutes) for an extended token.
NodeName	Enter the logical name for the first node.
MachineName	Enter the physical machine name for the first node.
NodePassword	Enter the password for the first node.
NodeName1	Enter the logical name for the second node.
MachineName1	Enter the physical machine name for the second node.
NodePassword1	Enter the password for the second node.

Sample jde.ini Node Settings for Single Signon

The following are examples of node settings in the jde.ini file for single signon configurations:

Example 1:

A system administrator wants to install the EnterpriseOne system on three machines: SUN1, IBM1 and HP1. He wants all three machines to trust each other, and no other machines will be trusted. In this case, the administrator can configure the jde.ini as follows and deploy it on SUN1, IBM1, and HP1:

```
[TRUSTED NODE]
numTrustedNodes=3
```

For Sun:

```
NodeName=NodeSUN1
MachineName=SUN1
NodePassword=NodePwd
```

For IBM:

```
NodeName1=NodeIBM1
MachineName1=IBM1
NodePassword1=IBM1Pwd
```

For HP:

```
NodeName2=NodeHP1
MachineName2=HP1
NodePassword2=HP1Pwd
```

Example 2:

A system administrator wants all EnterpriseOne servers in the network to trust each other. Moreover, he wants to change the default node configuration as follows:

- Change the node password to NewPwd.
- Change the regular token lifetime to 30 minutes instead of 12 hours.
- Change the extended token lifetime to 60 minutes instead of 30 days.

In this case, the administrator can configure the jde.ini as follows and deploy it to all the enterprise servers in the network:

```
[TRUSTED NODE]
numTrustedNodes=1
RegularLifeTime=30
ExtendedLifeTime=60
NodeName=_GLOBALNODE (The node name must be _GLOBALNODE)
MachineName=_GLOBALNODE (The machine name must be _GLOBALNODE)
NodePassword=NewPwd
```

Configuring Single Signon Without a Security Server

When there is no security kernel available in the system, a user can directly sign in to the PeopleSoft EnterpriseOne Windows client without using the security server. To sign in to EnterpriseOne without a security server, you must:

- Set SecurityServer=<blank> in the [Security] section of the client jde.ini file.
- Sign on to EnterpriseOne using the proxy (database) user ID and password.

In this case, the EnterpriseOne Windows client generates an authenticate token locally. This token is referred to as a local token. A local token is very similar to a regular token except that it has a fixed node name (_LOCALNODE) and contains the proxy user name and password. A local token can only be accepted by a local fat client or an enterprise server without a security server, for example SecurityServer=<blank> in the server jde.ini.

Note. If you sign in to EnterpriseOne without a security server, you can only run the business functions and UBEs that are mapped to either the local machine or the enterprise server without a security server.

When a local token is used, the default value for regular token lifetime is 12 hours and the default value for extended token lifetime is 30 days. You can override these default values for the local token using the SSO Environment Configuration Tools application or by modifying the appropriate settings in the jde.ini file of the Windows client, deployment server, and enterprise server.

The following are sample jde.ini node settings to override _LOCALNODE for the local token:

```
[TRUSTED NODE]
numTrustedNodes=1
RegularLifeTime=4320
ExtendedLifeTime=43200
NodeName=_LOCALNODE
```

```
MachineName=_LOCALNODE
```

Note. You cannot override the node password for _LOCALNODE in the jde.ini file; you must use the SSO Environment Configuration Tools application to do this.

Configuring Single Signon for Collaborative Portal

The Collaborative Portal now uses token-based authentication for single signon between the Collaborative Portal and the EnterpriseOne JAS/Web client server or EnterpriseOne enterprise server.

Portlets that access information on an EnterpriseOne server generate a token based on the user ID, and send the token to the EnterpriseOne server. The server validates the token and enables the user to sign in. The requested information is returned to the portlet.

The system generates a token through calls from a Java Native Interface (JNI) to a set of C libraries, which is responsible for the encoding and encryption of the token. These libraries and their associated environment setup are installed as part of the Collaborative Portal install.

The token-based system requires that the Collaborative Portal user ID and the EnterpriseOne user ID are the same, or that a mapping be set up for the user IDs on the EnterpriseOne server.

Note. If EnterpriseOne and Collaborative Portal are sharing an LDAP instance, this is not an issue. Since EnterpriseOne only accepts uppercase user IDs in its database, Collaborative Portal will also require uppercase user IDs for the generated token to be validated.

See Also

[Chapter 16, “Setting Up EnterpriseOne Single Signon,” Managing User ID Mapping in EnterpriseOne, page 225](#)

Configuring Single Signon for Collaborative Portal in the *EnterpriseOne PeopleTools 8.11 Collaborative Portal Installation and Configuration documentation*

Configuring Single Signon for Portlets

This section provides information on how to modify the tokengen.ini file settings for single signon and contains single signon configuration information for the following portlets:

- EnterpriseOne Portlet (JSR168)
- Collaborative Portal EnterpriseOne Menu
- Hosted EnterpriseOne Portlet
- CSS, ESS, SSS
- EnterpriseOne Links
- CRM

Configuring tokengen.ini File Settings

Single signon requires that you change the tokengen.ini settings for Node Name and Node Password to correspond to the entries in the EnterpriseOne security server. The values shown in the [NODE MANAGER] section are for a default install:

```
[NODE MANAGER]
NodeName=_GLOBALNODE
NodePwd=_GLOBALPWD
```

To modify these settings after the install, locate the tokengen.ini file in the following directory:

<WebSphere home>/properties

EnterpriseOne Portlet (JSR168)

With the EnterpriseOne portlet, the JAS server runs as part of the portlet rather than being connected to remotely. This also means that the EnterpriseOne portlet uses the jas.ini and jdbj.ini files that were installed as part of the Collaborative Portal install.

The user IDs must be synchronized between the Collaborative Portal and the EnterpriseOne user database. If the default environment and role are set in the OWWEB section of the jas.ini, these entries will be used for all users. If no default entries are set, the user will be asked to choose from a list of environments and roles when they go to a page with the EnterpriseOne portlet on it.

When multiple EnterpriseOne portlets are placed on a page, only one of the portlets displays the environment and role list. The other portlets display the warning message, "This portlet is waiting for authentication to be completed."

See Also

EnterpriseOne PeopleTools 8.94: Web Server Installation for information about the jas.ini file settings

Collaborative Portal EnterpriseOne Menu

Before release 8.11, EnterpriseOne Menu (then called Task Explorer) used inherited trust for single signon. As of 8.11, the portlet uses the authenticate token. The environment and role are configured through the configuration screen of the portlet by the administrator. Alternatively, the default environment and role can be set in the jas.ini of the remote JAS server.

Hosted EnterpriseOne Portlet

Before release 8.11, the Hosted EnterpriseOne Portlet used inherited trust for single signon. As of release 8.11, the portlet uses the authenticate token. Environment and role are configured through the edit screen by each user. Alternatively, the administrator can set the default environment and role in the jas.ini of the remote EnterpriseOne JAS server.

CSS, ESS, SSS

Before release 8.11, these portlets used inherited trust for single signon. As of release 8.11, these portlets use the authenticate token. The environment and role are set through the portlet configuration screen by the administrator.

EnterpriseOne Links

Before release 8.11, EnterpriseOne Links used inherited trust for single signon. As of release 8.11, this portlet uses the authenticate token. The environment and role are still set through the portlet configuration screen by the administrator.

CRM

The CRM portlets continue to use the inherited trust system for single signon.

Configuring Single Signon Between Enterprise Portal and EnterpriseOne

This section provides an overview of setting up single signon between Enterprise Portal and EnterpriseOne applications and discusses how to:

- Manage user ID mapping in EnterpriseOne.
- Manage user ID mapping when using LDAP.
- Synchronize user mapping between LDAP and EnterpriseOne while using LDAP authentication.
- View user ID mapping when using LDAP.

Understanding Single Signon Between Enterprise Portal and EnterpriseOne

Prior to EnterpriseOne release 8.11, single signon between Enterprise Portal and EnterpriseOne was accomplished as follows:

1. Enterprise Portal generated a token and sent it to EnterpriseOne.
2. EnterpriseOne called back to the Enterprise Portal application server to validate token and received back a user ID.
3. The system used the user ID to sign on to EnterpriseOne.

Since EnterpriseOne can validate and sign on with a token generated by the Enterprise Portal, it is no longer necessary to call back to the Enterprise Portal side to validate the token. This simplification of the single signon setup between Enterprise Portal and EnterpriseOne means that the following items are no longer required:

- The psjoa.jar, psft.jar, and PeopleSoft.Generated.CompIntfc.jar files in the EnterpriseOne system. The latest Collaborative Portal installer does not install these files.
- The PeopleSoftAppServer, PeopleSoftAppServerUser, and PeopleSoftAppServerPassword jas.ini entries in the OWWEB section.
- The DBUser and DBPassword entries in the jas.ini are no longer required in the SECURITY section.
- The setup of the component interface (PRTL_SS_CI) on the Enterprise Portal. Additionally, the admin user for accessing this interface no longer needs to be set up.
- The entry in the PSTRUSTNODES table on the Enterprise Portal for the local node.

Note. The environment and role entries are still set up the same as in previous releases, as defaults in the `jas.ini` on the EnterpriseOne JAS server.

See Also

Integrating the PeopleSoft EnterpriseOne Menu Portlet with the PeopleSoft Enterprise Portal

Time Zone Adjustment for Enterprise Portal

When setting up single signon between Enterprise Portal and PeopleSoft EnterpriseOne, you must properly configure the ENTERPRISE TIMEZONE ADJUSTMENT setting in the EnterpriseOne enterprise server `jde.ini` file. This setting enables you to enter the difference in time between Greenwich Mean Time (GMT) and Enterprise Portal Node time. You should change this setting whenever daylight saving time changes to reflect the difference between GMT time and the Enterprise Portal Node time.

In the following example of the ENTERPRISE TIMEZONE ADJUSTMENT setting, the difference between the GMT and Enterprise Portal Node time is entered in minutes for an Enterprise Portal that is running in Mountain Standard Time (MST):

```
[ENTERPRISE TIMEZONE ADJUSTMENT]
EntNode=-360
```

User ID Mapping for Single Signon

Since Enterprise and EnterpriseOne systems have different user IDs, you must map the user IDs between the two systems in order for single signon to work. If you manage user IDs in an EnterpriseOne database, then you can use an EnterpriseOne application to map users. If you use LDAP to manage user information such as user IDs, passwords, and role relationships, then you must use the third-party LDAP tool to set up user ID mapping.

Managing User ID Mapping in EnterpriseOne

Access the SSO Environment Configuration Tools form. In PeopleSoft Solution Explorer, select System Administration Tools (GH9011), User Management, User Management Advanced and Technical Operations, and then double-click SSO Environment Configuration Tools.

To manage user ID mapping in EnterpriseOne:

1. On SSO Environment Configuration Tools, click the Configure the UserID Mapping link.
2. On Work with SSO E/E1 UserID Mapping, use the Add, Select, and Delete buttons to manage user ID mappings.
3. If you clicked Add to add a user ID mapping, on SSO E/E1 UserID Mapping Revisions form complete these fields:
 - EnterpriseOne UserID
 - Enterprise UserID

The system saves the record in the F00927 table.

Note. If the EnterpriseOne user ID is not in the F0092 table, the system generates an error stating that it cannot add the mapping record.

Managing User ID Mapping when Using LDAP

EnterpriseOne can use LDAP (Lightweight Data Access Protocol) to manage user IDs, password, and role relationships. If the EnterpriseOne system is LDAP-enabled, the following setting must be added to the jde.ini file:

```
[SECURITY]
LDAPAuthentication=true
```

See Also

Chapter 14, “Employing LDAP in PeopleSoft EnterpriseOne,” page 187

Synchronizing User Mappings Between LDAP and EnterpriseOne While Using LDAP Authentication

EnterpriseOne provides an optional UBE (R9200040) that you can run to batch synchronize all of the user mappings between the LDAP and EnterpriseOne databases. The user mapping synchronization also occurs when a user signs on to EnterpriseOne. However, the synchronization only applies to the user who just signed on. Therefore, you should run this UBE to:

- Synchronize all users.
- Purge obsolete users (such as the users that have already been removed from LDAP) from the database.

Note. You should be extremely cautious when running this UBE since it not only synchronizes user mappings, but also synchronizes other user profiles such as user-role relationship. Moreover, it will delete all the users that do not exist in LDAP.

To synchronize all user mappings between the LDAP and EnterpriseOne databases:

In PeopleSoft Solution Explorer, run the UBE R9200040.

The following is an example of the results of running the UBE:

Worldwide Company				
Synchronize the LDAP and EnterpriseOne Database				
<u>Table Name</u>	<u>Records Added</u>	<u>Records Deleted</u>	<u>Records Failed</u>	<u>Synchronization Status</u>
F0092	17	219	0	Successful
F00921	17	219	0	Successful
F98OWSEC	34	148	0	Successful
F95921	43	272	0	Successful
F9312	0	0	0	Successful
F0093	0	133	0	Successful
F00922	0	13	0	Successful
F00924	0	3	0	Successful

UBE R9200040 output

Viewing User ID Mapping When Using LDAP

When using LDAP to manage user signon information, you can still view the user ID mappings for single signon through EnterpriseOne.

In PeopleSoft Solution Explorer, select System Administration Tools (GH9011), Security Maintenance, and SSO Environment Configuration Tools to access the SSO Environment Configuration Tools form.

To view the User ID mapping:

1. On SSO Environment Configuration Tools, click the View UserID Mapping option.
2. On Work with SSO E/E1 UserID Mapping, choose a mapping record and then click the Select button to view the mapping.

CHAPTER 17

Setting Up PIM Synchronization for PeopleSoft EnterpriseOne CRM Users

This chapter provides an overview of Personal Information Management (PIM) synchronization and discusses how to:

- Set Up the PIM Server processing option.
- Set up users for PIM synchronization.
- Export PIM user records.
- Import PeopleSoft EnterpriseOne PIM synchronization records into Intellisync Server.

Understanding PIM Synchronization

PeopleSoft EnterpriseOne provides the ability to synchronize user data between third-party personal information management (PIM) systems and PeopleSoft EnterpriseOne CRM users. With this synchronization, CRM users can share and manage personal information such as contacts, appointments, and tasks stored in IBM Domino or Microsoft Exchange PIM systems. For example, as appointments are created in the CRM system, corresponding objects are created in the PIM system database. If users update or delete items in either the CRM or PIM system, the changes are synchronized in both locations.

PeopleSoft EnterpriseOne relies on a third-party software product, Intellisync Server, to enable data synchronization between PeopleSoft EnterpriseOne CRM and PIM systems. Intellisync Server uses these items to synchronize PIM data:

- CSV file. The CSV file contains the PIM server records for each PeopleSoft EnterpriseOne user that you set up for PIM synchronization. You generate this file from PeopleSoft EnterpriseOne after you set up users for PIM synchronization.
- Synchronizing template. This template determines the types of information that is synchronized between the PeopleSoft EnterpriseOne and PIM systems.

The process for setting up PIM synchronization is as follows:

1. Enter each PeopleSoft EnterpriseOne user's PIM system information into PeopleSoft EnterpriseOne.
2. Export this information from PeopleSoft EnterpriseOne into a CSV file.
3. Using Intellisync Server Bulk User Import, import the CSV file, along with a synchronizing template, into the Intellisync Server.

Note. PeopleSoft EnterpriseOne provides a standard synchronizing template for PIM synchronization.

User Defined Codes for PIM

PeopleSoft EnterpriseOne uses these user defined codes (UDCs) to categorize the data that is shared with the PIM system:

UDC Type	UDC Code	UDC Values and Definitions
Phones	01 PH	HOM: PIM-Home <blank>: PIM-Business FAX: PIM-Fax CAR: PIM-Car
Relation Type	01 RT	A: PIM-Assistant S: PIM-Spouse C: PIM-Child
Address Type	01 AT	H: PIM-Home W: PIM-Work
Email Type	01 ET	E: PIM-Email Address I: PIM-Web Address
PIM Sync Category	01 SG	PIMSG: PeopleSoft

Note. You should not change the Description Line 2 value for PIM UDCs that have Description Line 2 values.

In addition, the 01|SG UDC type is a new UDC created solely for PIM synchronization and is hard-coded, which means that only the description can be changed. "PeopleSoft" is the default Description Line 1 value.

Prerequisites

Install the PIM Sync Servlet.

See EnterpriseOne PeopleTools 8.94: Domino Exchange Integration

Setting Up the PIM Server Processing Option

If all users use the same type of PIM system (Microsoft Exchange or IBM Domino), you can set a processing option to specify the type of PIM server to set up synchronization with.

Note. Do not set this processing option if both PIM servers are used.

From the System Administration Tools menu (GH9011), select User Management. Right click User Profiles, select Prompt for, and then select Values.

To set up PIM Server processing options:

On Processing Options, click the PIM Server Setup tab and then enter the appropriate value for the PIM server:

- Enter D for IBM Domino Server.
- Enter X for Microsoft Exchange Server.

Setting Up Users for PIM Synchronization

Access the E1 – PIM User Information Setup form.

From the System Administration Tools menu (GH9011), select User Management and then select User Profiles. On Work with Users/Roles, select a user record and then select PIM User Setup from the Row menu.

E1 – PIM User Information Setup form

To set up a user for PIM synchronization:

1. On E1 – PIM User Information Setup, select the user's PIM server type:
 - IBM Domino Server
 - Microsoft Exchange Server

Note. If you specified the PIM server type in the PIM Server Setup processing option, you cannot select this option here.

2. For IBM Domino Server, complete these fields:

- Mail File Location
Enter the user's Lotus Notes mail database file. Specify the full name relative to the Domino Data Directory, without the .nsf extension, for example mail\UserMailDatabase.
 - Address Book Name
Enter the user's Lotus Notes address book database name. Specify the full name relative to the Domino Data Directory, without the .nsf extension, for example contacts\UserAddressBook.
 - Address Book Server
Enter the user's Lotus Notes address book database server.
3. In the Template field, click the search button to specify the Intellisync Server synchronizing template:
 - a. On E1 – PIM Template Revisions, complete these fields:

Template
Enter a name for the template. You can name the template based on the role or function of the PeopleSoft EnterpriseOne users that you associate this template to, for example you can name the template CRMHR template for human resources users or DEFAULT as the name of the default template for all users.

Template File
Enter a fully qualified pathname to the synchronizing template file. This must be a pathname that Intellisync can recognize.
 - b. After you create the template, double-click the template to select it and then click OK.
 4. For Microsoft Exchange Server, complete these fields:
 - Primary Windows NT Account
Enter the user's Windows NT account user name and domain name. The Intellisync server user name must be unique, for example Domain\SampleUser1.
 - Alias
Since an Intellisync account can only reference one mailbox, you must enter an alias to specify which mailbox to use.
 - Template
See step 3 for instructions on how to specify the template.

Exporting PIM User Records

After you set up users for PIM synchronization, you must export each user record to a CSV file. The CSV file contains each user's PIM system information. Subsequently, you must import this file into the Intellisync Server to complete the synchronization setup.

Access the Work With User/Role Profiles form.

From the System Administration Tools menu (GH9011), select the User Management menu and then select User Profiles (P0092).

To export all PIM user records:

1. On Work With User/Role Profiles, click Find.
2. From the Form menu, select PIM Export All Users.

3. On Report Output Destination, make sure that the Export to CSV option is selected and click OK.

To export a selected list of PIM user records:

1. On Work With User/Role Profiles, click Find and then select the user records that have been set up for PIM synchronization.

To determine which users have been set up for PIM synchronization, scroll to the PIM Server column. Records that have a value in this column have been set up for PIM synchronization.

2. From the Row menu, select PIM Export User(s).
3. On Report Output Destination, make sure that the Export to CSV option is selected and click OK.

The system generates and displays a CSV file. Use this file to import PIM synchronization records into Intellisync Server.

Importing PIM Synchronization Files into Intellisync Server

To complete the PIM data synchronization with PeopleSoft EnterpriseOne, use the Intellisync Server Bulk User Import tool to import these items into Intellisync Server:

- CSV file
- Synchronizing template

Note. The synchronizing template must match the template you associated with PeopleSoft EnterpriseOne users when you set up users for PIM synchronization.

See EnterpriseOne PeopleTools 8.94: Domino Exchange Integration for information on how to import these files.

CHAPTER 18

Enabling Mobile Client Functionality

This chapter provides an overview of distributed next numbers for mobile clients and discusses how to set up distributed next numbers for mobile clients.

Understanding Distributed Next Numbers for Mobile Clients

Any EnterpriseOne mobile application that assigns unique numbers using the EnterpriseOne next number facilities (namely the X0010 and X00022 business functions) must have its parameters registered as distributed next numbers. These parameter sets are identified during application development. For applications that call X0010, these parameters include a system code, next numbering index, company, document type, century, and fiscal year. For applications that call X00022, the parameter is an object name.

Setting Up Distributed Next Numbers for Mobile Clients

This section discusses how to:

- Activate mobile client functionality.
- Define the starting next number.
- Enable distributed next numbers.
- Set up distributed next numbers by system code.
- Map the EnterpriseOne user ID to the Distributed Next Numbers application (P950411).
- Set up distributed next numbers by application.
- Schedule updates to distributed next numbers applications (P93100).

See Also

Setting Up System Next Numbers in the *PeopleSoft EnterpriseOne Address Book 8.11 PeopleBook*

Activating Mobile Client Functionality

In order to enable mobile client functionality, make sure that the F99410 table has records that contain the following system codes:

- SY90CA
- CRMMSL
- SY49

Follow this procedure to add these records.

On the EnterpriseOne enterprise server, access the P99410 application.

To activate mobile client functionality:

1. On Work with EnterpriseOne System Control, click Add.
2. On EnterpriseOne System Control Revisions, enter each of the following system codes, one at a time, in the Data Item field:
 - *SY90CA*
 - *CRMMSL*
 - *SY49*
3. Click Yes.
4. Click OK.
5. Repeat these steps to add each system code.

Defining the Starting Next Number

On the EnterpriseOne enterprise server, access the P0002 application through the EnterpriseOne Web Client.

To define the starting next number:

1. On Work with Next Numbers, click Add.
2. Enter *42E* in the System field.
3. Complete these fields:
 - Use
The description of the next number parameter.
 - Next Number
The starting next number, for example 1.
 - Check Digit Used
If checked, EnterpriseOne appends a random digit to the next number for uniqueness.
4. Click OK.

Enabling Distributed Next Numbers

On the EnterpriseOne enterprise server, access the P00098 application through the EnterpriseOne Web Client.

To enable distributed next numbers:

1. On Enable Distributed Next Numbers, click Add.
2. Create separate rows for each of the following product codes:

Product Code	Order Type Next Number	Enabled
42E	1	Y
47	2	Y

Product Code	Order Type Next Number	Enabled
32	2	Y
01	1	Y

3. Create additional rows for the following tables:

Object Name	Enabled
F0111 (Address Book - Who's Who)	Y
F01112 (Related Person)	Y
F0115 (Address Book - Phone Numbers)	Y
F01151 (Electronic Address)	Y
F0450 (Payee Control)	Y
F42140 (Customer Master Commission Information)	Y
F42150Z1 (Header Commission Unedited Transaction File)	Y
F42160Z1 (Detail Commission Unedited Transaction File)	Y
F90CA06A (Competitor_KillSheet Table)	Y
F90CB010 (Lead Table)	Y
F90CB020 (Opportunity Table)	Y
F90CB02E (Opportunity - Employee Table)	Y
F90CB02J (Opportunity - Sales Cycle Table)	Y
F90CB030 (CRM Address Table)	Y
F90CB043 (Qualification Object Table)	Y
F90CB05A (Sales Cycle Table)	Y
F90CB05C (Sales Cycle Notification Ledger Table)	Y
F90CB060 (Forecast Table)	Y

4. Click OK.

Setting Up Distributed Next Numbers by System

On the EnterpriseOne enterprise server, access the P00023A application through the EnterpriseOne Web Client.

To set up distributed next numbers by system code:

1. On Work with Distributed Next Numbers by System Code, select ZJDE0001.

2. Click Add.
3. For each EnterpriseOne mobile user, create additional rows for the different system codes, as follows:

Third Party User ID	System Code	OrderType Next Number	Allotment
Enter the EnterpriseOne user ID of a mobile client	42E	1	500
	47	2	500
	32	2	500
	01	1	<p>Assign a large enough allotment of next numbers so that users can enter enough new records before synchronizing with EnterpriseOne.</p> <p>Note. The mobile client is not allowed to add more records than specified by this allotment. When the mobile client synchronizes with the server, the user is granted a new allotment of next numbers.</p>

4. Click OK.

Mapping the EnterpriseOne User ID to the Distributed Next Numbers Application (P950411)

On the EnterpriseOne enterprise server, access the P950411 application through the EnterpriseOne Web Client.

To map the EnterpriseOne user ID to the Distributed Next Numbers application:

1. On Work with Third Party User ID Map, for each mobile user, click Add.
2. Complete these fields:
 - UserID Type
Synchronization application (default).
 - User ID
Enter the user ID of the mobile client.
 - Environment Name
Enter the EnterpriseOne environment that you are currently signed on to.
 - Third-Party User ID
Accept the default value.
3. Click OK.

Setting Up Distributed Next Numbers by Application

On the EnterpriseOne enterprise server, access the P00023A application through the EnterpriseOne Web Client.

Note. You must make sure that you perform the steps in this task in the order that they appear. Particularly, you must enter the server user ID before you enter the EnterpriseOne user IDs.

To set up distributed next numbers by application:

1. On Work with Distributed Next Numbers by Object Name, select ZJDE0002 and click Add.
2. Enter the following information into separate rows:

Third Party User ID	EnterpriseOne Table	Allotment
SERVER	F0111 (Who's Who)	6250
SERVER	F01112 (Related Person)	2500
SERVER	F0115 (Phone Numbers)	1250
SERVER	F01151 (Electronic Address)	1250

Note. The SERVER value must be entered in upper case.

3. Click OK.
4. Select ZJDE0002 and click Add.
5. For each EnterpriseOne mobile user, create rows for each of the following EnterpriseOne tables:

Third Party User ID	EnterpriseOne Table	Allotment
Enter the EnterpriseOne user ID of a mobile client.	F0111	<p>Assign a large enough allotment of next numbers so that users can enter enough new records before synchronizing with EnterpriseOne.</p> <p>Note. The mobile client is not allowed to add more records than specified by this allotment. When the mobile client synchronizes with the server, the user is granted a new allotment of next numbers.</p>
	F01112	
	F0115	
	F01151	
	F0450	
	F42140	
	F42150Z1	
	F42160Z1	
	F90CA06A	
	F90CB010	
	F90CB020	
	F90CB2E	
	F90CB02J	
	F90CB030	
	F90CB043	
	F90CB05A	
	F90CB05C	
	F90CB060	

6. Click OK.

Scheduling Updates to Distributed Next Numbers Applications

You should schedule the Distributed Next Number Update UBE (R0002D1) to run at a regular interval. This UBE is typically set up to run nightly.

CHAPTER 19

Working with Vocabulary Overrides

This section provides an overview of vocabulary overrides and discusses how to:

- Access Vocabulary Overrides from System Administration Tools.
- Access Vocabulary Overrides from Object Management Workbench.
- Create interactive vocabulary overrides.
- Create batch vocabulary overrides.
- Review vocabulary overrides.
- Reset a vocabulary override.
- Reset all vocabulary overrides in an application (interactive and batch).

Understanding Vocabulary Overrides

Vocabulary Overrides is an application that you can use to change the text that appears on forms and reports. You can specify both form columns and row headings, provide customization for multiple languages and industries, and retain your overrides with the next software update.

Because the Vocabulary Overrides application (P9220) affects the user interface throughout PeopleSoft EnterpriseOne, it is important that you secure this application from most of the users. When you work with vocabulary overrides for an interactive or batch application, the Vocabulary Overrides application simulates an application checkout from the central objects repository, just as if you checked out the application by using Object Management Workbench. This checkout is done so that, while you are working on the application in the Vocabulary Overrides application, no one can check out the application.

Note. When the Object Management Workbench line is written for the Vocabulary Overrides application, the system does not bring down specifications to the requesting workstation. Instead, the requesting workstation accesses the relational database tables directly.

After you make vocabulary override changes, use an update package to push these changes to the users.

Creating Vocabulary Overrides

You can create vocabulary overrides to customize the interactive and batch applications. After you make vocabulary override changes, use an update package to push these changes to the users. For example, you could create vocabulary overrides for the Verify OCM report. After you make vocabulary override changes, you should use an update package to push these changes to the users.

Note. When you create a vocabulary override for a report, the override occurs at the version level. When you run the version, the vocabulary override appears on the report instead of the data dictionary description. The vocabulary override does not affect the base report specifications or any other version of the report.

Forms Used to Work with Vocabulary Overrides

Form Name	Form ID	Navigation	Usage
Work With Vocabulary Overrides	W9220H	System Administration Tools (GH9011), Vocabulary Overrides (P9220)	Locate an interactive or batch application to which you want to apply vocabulary overrides. Review existing vocabulary overrides.
Object Management Workbench	W98220A	Enter <i>OMW</i> in the Fast Path field in PeopleSoft Solution Explorer.	Locate an interactive or batch application to which you want to apply vocabulary overrides.
SAR Requirement	W559220A	On Work With Vocabulary Overrides, select an application and click Select.	This form only appears if the system administrator set up the processing option for vocabulary overrides to require a software action request (SAR) number for overrides.
Interactive Vocabulary Overrides	W9220A	On Work With Vocabulary Overrides, click Interactive and then click Find. Select an application, and click Select.	Create and reset interactive vocabulary overrides.
Batch Vocabulary Overrides	W9220B	On Work With Vocabulary Overrides, click Batch and then click Find. Select a batch version and click Select.	Create and reset batch vocabulary overrides.
Overridden Data Item Search	W9220E	On Work With Vocabulary Overrides, from the Form menu, select Data Item Search.	Review data items that contain vocabulary overrides.

Accessing Vocabulary Overrides from PeopleSoft Solution Explorer

To access Vocabulary Overrides from System Administration Tools:

1. On Work With Vocabulary Overrides, click Interactive or Batch, and click Find.
Use the query by example fields to refine the search.
2. Select an application and click Select.

If the application that you selected is checked out or is in the save location, the system displays the following error message: This object is currently in use by a project in the Object Management Workbench (either through check out or in the save location) and is, therefore, unavailable.

You must create vocabulary overrides for this application at another time or contact the users of the application to check in, erase their checkout, or delete the object from the save location.

3. If the SAR Requirement form appears, enter a SAR number in the SAR Number field.

This form appears if the system administrator set up the processing option for vocabulary overrides to require a SAR number for overrides.

4. Click OK.

The Interactive Vocabulary Overrides form or the Batch Vocabulary Overrides form appears. All of the interactive forms or batch versions associated with the application that you chose appear in the detail area. You can expand any row that has a plus (+) sign on the left side.

The Vocabulary Overrides application essentially checks out this application in Object Management Workbench so that while you are working on the application in Vocabulary Overrides, no one else can check out the application. After you finish creating overrides, Vocabulary Overrides erases the checkout in Object Management Workbench.

Application

The name that identifies a system object. PeopleSoft EnterpriseOne architecture is object-based. Discrete software objects are the building blocks for all applications, and developers can reuse the objects in multiple applications. The Object Librarian tracks each object. Examples of system objects include:

- Batch applications (such as reports).
- Interactive applications.

Accessing Vocabulary Overrides from Object Management Workbench

Access Object Management Workbench.

To access Vocabulary Overrides from Object Management Workbench:

1. On Object Management Workbench, add the object to an OMW project.
2. Select the interactive or batch application, and then click the Design button.

The Interactive Application Design form or the Batch Application Design form appears.

3. On the Design Tools tab, click Vocabulary Overrides.

The system displays the following warning: Warning! You are now accessing Vocabulary Overrides. This application will override currently checked in objects. You must have authority to make changes.

4. If you have authorization to make vocabulary override changes, click OK.
5. If the SAR Requirement form appears, enter a SAR number in the SAR Number field.

This form only appears if the system administrator sets the processing option that requires a SAR number for vocabulary overrides.

6. On the Work with Vocabulary Overrides form, click Select.

The Interactive Vocabulary Overrides form or the Batch Vocabulary Overrides form appears. All of the interactive forms or batch versions associated with the application appear in the detail area. You can expand any row that has a plus (+) sign on the left side.

The Vocabulary Overrides application essentially checks out this application in Object Management Workbench so that while you are working on the application in Vocabulary Overrides, no one else can check out the application. After you finish creating overrides, Vocabulary Overrides erases the checkout in Object Management Workbench.

Creating Vocabulary Overrides

To create interactive vocabulary overrides:

1. To work with a language other than the domestic language, on Interactive Vocabulary Overrides, complete the Language field, and then click Find.
2. Enter a language code.
Leave this field blank if you are creating vocabulary overrides in the domestic language.
3. Double-click the + button next to one of the forms listed in the detail area.
The form expands, displaying the types of text that are available on that form, such as find/browse text, control text, grid column text, exit text, and text variables.
4. Double-click the + button for one of the types of text.
The type of text expands, displaying all of the text that you can override.
5. To create a vocabulary override, change the text in the Description column for a particular item.
Click OK when you finish creating overrides.

Note. Some descriptions for data items contain carriage returns and new-line characters. To create a vocabulary override for these descriptions (indicated with an icon to the left of the row), select the data item row and, from the Row menu, select Extended Text Revision.

6. On the Extended Text Revision form, change the text in the field and click OK.

The Vocabulary Overrides application essentially checks out this application in Object Management Workbench so that while you are working on the application in Vocabulary Overrides, no one can check the application out. After you finish creating overrides, Vocabulary Overrides erases the checkout in Object Management Workbench.

To actually see the description change applied to the application, you must first retrieve the specifications for the application to the local client machine and run it. Do this by clicking either the Check Out or Get button in Object Management Workbench.

Language	A user defined code (01/LP) that specifies the language to use on forms and printed reports. Before you specify a language, a code for that language must exist at either the system level or in the user preferences.
Form Name	The unique name that identifies a form.
Override	<p>A code that indicates whether the default value of a particular text item has been overridden. Overrides are defined during development of interactive and batch applications when the developer determines that the data dictionary value, or current text, is not appropriate or explicit enough for the particular application. When the interactive or batch application runs, the text is changed and this flag is set.</p> <p>Valid values are:</p> <ul style="list-style-type: none">• 0

The text is the original value. If it is a data item related field, then it is the same as the data dictionary.

- *1*

The original text, often the data dictionary default, has been overridden.

Data Item

A code that identifies and defines a unit of information. It is an alphanumeric code up to eight characters long that does not allow blanks or special characters, such as %, &, or +. You create new data items by using system codes 55-59. You cannot change the alias.

Text Type

A user defined name or remark.

Visible

Indicates whether the data item or text for a data item is visible on a form or report. This is defined during development of the form or report when the developer determines that a data item is required for processing, but should not necessarily be visible on the form or report. The valid values are:

- *1*

The data item or data item text is visible on the form or report.

- *0*

The data item or data item text is not visible on the form or report.

Creating Batch Vocabulary Overrides

Access the Batch Vocabulary Overrides form.

To create batch vocabulary overrides:

1. To work with a language other than the domestic language, on Batch Vocabulary Overrides, complete the Language field, and then click Find.
2. Enter a language code.
Leave this field blank if you are creating vocabulary overrides in the base (domestic) language.
3. Double-click the + button next to one of the versions listed in the detail area.
The version expands, displaying the types of text that are available on that version, such as page header and group sections.
4. Double-click the + button next to one of the types of text.
The type of text expands, displaying all of the text that you can override.
5. To create a vocabulary override, change the text in the Description column for a particular item.
6. Click OK when you finish creating overrides.

The Vocabulary Overrides application essentially checks out this application in Object Management Workbench so that while you work on the application in Vocabulary Overrides, no one can check the application out. After you finish creating overrides, Vocabulary Overrides erases the checkout in Object Management Workbench.

Version

The name given to identify a version of the software.

Section

A user defined name or remark.

Control Type

A user defined name or remark.

Reviewing Vocabulary Overrides

Access the Overridden Data Item Search form.

You can use vocabulary overrides to review every location where someone has overridden a data item. You can view the override locations from a form or from a report.

To review vocabulary overrides:

1. On Work With Vocabulary Overrides, from the Form menu, select Data Item Search.
2. On the Overridden Data Item Search form, enter a data item to search for and then click OK.
3. Click one of the following options to select a scope for the application search:
 - Interactive Application
 - Batch
 - Both
4. Select one of the following options for the output results:
 - Interactive
If you view the search results by using the interactive application, the Data Item Locator form appears when this search is complete. This form displays a list of all of the applications in which the data item appears.
 - Printed Report
If you view the search results by using the printed report, an Adobe Acrobat Portable Document Format (.pdf) file is created, which you can view or print.
5. From the Form menu, select Run Report.

Resetting a Vocabulary Override

Access the Interactive Vocabulary Overrides form or the Batch Vocabulary Overrides form, depending on the type of application in which you want to reset a vocabulary override.

You can reset vocabulary overrides to the original data dictionary definition. If you need to reset multiple vocabulary overrides to the default data dictionary definition, PeopleSoft EnterpriseOne provides an automated process that resets overrides at the interactive form level, the batch version level, and the interactive and batch application level. When you reset vocabulary overrides at the form level, you reset all vocabulary overrides on a specific form—for example, the Work with Addresses form (W01012B) in the Address Book application. When you reset vocabulary overrides at the application level, you reset all vocabulary overrides on all forms or versions in an entire interactive or batch application—for example, the Address Book application (P0101) or the Print Mailing Labels report (R01401).

To reset a vocabulary override:

1. Double-click the + button in the row header for one of the forms or versions in the detail area, and then double-click the + button in the row header for a type of text on the form or a type of section in the version.
The detail area expands to display the data items associated with the type of text or section.
2. Select the data item that you want to reset, and then, from the Row menu, select Reset Description.

Note. The Reset Description menu option is inactive if a vocabulary override does not exist for the data item.

3. Click OK to return to the Work With Vocabulary Overrides form.

If you click Cancel to return to the Work With Vocabulary Overrides form *after* you reset a vocabulary override, you *do not* cancel the action. The data item remains at the default data dictionary definition.

Resetting All Vocabulary Overrides on a Form (Interactive and Batch)

Access the Work With Vocabulary Overrides form.

To reset all vocabulary overrides in an application (interactive and batch):

1. Click one of the following options and then click Find:

- Interactive
- Batch

2. Select an application and click Select.

Depending on the type of application, either the Interactive Vocabulary Overrides form or the Batch Vocabulary Overrides form appears. The detail area displays forms for interactive applications and versions for batch applications.

3. From the Form menu, select Reset by Application for interactive applications or Reset by Batch for batch applications.

The software clears all vocabulary overrides from the *entire* application and resets the data items to the base definitions. If no base definition exists for a data item, the software resets the data item to the default data dictionary definition.

Important! When you select either the Reset by Application or the Reset by Batch menu option, the decision is final; the software does not provide a confirmation box or a proof mode.

CHAPTER 20

Using the Scheduler Application

This chapter provides an overview of the Scheduler application and discusses how to:

- Work with the Job Scheduler.
- Use advanced scheduling options.
- Work with the Scheduler server.
- Work with daylight savings rules.
- Run Scheduler reports.

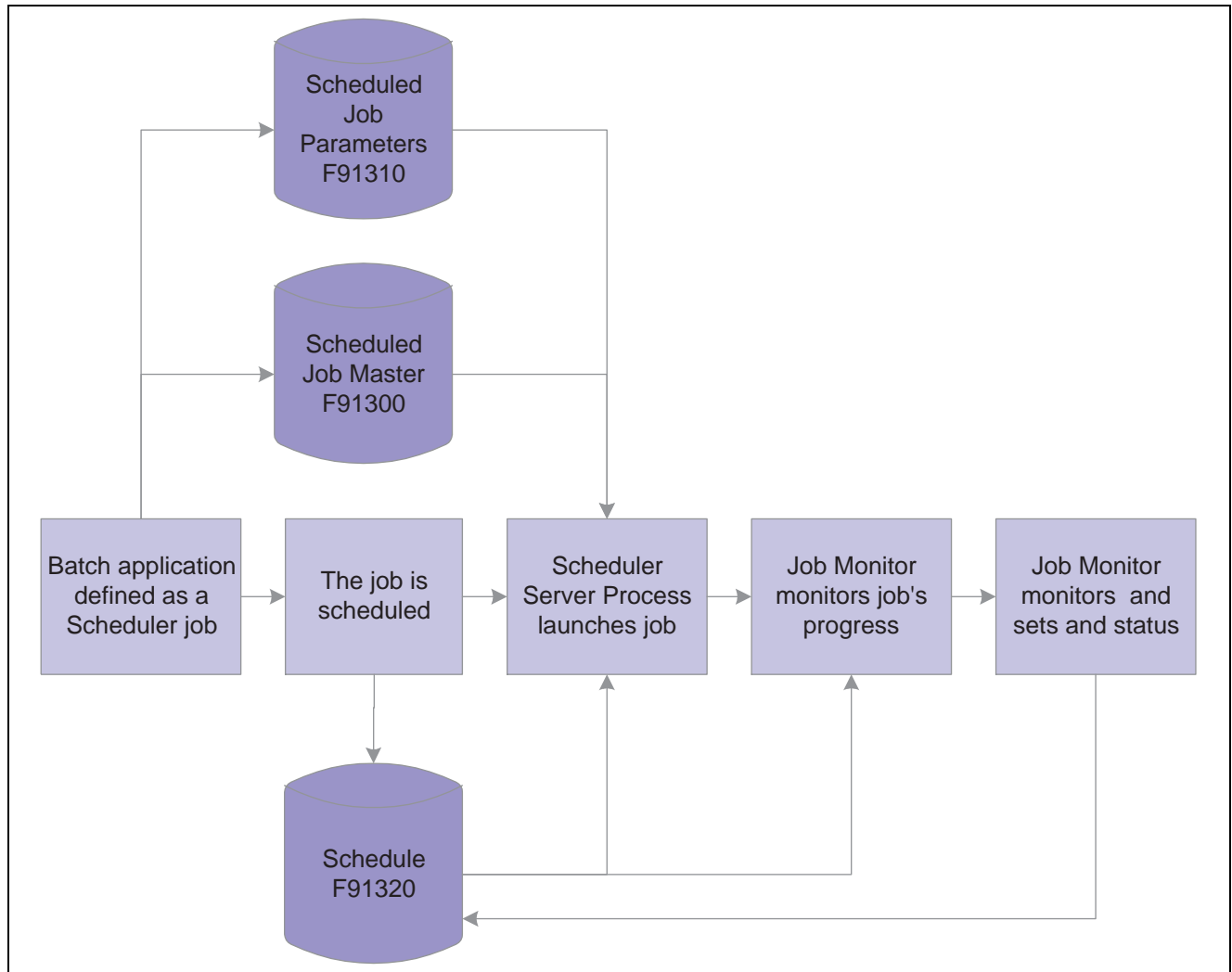
Understanding the Scheduler Application

Occasionally, you might want to run batch jobs that take up a great deal of machine resources or that require users to be signed off after normal working hours. You also might want the flexibility to run jobs at scheduled intervals during the day or even periodically throughout the month or year.

The Scheduler application enables you to schedule batch jobs to run after hours or periodically throughout the day, according to a schedule that you define. You can schedule jobs by time (daily, weekly, monthly, yearly) or based on a specified period. You also can set up the scheduler to restart a job in the event of a job failure.

You can specify the server on which you want the job to run, as well as the time zone, regardless of the locale. The Scheduler system uses a modified version of Universal Coordinated Time (UCT), which counts the number of minutes, not seconds.

The following graphic illustrates the scheduling process:



The scheduling process

When you define a scheduled job, the parameters of that job are stored in the F91300 table.

After the job is scheduled, the system writes records to the F91320 table, indicating each time that the job should be launched. As the job runs, the Job Monitor monitors the progress of the job.

When the job ends, the Job Monitor assigns an end status to the job and updates the record of the job in the Job Schedule table to indicate that the job either ended successfully or in error.

Working with the Job Scheduler

This section provides an overview of the job scheduler and discusses how to:

- Enter processing options for the Scheduler.
- Schedule a job.
- Schedule a recurring job.
- Revise a scheduled job.

- Review all jobs or local jobs.

Understanding the Job Scheduler

When you schedule a batch process to run through the Scheduler, you can also add a recurrence pattern to the job, which means that the job will restart at the intervals that you define, such as once a week, once a month, or once a year. You can also specify how many times you want the job to run before it ends, or you can define a date after which the job will no longer run.

You schedule jobs in the local time of the server on which the job will run. For example, when you schedule a job, you might select the version that specifies the eastern time zone to run jobs in eastern standard time (EST).

Prerequisite

To use a server's time zone, you must first specify the time zones that you want to use. To do this, copy the Scheduler processing options (version ZJDE0001 on the Work with Versions form), and modify them according to your needs. If you use more than one time zone, you should modify the processing options to display the Work with Versions form each time that you invoke the Schedule Jobs application. That way, you can select the correct version for the time zone in which you want to schedule the job.

See Also

[Chapter 20, "Using the Scheduler Application," Scheduling a Recurring Job, page 253](#)

[Chapter 20, "Using the Scheduler Application," Setting Processing Options for the Job Scheduler, page 252](#)

Forms Used to Work with the Job Scheduler

Form Name	Form ID	Navigation	Usage
Work With Versions	W983050B	Report Management (GH9111), Job Scheduler (GH9015), Schedule Jobs (P91300)	Locate the version that specifies the time zone in which the scheduled job will run.
Work With Scheduled Jobs	W91300B	Report Management (GH9111), Job Scheduler (GH9015), Schedule Jobs (P91300) On Work With Versions, click the version and then click Add.	Access forms to schedule a job.
Scheduling Information Add	W91300A	On Work With Scheduled Jobs, click Add.	Schedule a job.
Scheduling Advanced Options	W91300I	On Scheduling Information Add, select Advanced Options from the Row menu.	Enter the user and machine information for the scheduled job.
Recurring Scheduling Information Revisions	W91300C	On Scheduling Information Add, select Recurrence from the Form menu.	Schedule a recurring a job.

Setting Processing Options for the Job Scheduler

Processing options enable you to specify the default processing for programs and reports.

For programs, you can specify options such as the default values for specific transactions, whether fields appear on a form, and the version of the program that you want to run.

For reports, processing options enable you to specify the information that appears on reports. For example, you set a processing option to include the fiscal year or the number of aging days on a report.

Do not modify PeopleSoft EnterpriseOne demo versions, which are identified by ZJDE or XJDE prefixes. Copy these versions or create new versions to change any values, including the version number, version title, prompting options, security, and processing options.

Display

Although processing options are set up during PeopleSoft EnterpriseOne implementation, you can change processing options each time you run a program.

View Local Time

Local Time Zone

Enter '1' to adjust time for daylight savings. Enter '0' to never adjust for daylight savings.

Use this Daylight Savings Rule when adjusting for daylight savings.

Process

Although processing options are set up during PeopleSoft EnterpriseOne implementation, you can change processing options each time you run a program.

Maximum number of job schedule records

Defaults

Although processing options are set up during PeopleSoft EnterpriseOne implementation, you can change processing options each time you run a program.

Default Job Type

Number Of Job Occurrences

Max Number of Job re-submissions

Scheduling a Job

Access the Work With Versions form.

Note. If you use only one time zone, you might not be prompted to choose a version. In this case, the Work With Versions form does not appear. You can delete the Work With Versions form in the menu properties for P91300. PeopleSoft ships GH9015/P91300 to prompt for the version.

To schedule a job:

1. On Work with Version, double-click the version that specifies the time zone in which the scheduled job will run.
2. On Work With Scheduled Jobs, click Add.
3. On Scheduling Information Add, complete the following fields:
 - Scheduled Job Name
 - Scheduled Job Status
 - Scheduled Batch Application
 - Scheduled Version
 - Scheduled Start Date/Time
4. Click OK.

Scheduled Job Name	A name that uniquely identifies to the system and the user a scheduled job. Use this name to indicate the job function, such as <i>Monthly Close</i> or <i>Nightly Back Up</i> .
Scheduled Job Status	The current status of the scheduled job. As long as the status is active, the Scheduler determines if the job should be submitted to the server for execution. When the scheduled end date for the job has been reached, the status changes to <i>Not Active</i> . To stop the Scheduler from considering the job for submission, you can change the status to <i>Not Active</i> (or suspended) at any time prior to the end date. You can reactivate the job if you want the Scheduler to include the job again, but you can reactivate a job only if the end date is in the future.
Scheduled Start Date/Time	The next date on which the Scheduler submits the scheduled job to the server for execution.
Scheduled Batch Application	The object name of the report that the Scheduler submits to the server.
Scheduled Version	The version of the report that is scheduled to run. A version identifies a specific set of data selections and sequencing settings that the batch job uses.

Scheduling a Recurring Job

Access the Recurring Scheduling Information Revisions form.

To schedule a recurring job:

1. Select one of the following options, and complete the accompanying fields that appear after you select an option:

- **By Time**
Run the job every n days or every weekday.
Run the job at the specified time interval. For example, run the job every 40 minutes or every eight hours.
 - **Daily**
Run the job at the specified interval of days or every weekday. For example, run the job every seven days or every weekday.
 - **Weekly**
Recur every n weeks on Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday.
Run the job at the specified weekly interval on the specified day of the week. For example, run the job every two weeks on Monday.
 - **Monthly**
Day n of every x months or the [first, last, and so on] [day, Sunday, Friday, and so on] of every n months.
Run the job on the specified day of every n months or on a specific day of every n months. For example, run the job on day one of every four months or on the last Friday of every second month.
 - **Period**
Day n of every x periods or the [first, last, and so on] [day, Sunday, Friday, and so on] of every n periods.
 - **Company**
 - **Yearly**
Every [month name] [date] OR
The [first, last, and so on] [day, Sunday, Friday, and so on] of [month name] OR
Day x of the [first, last, and so on] period OR
The [first, last, and so on] [day, Sunday, Friday, and so on] of the [first, last, and so on] period.
Schedule the job at the specified time of the year. For example, you might want to run the job on the last day of December of each year, every January 1, on the first Monday of June, on day 15 of the last period, or on the second Tuesday of the fourth period.
2. Specify when you want the Scheduler to stop submitting the job by selecting one of the following options:
 - No end date
 - End after
 - End by
Enter the month, day, and year on which you want the job to expire.
 3. Click OK.

Scheduled Start Date	The next date on which the Scheduler submits the scheduled job to the server.
By Time	The type of interval for which the scheduled job should run, such as daily, weekly, monthly, or yearly.
Daily	The type of interval for which the scheduled job should run, such as daily, weekly, monthly, or yearly.

Weekly	The type of interval for which the scheduled job should run, such as daily, weekly, monthly, or yearly.
Monthly	The type of interval for which the scheduled job should run, such as daily, weekly, monthly, or yearly.
Period	The type of interval for which the scheduled job should run, such as daily, weekly, monthly, or yearly.
Yearly	The type of interval for which the scheduled job should run, such as daily, weekly, monthly, or yearly.
No end date	These options limit the time that the job is considered active by the Scheduler. You can select either the number of times this job is allowed to run or a date and time after which the job will no longer run. The job will always be considered active if the No end date option is selected.
End after	These options limit the time that the job is considered active by the Scheduler. You can select either the number of times this job is allowed to run or a date and time after which the job will no longer run. The job will always be considered active if the No end date option is selected.
End by	These options limit the time that the job is considered active by the Scheduler. You can select either the number of times this job is allowed to run or a date and time after which the job will no longer run. The job will always be considered active if the No end date option is selected.

Revising a Scheduled Job

You might want to revise the information for a job. For example, you might want to change the job status to *Active* or *Not Active*, enter a new batch process as the scheduled job, or change the job start date and time.

Access the Work With Versions form.

To revise a scheduled job:

1. On Work With Versions, select the version that specifies the time zone in which the job will run and click Select.
2. On Work with Scheduled Jobs, select the job that you want to revise, and then select Job Revisions from the Row menu.
3. On Scheduling Information Revisions, modify the following fields as necessary and click OK:
 - Scheduled Job Status
 - Scheduled Batch Applications
 - Scheduled Version
 - Scheduled Start Date/Time
4. If you want to remove recurrence from a scheduled job, select Remove Recurrence from the Form menu.
5. If you want to add category codes to the scheduled job, select Category Codes from the Form menu.
6. On Scheduler Category Codes, if you want to revise the advanced options for this job, select Advanced Options from the Form menu.

The Scheduling Advanced Options form appears.

Note. You can also activate or inactivate a job by selecting the job on Work With Scheduled Jobs, and then selecting Change Status from the Row menu.

Reviewing All Jobs or Local Jobs

If necessary, you can review all of the jobs in all time zones, or local jobs only. Depending on the view that you are currently using, the system protects the other choice. For example, if you are currently viewing local jobs, the system protects the Local Jobs choice and allows you to select only All Jobs.

Access the Work With Scheduled Jobs form.

To review all jobs or local jobs:

1. On Work With Scheduled Jobs, select Display from the Form menu.
2. Click either All Jobs or Local Jobs.

Job Status	The current status of the scheduled job. As long as the status is active, the Scheduler determines if the job should be submitted to the server for execution. When the scheduled end date for the job has been reached, the status changes to <i>Not Active</i> . To stop the Scheduler from considering the job for submission, you can change the status to <i>Not Active</i> (or suspended) at any time prior to the end date. You can reactivate the job if you want the scheduler to include the job again, but you can reactivate a job only if the end date is in the future.
Report Name	The object name of the report that the Scheduler submits to the server.
Scheduled Version	The version of the report scheduled to run. A version identifies a specific set of data selections and sequencing settings that the batch job uses.

Using Advanced Scheduling Options

This section provides an overview of the Scheduler's advanced options and discusses how to:

- Override the environment.
- Override job expiration specifications.
- Define when the Scheduler resubmits a job.
- Override batch application specifications.
- Add values to a report interconnect.

Understanding Advanced Scheduling Options

You can use advanced options to override the job properties, such as the location where the job will run and the environment in which it will run. You can also use advanced options to specify whether you want the system to resubmit a job if it ends in error or if you want to change job expiration specifications.

You can define whether to log errors to the jde.log or jdedebug.log, and whether you want the system to override printer locations and job queues. You can also add a report interconnect to a job if you want to pass parameters to it.

Note. To restore the default values in the advanced options application, click the default button on Scheduling Advanced Options.

Forms Used to Work with Advanced Scheduling Options

Form Name	Form ID	Navigation	Usage
Work With Scheduled Jobs	W91300B	Report Management (GH9111), Job Scheduler (GH9015), Schedule Jobs (P91300)System On Work With Versions, click the version and then click Add.	Access forms to schedule a job.
Scheduling Advanced Options	W91300I	On Work With Scheduled Jobs, select the job, and then select Advanced Options from the Row menu.	Override the environment, job expiration, and batch application specifications. Define when the Scheduler resubmits a job.

Overriding the Environment

A situation might exist in which you need to override an environment. For example, you would override the environment if the environment in which you want to run the job is not available or is different from the environment that you were logged into when you scheduled the job.

Access the Launch Overrides tab on the Scheduling Advanced Options form.

Scheduled Environment	Indicates the environment in which the scheduled job will run.
Scheduled Logical Server	The PeopleSoft EnterpriseOne logical server against which the job is submitted.
Scheduled User	Indicates the user ID for which the job will start.
Scheduled User Role	Indicates the role ID for which the job will start.
Scheduled Password	Indicates the password for the scheduled user submitting the job. The password is encrypted before it is stored in the Job Schedule Master table.

Overriding Job Expiration Specifications

Job expiration specifications ensure that servers do not become overloaded with unexpired jobs. If necessary, you can override job expiration specifications so that the job never expires, or expires after a certain number of minutes.

For example, suppose you schedule a job to run at midnight and another job for 1:00 a.m., but the server goes down and probably will not come back up again before the jobs are scheduled to run. In this case, you can specify that the first job, which you scheduled to run at midnight, expires in 30 minutes (12:30 a.m.), so that if the server does not come back up within 30 minutes, the job expires.

Access the Job Expirations tab on the Scheduling Advanced Options form.

Job expires after

This field indicates when the scheduled job expires. The job will not run after it expires. Select one of the following:

- *Job never expires:* The job has no expiration.
- *Job expires after:* The job expires after x<F0> number of minutes past the scheduled start time.

Job never expires

This field indicates when the scheduled job expires. The job will not run after it expires. Select one of the following:

- *Job never expires:* The job has no expiration.
- *Job expires after:* The job expires after x<F0> number of minutes past the scheduled start time.

Defining When the Scheduler Resubmits a Job

You can define when the Scheduler resubmits jobs. This feature is useful if a job ends in error, for example, because the Scheduler will submit the job after a certain period of time.

To avoid the use of system resources, you can limit the number of times that a job can be resubmitted. You also can have the Scheduler check for connection errors or runtime errors when the job runs. Connection errors occur when the system fails to connect to the server to submit the job. Runtime errors occur when the server on which the job is running places the job in an error state. You can set up the system to monitor for both cases.

Access the Scheduling Advanced Options form.

To define when the system resubmits jobs:

1. On Scheduling Advanced Options, select the Job Resubmission tab.
2. Specify the number of minutes that elapse before the job continues or terminates, and then activate one of the following options:
 - Let the job continue.
 - Terminate the job.
 - Terminate the job and resubmit.
3. If you want to terminate the job and resubmit it after a certain period of time, select the terminate the job and resubmit after option, and enter the number of minutes that you want to elapse before the system resubmits the job.
4. Select one of the following options that apply when the job ends in error:
 - Do nothing.
 - Resubmit immediately.
 - Resubmit after.
5. Specify whether you want the system to check for connection errors, runtime errors, or both.
6. In the Max Number of Job Resubmissions field, specify the maximum number of times that you want the job to be resubmitted.
7. Click OK.

Let the job continue

Indicates how to handle a job that is in process too long.

Terminate the job

Indicates how to handle a job that is in process too long.

Terminate the job and resubmit	Indicates how to handle a job that is in process too long.
Terminate the job and resubmit after	Indicates how to handle a job that is in process too long.
Do nothing	Indicates the method for resubmitting a job if the job has an error status.
Resubmit immediately	Indicates the method for resubmitting a job if the job has an error status.
Resubmit after	Indicates the method for resubmitting a job if the job has an error status.
Check Connection Errors	Indicates the method for resubmitting a job if the job has an error status.
Max Number Of Job Resubmissions	<p>This is the maximum number of times that a job schedule instance can be resubmitted.</p> <p>For example, suppose a job is scheduled to be submitted at 12 a.m. on April 2. The scheduler is instructed to resubmit this job if it ends in error.</p> <p>However, this field is set to 3. That means that the job can only be resubmitted three times. The fourth time this job ends in error, the Scheduler will no longer submit it.</p>

Overriding Batch Application Specifications

You can specify if you want errors written to the `jde.log`. If you want errors written to the `jddebug.log`, you can set the trace level to determine what types of errors to include in the log.

You can also override the printer at which a report is printed. This feature is useful if a specific printer is down or if you want to print a report to a printer other than the default. You can specify whether a job should be printed immediately upon completion or held in the job queue to be printed later.

Also, you can override the queue to which the output of a submitted job is sent. If you want to pass parameters to a particular batch job, you can attach a report interconnect through Batch Application Specifications.

Access the Scheduling Advanced Options form.

To override batch application specifications:

1. On Scheduling Advanced Options, select the Batch Application Overrides tab.
2. Select one or more of the following options:

- `Jde.log`
- `Jddebug.log`

If you select `jddebug.log`, you must also select the `jde.log` option.

3. Complete these fields:

- UBE Logging Level

If you select `jddebug.log`, you can set a trace level to log certain levels of errors.

- Printer Name

Enter the name of the printer to which you want to print the report that the job generates. If you want to use a default printer, specify *DEFAULT*.

- Print Immediate

If you want the job output to be sent to the printer immediately, select this option.

- Job Queue

Enter the name of the job queue to which you want the job output sent.

4. Click OK.

Adding Values to a Report Interconnect

You can add values to be passed through a report interconnect into a batch process when that batch process is launched. The batch process must first contain a report interconnect.

Access Work With Scheduled Jobs form.

To add values to a report interconnect:

1. On Work With Scheduled Jobs, select the job and then select Advanced Options from the Row menu.
2. On Scheduling Advanced Options, select Parameters from the Form menu.
3. On Report Interconnect, enter the values that you want to pass to the batch process when the process runs.
4. Click OK.

Reviewing the Job Schedule

This section provides an overview of how to review and change scheduled job information and discusses how to:

- Review all job schedules.
- Change the launch status of a job.
- View job details.
- Set the job status manually.
- Reset the job schedule.

Understanding Job Schedule Reviewing

When you schedule a job that includes a recurrence pattern, the system creates a set of schedule records, or instances, for the job in the F91320 table. The F91320 table indicates the times and dates that the job will run. You can review these instances and their statuses, and also change the scheduled job information. For example, you can change the location at which you want a job to process, delete a job instance, or override any advanced functions.

Note. Because the F91320 table is also used for audit information, you can modify or delete only jobs that have not yet run.

See Also

Chapter 20, “Using the Scheduler Application,” Revising a Scheduled Job, page 255

Forms Used to Review the Job Schedule

Form Name	Form ID	Navigation	Usage
Work With Versions	W983050B	Job Scheduler (GH9015), Schedule Jobs	Locate a version that you want to review.
Work With Scheduled Jobs	W91300B	On Work With Versions, select a version and then click Select.	Review all scheduled jobs for a version.
Work With All Job Schedule	W91300M	On Work With Scheduled Jobs, select All Schedules from the Form menu.	Review all scheduled jobs for a version.
Job Schedule	W91300F	On Work With Scheduled Jobs, select the job, and then select Job Schedule from the Row menu.	Change the launch status of a job instance. Reset the job schedule.
Job Maintenance	W986110BC	On Job Schedule, select the job, and then select View Detail from the Row menu.	View details about a job, as well as the job queue, the priority in which the job will run, and the location of the report printer. From this form, you can also change the job priority or the location where the report will print.
Manually Set Job Status	W91300L	On Job Schedule, select the job instance for which you want to manually set the job status, and then select Set Status from the Row menu.	Set the job status manually.

Reviewing All Job Schedules

When you review all of the job schedules, you can view all instances of jobs that have been launched. You can even revise a job by choosing a job instance and then choosing Revise Job from the Row menu.

You can filter the job instances that you want to review by launch date, start date, and time. For example, you can review all of the job instances for today's date by entering that date in the Scheduled Start Date field. Or you can review all job instances that were launched on a certain date by entering that date in the Job Launch Date field. You can also filter job instances by scheduled job name, launch status, report name, or scheduled version.

Access the Work With All Job Schedule form.

To review all job schedules:

- On Work With All Job Schedule, filter by start date or start time by completing these fields:
 - Scheduled Start Date
 - Scheduled Start Time
- To filter by launch date or launch time, complete these fields:
 - Job Launch Date

- Job Launch Time
3. To filter by job name, launch status, report name, or scheduled version, complete these fields:
 - Scheduled Job Name
 - Launch Status
 - Report Name
 - Scheduled Version
 4. To view all scheduled jobs in all time zones, select All Time Zones from the Form menu.
 5. To view all scheduled jobs in the local time zone, select Local Time Zone from the Form menu.

Changing the Launch Status of a Job

You can change the launch status of a job. For example, you might need to put a job on hold or reschedule a job.

Access the Work With Version form.

To change the job launch status of a job:

1. On Work With Versions, select the time zone in which the job will run, and then click Select.
2. On Work With Scheduled Jobs, locate the job that you want to change.
3. From the Row menu, select Job Schedule.
4. On Job Schedule, select the job instance for which you want to change the status, and then enter a new status in the Launch Status field.
Enter *1* for a scheduled status or *50* for hold.
5. Click OK.

Viewing Job Details

Access the Job Schedule form.

To view job details:

1. On Job Schedule, select the job, and then select View Detail from the Row menu.
2. On Job Maintenance, complete the following fields, if necessary, and click OK:
 - Job Priority
 - Printer Name

Setting the Job Status Manually

As a system administrator, you can change the status of jobs if the Scheduler is not updating the launch status or if the Job Monitor is disabled.

Note. If you need to stop a job, select Work with Servers from the Form menu on the Work with Scheduled Jobs form.

Important! You should secure other users from accessing the Set Status option. Only the PeopleSoft EnterpriseOne administrator should have access to this option.

Access the Job Schedule form.

To set the job status manually:

1. On the Work With Scheduled Jobs form, select the job, and then select Job Schedule from the Row menu.
2. On Job Schedule, select the job instance for which you want to manually set the job status, and then select Set Status from the Row menu.
3. On Manually Set Job Status, complete the Scheduled Launch Status field.

Resetting the Job Schedule

If you configure a job schedule and then change your mind, you can remove the changes and regenerate the job schedule by using the previously defined recurrence pattern. The job schedule is reset to the way it was before you made the changes.

Access the Job Schedule form.

To reset the job schedule:

1. On Job Schedule, select Reset Schedule from the Form menu.

The system displays the following warning message: This will remove any custom changes to this job's schedule and regenerate the schedule using the recurrence pattern. Are you sure you want to continue?

2. Click Yes to confirm resetting the job's schedule.

Working With the Scheduler Server

This section provides an overview of the Scheduler server and discuss how to:

- Stop or restart the Scheduler server.
- Pause the job launcher or job monitor.
- Reset the Scheduler server.
- Refresh the Scheduler server settings.
- Modify the Scheduler server and monitor sleep time.

Understanding the Scheduler Server

The Scheduler server is a process that performs two distinct functions: it launches all jobs at the scheduled times, and it monitors each job's progress and ending state. These functions are started by a JDENET message, as defined in the following kernel type in the jde.ini file:

```
[JDENET_KERNEL_DEF10]
dispatchDLLName=jdekrnl.dll
dispatchDLLFunction=_JDEK_DispatchScheduler@24
maxNumberOfProcesses=1
beginningMsgTypeRange=2001
endingMsgTypeRange=2256
newProcessThresholdRequests=0
numberOfAutoStartProcesses=1
```

The Scheduler launches batch processes in a server, environment, and user combination, based on the information in the F91300 table. After the Scheduler is started, JDENET keeps it in a wait state by calling the Scheduler dispatch function every minute with an idle message. This idle message allows the Scheduler process to check whether it should launch a job or monitor the jobs that are running. In addition, JDENET sends the Scheduler any message sent from the workstation (for example, messages that new job schedules were added).

You can stop, reset, restart, and refresh the Scheduler server. For example, if the server goes offline, it needs to be reset. You can also modify the server and monitor sleep time, specifying how many seconds you want JDENET to wait until it checks to see if it needs to initialize, or wake up, the Scheduler server.

You also might encounter situations for which you need to activate or deactivate the Job Launcher or Job Monitor. For example, you might need to take down the servers to which you submit jobs and for which you want to avoid unnecessary connection errors when jobs are submitted.

You can also change the `jde.ini` file to enable the Scheduler to restart automatically by changing the `numberOfAutoStartProcesses` line. If you enable this feature, and the server on which the Scheduler server is running comes down, the Scheduler server automatically restarts when the server comes back up, instead of having to be restarted manually. When the Scheduler server restarts, the Scheduler checks the F91320 table to determine if it should restart on that server. If not, the Scheduler shuts down.

JDENET handles the calls to initialize the Scheduler server. The JDENET process either sends a message to initialize the Scheduler to launch a job if it receives a message that table F91320 has changed, or it sends an idle message if no change is detected. For faster response time, you can decrease the number of seconds that you want JDENET to wait until it checks to see if table F91320 has changed.

Note. This application is for administrators only. You should secure users from accessing the Scheduler server application.

Control Record

A control record is a job record in the F91300 table. It is named `*SCHEDULE` and is hidden from the user. The `*SCHEDULE` record contains information about the state of the Scheduler processes on the server, and it is the method of communicating to those processes.

For example, when the launch loop starts on the server, it sets a flag in this record to indicate that it is up and running. You can end the launch loop by toggling the corresponding end process flag (such as Job Launcher Status or Job Monitor status) from the Form menu on Scheduler Server Control. The next time that the launch loop fetches the control record, it finds the flag, resets both flags, and ends.

If the system does not find the control record when it is fetched, the record is recreated by P91300 when entering the Scheduler Server Control form. In addition, if the record is corrupt, the aforementioned function is called to recreate it. The sleep times for the job monitor are reset to 15 minutes, and the audit information in this record is updated with the user ID set to `SCHEDULER`.

Dispatch Function

The dispatch function handles the incoming message from the workstation and starts the requested process. The JDENET process either sends a message to initialize the Scheduler, signals that the F91320 table has changed, or gives an idle message. The idle message is sent every minute unless one of the other messages is sent. When the idle message is sent, the dispatch function checks to see if the launch loop or job monitor needs to be called. If neither does, control is given back to JDENET.

Launch Loop

The launch loop function selects all of the jobs up to the current time. It then loops through the selected records and launches the active jobs if they have not expired. After launching all current jobs, the launch loop fetches all future jobs sorted by start time. If the fetch succeeds, the next select time (NST) is set to the difference between the current time and the start of the next job. If the fetch fails, the NST is set to zero, which indicates that this function should be run the next time that any record is added to or updated by the F91320 table. In addition to launching jobs, the launch loop checks the control record periodically to see if it should exit.

The launch loop also looks for updates of all the schedule instances (F91320 records) and job headers (F91300 records) that it fetches. After the launch loop has processed these records, it then commits any changes and unlocks all of the records.

Job Monitor Loop

The job monitor loop monitors the ending statuses of the launched jobs and re-launches those that end in error if requested to do so by the user. This loop cycles through the internal job list that the job launch loop populates. In addition, it terminates jobs that run too long, if requested to do so. A job cannot be re-launched for more times than specified in the F91300 record of the job.

Like the launch loop, the job monitor loop periodically fetches the control record to see if it should end.

See Also

EnterpriseOne Tools 8.94 PeopleBook: Development Tools: Additional Tools and Topics, “Creating Report Interconnections”

EnterpriseOne Tools 8.94 PeopleBook: Development Tools: Application Development, “Debugging EnterpriseOne Applications,” Using Debug Tracing

Forms Used to Work With the Scheduler Server

Form Name	Form ID	Navigation	Usage
Work with Versions	W983050B	Job Scheduler (GH9015), Schedule Jobs (P91300)	Locate the version that specifies the time zone in which the scheduled jobs run.
Work with Scheduled Jobs	W91300B	On Work with Versions, select a version and then click Select.	Access the Scheduler Server Control form.
Scheduler Server Control	W91300G	On Work with Scheduled Jobs, select Scheduler Server from the Form menu.	Stop, restart, reset, refresh, or modify the Scheduler server. Pause the job launcher and job monitor. Modify the Job Monitor sleep time.

Stopping or Restarting the Scheduler Server

Access the Work with Versions form.

To stop or restart the Scheduler server:

From the Job Scheduler menu (GH9015), select Schedule Jobs (P91300).

1. On Work with Versions, select the version that specifies the time zone in which the scheduled jobs run, and then click Select.
2. On Work with Scheduled Jobs, select Scheduler Server from the Form menu.
3. On Scheduler Server Control, do one of the following:
 - To stop the server, select Stop Scheduler from the Form menu.
 - To restart the server, select Start Scheduler from the Form menu.
4. Click OK.

Pausing the Job Launcher or Job Monitor

Access the Scheduler Server Control form.

To pause the job launcher or job monitor:

Note. You might want to pause the job launcher or job monitor, such as when you want to take down the servers to which you submit jobs, and you want to avoid server connection errors that might occur while those servers are down. When you pause the job launcher, the Scheduler stops looking at the F91320 table for jobs to launch. When you pause the job monitor, the Scheduler stops monitoring the status of launched jobs.

1. On Scheduler Server Control, select Pause Job Launcher from the Form menu to pause the job launcher.
2. To pause the job monitor, select Pause Job Monitor from the Form menu.
3. Click OK.

Resetting the Scheduler Server

Access the Scheduler Server Control form.

To reset the Scheduler server:

Note. You reset the Scheduler server after you change the status of the Job Monitor or Job Launcher. For example, if you change the status of the Job Monitor, you would select Reset to refresh the settings on the server.

1. On Scheduler Server Control, select Reset from the Form menu.
2. Click OK.

Refreshing the Scheduler Server Settings

Access the Scheduler Server Control form.

To refresh the Scheduler server settings:

Note. When you refresh the Scheduler server settings, the server refreshes its cache of launched jobs, and closes and restarts all environment and table handles. It is a refresh of the server's internal structures. You might want to refresh the Scheduler server settings if you had to restart the server.

1. On Scheduler Server Control, select Refresh from the Form menu.
2. Click OK.

Modifying the Scheduler Server and Monitor Sleep Time

Access the Scheduler Server Control form.

Note. Sleep time is the time that the Scheduler server or monitor is idle.

Scheduler Sleep Time	This field indicates the number of seconds that the scheduler server will sleep (or idle). For example, if this field is set to 60 seconds, the Scheduler server checks every 60 seconds to see if it needs to launch or monitor jobs. The default is 60, and it must be greater than zero.
Job Monitor Sleep Time	This field indicates the number of minutes the job monitor will pause between job status checks.

Working with Daylight Savings Rules

This section provides an overview of working with daylight savings rules and discusses how to:

- Add daylight savings rules
- Revise daylight savings rules

Understanding How to Work with Daylight Savings Rules

Daylight savings rules tell the system how each locale implements its daylight savings time. The Scheduler uses these rules, along with time zone information, to determine when jobs should run on a particular server.

You can add a new daylight savings rule or modify an existing one.

Forms Used to Work with Daylight Savings Rules

Form Name	Form ID	Navigation	Usage
Work With Daylight Savings Rules	W00085A	Job Scheduler (GH9015), Daylight Savings Rules (P00085)	Click Add to access a form for adding a new daylight savings rule. Select an existing rule and click Select to access a form to revise an existing rule.
Add Daylight Savings Rule	W00085B	On Work With Daylight Savings Rules, click Add.	Add a daylight savings rule.
Daylight Savings Rule Revisions	W00085B	On Work With Daylight Savings Rules, select an existing rule and click Select.	Revise a daylight savings rule.

Adding Daylight Savings Rules

Access the Work With Daylight Savings Rules form.

To add a daylight savings rule:

1. On Work With Daylight Savings Rules, click Add.
2. On Add Daylight Savings Rule, complete these fields:
 - Rule Name
 - Description
3. In the Rule Type area, select the method that you want to use to determine a daylight savings rule:
 - By Day of Week Instance
 - By Day of Month
4. Depending on the method that you chose, complete the remaining fields to specify when daylight savings starts and ends.
5. Click OK.

Revising Daylight Savings Rules

Access the Daylight Savings Rule Revisions form and revise the appropriate fields.

Rule Name	Unique name identifying a daylight savings rule. Use daylight savings rules to adjust time for a geographic and political locale.
By Day of Week Instance	<p>A code that indicates the method that is used to determine a daylight savings rule.</p> <p>By Day of Week Instance indicates that daylight savings starts and stops on a certain day of the week for a certain month, such as the first Sunday of April to the first Sunday of October. By Day of the Month indicates that daylight savings starts and stops on a certain day of a certain month, such as April 3 to October 10.</p>
By Day of the month	<p>A code that indicates the method that is used to determine a daylight savings rule.</p> <p>By Day of Week Instance indicates that daylight savings starts and stops on a certain day of the week for a certain month, such as the first Sunday of April to the first Sunday of October. By Day of the Month indicates that daylight savings starts and stops on a certain day of a certain month, such as April 3 to October 10.</p>

Running Scheduler Reports

Run the Scheduled Jobs report when you want to review a summary of scheduled jobs and their statuses. You can use processing options to specify whether to run this report based on UCT or local time. You also can adjust for daylight savings time.

If you want to purge records from the F91320 table, run the Scheduler Purge program. You can run the purge program in proof mode or final mode.

Printing the Scheduled Jobs or Purge Scheduled Jobs Report

Access the Work With Batch Versions - Available Versions form.

To print the Scheduled Jobs or Purge Scheduled Jobs report:

1. On Work With Batch Versions - Available Versions, select a version in the detail area, and then click Select.
2. On Version Prompting, select one or both of the following options, and then click Submit:
 - Data Selection
 - Data Sequencing
3. On Report Output Destination, select one of the following options, and then click OK:
 - On Screen
 - To Printer

CHAPTER 21

Understanding Media Objects and Imaging

This chapter discusses:

- Media objects.
- Imaging.
- Media object queues.
- Media object tables.
- Language considerations for media objects.

Media Objects

PeopleSoft EnterpriseOne media objects and imaging features enable you to attach useful information to an application, including information that might currently exist as a paper-based document. The media objects feature enables you to attach the information to applications, forms and rows, and Object Librarian objects. The imaging feature, within media objects, gives you flexibility to create a more efficient method of information storage.

This table describes the types of information that you can attach to a grid row or a form:

Text	Media objects provide a word processor that lets you create a text-only attachment. For example, you can use a text attachment to provide specific instructions for a form or additional information about a record.
Image	Images include files such as Windows bitmaps, Graphics Interchange Format (GIF) files, and JPEG files. These files might represent electronically created files, as well as scanned images of paper-based documents.
OLE	<p>Media objects can be files that conform to the OLE standard. OLE enables you to create links between different programs. By using these links, you can create and edit an object from one program in a different program. EnterpriseOne provides the links that you need to attach OLE objects.</p> <p>You attach OLE media objects at the base form level. Media objects attached at this level are attached to a form and not to any data that might appear in the form. You can attach media objects to a detail area or a form, but the files themselves exist in separate directories. The only file information that is included with the application to which the OLE object links is the path to the supporting file.</p> <p>You can only use OLE objects that you properly register and install as OLE objects through EnterpriseOne.</p>

Shortcuts	A shortcut is a link that opens an EnterpriseOne application. Within media objects, you can only attach EnterpriseOne shortcuts; that is, you cannot attach Windows shortcuts to media objects.
Uniform Resource Locations (URL) and files	Media objects can be links to web page URLs or other related files. When a developer attaches a URL media object to a control object on a form, the web page appears as part of the form. When a user attaches a URL to a form or Object Librarian object, the media object acts as a link to the URL.

System administrators can also set up templates. A template might include attachments of its own, such as images and shortcuts. For example, you can create a letterhead and a standard form for a memo. You might create a shortcut in the template to provide access to an application that uses data specific to the information that you add to the template.

PeopleSoft EnterpriseOne Text Items

Text items are items that you create using the PeopleSoft EnterpriseOne media objects word processor. They do not require media object queues. The F00165 table contains both the associated key value of the data record to which the text media object is attached, and the text itself. Text items that originate from applications external to EnterpriseOne (for example, Microsoft Word or WordPad) must be stored as OLE objects.

Imaging

The imaging capabilities available in EnterpriseOne enable you to link to a third-party imaging product. Imaging systems enable you to scan and electronically store paper-based information. For example, this information might include documents such as sales orders, purchase orders, vendor invoices, and product schematics. EnterpriseOne imaging integration includes a media objects viewer and a third-party product that provides scanning and searching interfaces to enable you to find and display images. Implementation of imaging also provides a view of integrated images by using the viewer of the native imaging product.

When you use a third-party vendor, the F00165 table stores the reference to image attachments, but the third-party software controls the search and retrieval of images.

Media Object Queues

PeopleSoft EnterpriseOne media object queues enable the storage location of media objects to be tracked by reference rather than physical network location, which simplifies the administration of media location. For example, the location for media objects on the server can change, and the change is reflected in only one place in EnterpriseOne.

You must define a media object queue to identify the pointer to the location where the actual image files or OLE objects reside. Media object queues provide the system administrator with the ability to easily manage the storage of media objects in the software. Within EnterpriseOne, you must set up media object queues to use images that are outside of the imaging product's domain (for example, scanned images). You can set up media object queues for these types of objects:

- Image objects (actual files)

- OLE objects (links to files)
- URLs (internet addresses)

Image Media Objects

Image media objects are individual files that are accessed and viewed by using a third-party imaging product. These objects are stored in locations defined with a name and a network-qualified path. For example, if all of the images for financial applications are stored in a directory on the network called `\\server1\financials\images`, an image media object queue could be defined as follows:

- Path: `\\server1\financials\images`
- Name: `FIN_IMAGES.BMP`

OLE Media Objects

OLE media objects are individual objects that are created and viewed by using an OLE-compliant application outside of EnterpriseOne. In EnterpriseOne, the OLE object attached to a row or form is actually a link to the OLE object that resides in a media object queue. The distinction between OLE objects and non-OLE objects is important because, other than graphics files, you cannot attach non-OLE objects from EnterpriseOne if they are not compliant. Examples of valid OLE objects are Microsoft Windows OLE-compliant applications such as Word, Excel, PowerPoint, and Visio. Other examples include sound or video files (.wav or .avi extensions).

URL Media Objects

URL media objects are internet addresses that point to web sites that are identified by industry-standard URLs. When defined in the media object table, these addresses can be connected to internet locations.

Media Object Tables

Media object queues typically represent network directory locations for EnterpriseOne media object files, such as OLE objects and images. The two media object tables are F98MOQUE and F98101.

The media object queues are stored in the Media Object Queues table, which, along with the Imaging Constants table, should be located in the system data source. The Media Object Queues table contains the associated key value of the data record to which the media object is attached, the image reference, and the OLE reference. The image reference and the OLE reference are queue names. The queue name is used to access the Media Object Queue table for the location of the OLE object or image.

Media object keys are stored in the F00165 table. Media object characterization properties are stored in the F00166 table. The F00167 table stores information indicating which categories the system activates for any given data structure.

Language Considerations for Media Objects

If you create a custom application that you want to enable for media object language handling, you must include a data item language preference (alias LNGP) in the generic text data structure that you create.

When you design an application, you can allow the end user to add separate and unique media objects to the same record or different records, based on the language chosen.

If language (LNGP) is not a database column, then you define the media object (GT) data structure to include language as part of the data structure. You place a data dictionary control (LNGP) on the application as a filter field, which should then be loaded with the system value for language. When you design the application this way, you attach two separate media objects, based on the language, to the same record.

If language (LNGP) is a database column, then you include LNGP (database) as a filter field, but you must add a separate record to the database table along with its media object attachment. The media object data structure still contains language as part of the key to retrieve the media object attachment. In both cases, the language filter fields (LNGP) must be loaded with the system value for language. LNGP must be built into the key and not associated with the LNGP column in the F00165 table.

For any database table that contains language as part of its key, you can attach media object functionality for records with different languages. For example, you can create one record for English and a copy of the record for French with unique media object attachments. For tables that do not include language as part of the key to that table, you can have media object languages.

CHAPTER 22

Setting Up Media Objects and Imaging

This chapter provides an overview of media object processing and imaging and discusses how to:

- Enable EnterpriseOne to use media objects.
- Add a language-specific media object attachment.
- Set up media object queues.
- Set up imaging.

Understanding Media Object Processing

To use media objects, PeopleSoft EnterpriseOne requires a set of event rules to process the media objects. This processing includes:

- Tracking where the media object files are stored.
- Tracking which media objects are attached to which objects (rows, forms, and reports).
- Indicating which objects have attachments.
- Creating or viewing attachments.

You can set up EnterpriseOne to use standard processing for media objects, which enables you to bypass all event rules that are required to implement media objects. All of the required information is gathered from a form in Form Design Aid and does not require you to define any event rules. Standard processing:

- Standardizes the usage of media objects across forms.
- For any detail area, places a paper clip button on the row header if a media object is defined for that row.
- For a form, places a button in the status bar if a media object is defined for the form.
- Enables you to attach documents to the form or to a row in the detail area.
- Enables you to double-click the paper clip in a row to view media objects for that row.
- Enables you to click the paper clip in the status bar to view media objects for the form.

If you choose not to use standard processing for a form, you can still develop a system for handling media objects by using existing event rules or event rules that you develop.

EnterpriseOne uses the F00165 table to store link records for media objects and imaging. You must define the media object data structure by using a unique key structure so that the F00165 table can store data correctly. The layout of this table is as follows:

```
GTxxx || F4211Keys || The media object text
```

Where:

GT (generic text) xxx is the naming convention used when defining a media object data structure.

F4211Keys is what the system uses to access the unique media object attachment for that particular record. The keys typically match what the unique key would be in the F4211 table for each detail line.

The media object text is the actual text attachment that stores information typed in by the user.

In addition to the media object categories provided by EnterpriseOne, you can define as many as 40 more. Users can associate these categories with a media object to group certain media objects and to enable other users to search for specific media objects. User defined categories reside in the F00166 table and are referenced using each object's unique key. The default titles for these categories are Category Codes 1-30, Dates 1-5, and Numeric 1-5.

Prerequisite

To enable users to see the media object paper clip column on a form, clear the Hide Row Headers option on the grid properties for the form.

Enabling EnterpriseOne to Use Media Objects

In Object Management Workbench, access an application on which you want to enable media objects and open it in Form Design Aid.

To enable EnterpriseOne to use media objects:

1. In Form Design Aid, select Media Objects Setup from the Form menu.
2. On Media Objects Setup, select the Enable Automatic Media Object Functionality option.
Selecting this option enables imaging and activates the other fields on the form.
3. On Media Objects Setup, select one of these options:
 - Media Objects Only
Choose this option if you do not want to interface with third-party products that include imaging. If you choose this option, you will only be able to use media objects that are defined for and supported from within EnterpriseOne.
 - Document Handling Only
Choose this option if you are developing a form that is enabled for media objects using functionality in event rules and you want to bypass standard processing.
 - Media Objects & Document Handling
Choose this option if you want to enable standard processing later. You must delete all of the event rules for media objects when you choose this option.
4. Click Edit mode or Display mode.
Edit mode allows the user to make changes; display mode is read-only.
5. Click Define Form Key.
The System Functions form appears. This form is identical to the parameter definition form used to define system functions in event rules, except that it includes only the Media Object header.
6. On the Function Selection tab, double-click the Media Object Structures folder.
A list of all currently defined data structures for Media Objects appears.
7. Choose the appropriate structure and define it on the Parameter Mapping tab.

Adding a Language-Specific Media Object Attachment

Open the application to which you want to add a language-specific media object attachment.

To add a language-specific media object attachment:

1. On the application that you want to use, type a language in the filter field.
2. Click Add.
3. Add multiple records if you want the attachment for multiple languages or base.

Setting Up Media Object Queues

This section discusses how to:

- Add a media object queue.
- Define the location of a media object queue.
- Delete a media object queue.

Forms Used to Set Up Media Object Queues

Form Name	Form ID	Navigation	Usage
Work With Media Object Queues	W98MOQUEA	System Administration Tools (GH9011), Media Object Administration, Media Object Queues (P98MOQUE)	Add a media object queue. Locate existing queues and delete queues.
Media Object Queue Revisions	W98MOQUEB	On Work With Media Object Queues, click Add.	Add information for a new media object queue. Define the location of a media object queue.

Adding a Media Object Queue

Access the Work With Media Object Queues form.

To add a media object queue:

1. On Work With Media Object Queues, click Add.
2. On Media Object Queue Revisions, complete these fields:
 - Queue Name
 - Queue Path On-Line
 - Queue Path Off-line
 - Type
 - On-Line Access Type
 - Off-Line Access Type

3. Click OK.

Queue Name

The value entered is used to define a media object queue name where images may be found. The queue name is a symbolic reference only. The media object queue name is one-half of a properly defined media object queue. The other half is the media object path.

Note. OLEQUE is a reserved queue name. It must be defined as it is used as the default queue name in the OLE object attachment mode of media objects. It is mandatory that this queue name be defined in order to use OLE object attachments.

Queue Path On-Line

A path that points to the location of OLE objects, images, or URLs. The queue path is the second half of a properly defined queue for a media object. The first half is the name of the media object. A valid queue path for a network location might be `\\server1\share3\images\financial`. To set the queue for a CD ROM, use `cd:` in the pathname; the system automatically substitutes the appropriate drive letter when it resolves the path.

The queue path and queue name are stored in the F98MOQUE table. Object Configuration Manager controls the location of this table. The system reads the F98MOQUE table to determine name of the queue and the location of the associated OLE objects, images, or URLs.

Queue Path Off-line

Identifies the local path that points to the location of OLE objects, images, or URLs. The queue path is the second half of a properly defined queue for a media object. The first half is the name of the media object. A valid queue path when working off-line might be `d:\data\media\images`.

The queue path and queue name are stored in the F98MOQUE table. Object Configuration Manager controls the location of this table. The system reads the F98MOQUE table to determine name of the queue and the location of the associated OLE objects, images, or URLs.

Defining the Location of a Media Object Queue

Access the Work With Media Object Queues form.

To define the location of a media object queue :

1. On Work With Media Object Queues, if an OLE queue does not exist, click Add.
2. On Media Objects Queue Revisions, complete these fields:
 - Queue Name
 - Queue Path On-Line
 - Queue Path Off-line
 - Type
 - On-Line Access Type
 - Off-Line Access Type
3. Click OK.

4. If you want to change an existing media object queue, on Work With Media Object Queues, click Find to display a list of queue names and their paths.
5. Choose the queue name that you want to modify and click Select.
6. On Media Object Queue Revisions, change the information in the Queue Path On-Line field to reflect the new location, and then click OK.

Deleting a Media Object Queue

Access the Work With Media Object Queues form.

To delete a media object queue:

1. On Work With Media Object Queues, click Find.
2. Choose the queue name that you want to delete.
3. From the Form menu, choose Delete.

Deleting a media object queue deletes only the definition of the queue, not the associated path or objects themselves.

Setting Up Imaging

This section contains an overview of imaging and the flow for imaging systems and discusses how to enable imaging in media objects.

Understanding Imaging

One way to attach images to EnterpriseOne forms and grid rows is to use the Image function of the Media Objects feature; however, this solution is not designed for use with sophisticated document handling systems. See the PeopleSoft web site for a complete list of imaging vendors partnered with PeopleSoft.

The software uses the OLE client/server model to interface with third-party document handling systems, including the OLE client interface and the OLE server. For the currently supported imaging systems, EnterpriseOne meets these minimum design goal tasks:

- Search

The search mechanism locates a document stored in the indexing system of a document handling system. The search mechanism navigates the storage structures of the document handling system so that the user can find a particular document or set of documents easily.

- Link

Upon a successful search operation, the link mechanism returns the unique document identifier to EnterpriseOne. This identifier is stored with the transaction.

- View

The view mechanism passes the unique document identifier to a document viewing mechanism so that the user can view the document.

Customers with requirements for third-party imaging systems other than those that the software currently supports can design custom OLE automation servers for interfacing purposes. The OLE server can be written in any OLE-compliant language. PeopleSoft EnterpriseOne has a published set of APIs to enable you to develop compatible middleware applications. The published APIs are described in a Windows help file that is installed with the software.

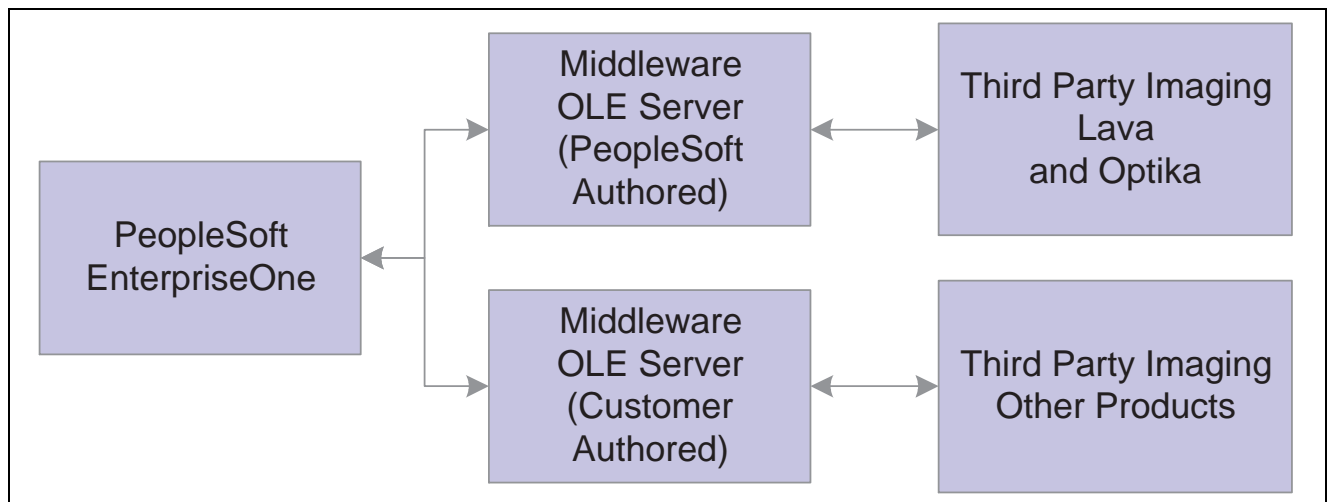
Understanding Flow for Imaging Systems

You can use imaging with a document handling system. The imaging system enables you to automatically scan and catalog documents. The system indexes the images so that you can recall them, based on certain sets of criteria. For example, you might index images according to type, department, and date. You can recall, view, and analyze an image at any given time. For example, in a transaction entry scenario, you might scan a paper-based file when the document enters the mailroom so that a data entry clerk can retrieve the image to use as a source document.

EnterpriseOne can retrieve and view documents based on selection criteria that are defined by the user. A linking system associates the EnterpriseOne transaction to the document for later retrieval and reference. You can attach a transaction identifier with the scanned image in the document handling system to enable a user to access an application directly from the image.

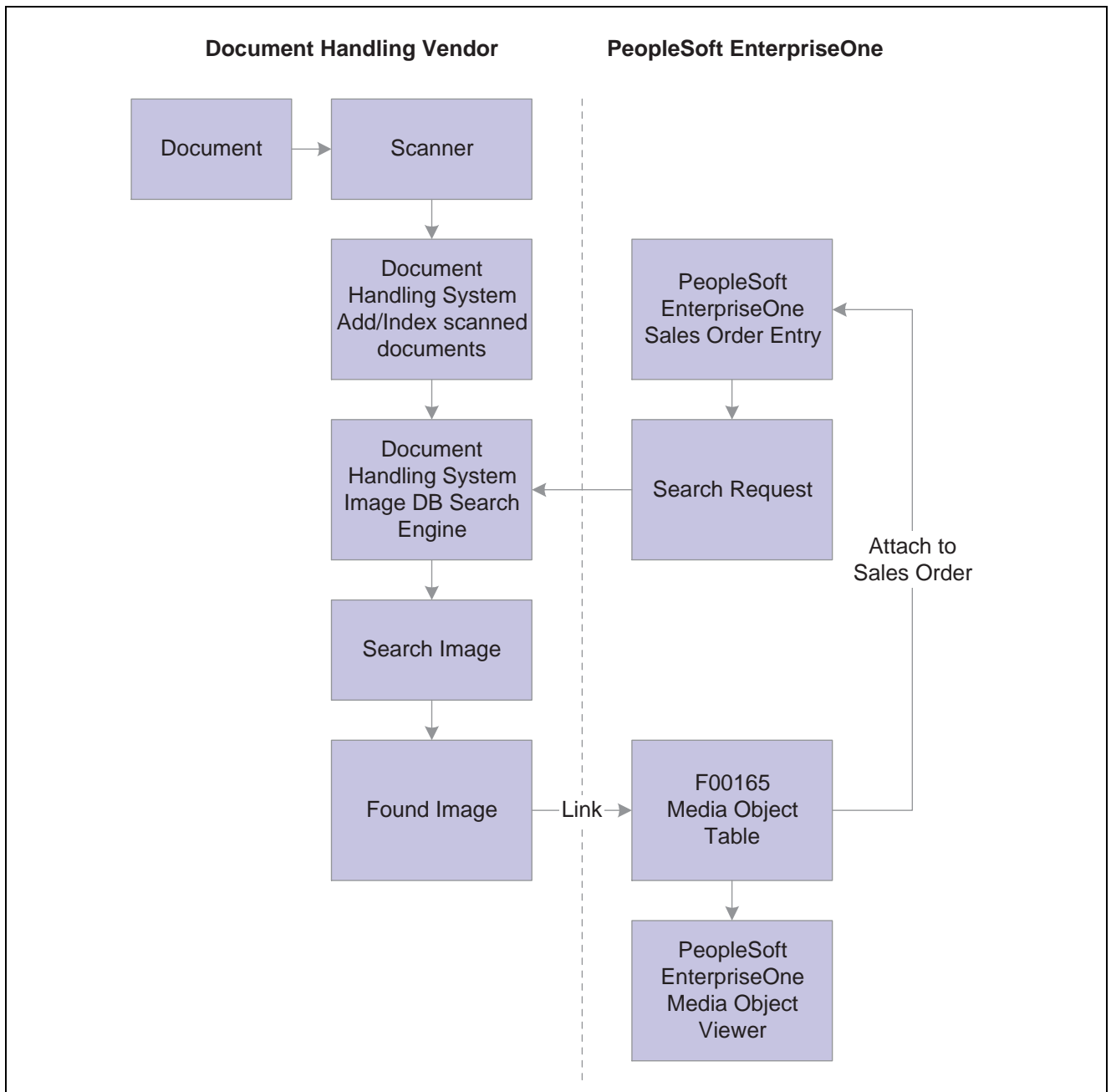
You set up imaging by enabling the imaging at the system level. For an imaging system to be enabled, it must have a registration record in the F98101 table.

This illustration explains how the software supports third-party imaging products through a middleware OLE server layer. Customers also can create their own OLE servers to support additional imaging systems:



EnterpriseOne imaging architecture

This diagram is a typical imaging scenario:



Imaging process flow

Forms Used to Set Up Imaging

Form Name	Form ID	Navigation	Usage
Work With Media Object Queues	W98MOQUEA	System Administration Tools (GH9011), Media Object Administration, Media Object Queues (P98MOQUE)	Set up imaging.
Imaging Constants Revisions	W98101A	On Work With Media Object Queues, choose Imaging from the Form menu.	Enter information about the imaging system and enable the imaging system.

Enabling Imaging in Media Objects

Access the Work With Media Object Queues.

To enable imaging in media objects:

1. On Work With Media Object Queues, from the Form menu, select Imaging.
2. On Imaging Constants Revisions, complete these fields:
 - Imaging System Vendor
 - Imaging Vendor Description
 - Image Program ID/DLL
3. Select these options:
 - Imaging Active
 - OLE

Imaging System Vendor	The name of the imaging system vendor that you are using on the system.
Imaging Vendor Description	The description of the imaging system vendor that you are using on the system.
Image Program ID/DLL	If the image type is an OLE, enter the program ID that uniquely identifies the imaging system in the system registry. If the image type is a DLL, enter the imaging system DLL name.
Imaging Active	Indicates whether an imaging system is currently active for the system.
OLE	Indicates the type of interface used by the imaging system

CHAPTER 23

Administering Text Search Indices

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

- Define text search indices.
- Build text search indices.
- Define text search properties.

Understanding Verity

Verity is the text search engine used by PeopleSoft EnterpriseOne. Verity takes information from the tables and associated media objects and builds a text search index. When a text search is initiated, it goes through the text search index and returns database records that match the search criteria. In EnterpriseOne, Verity uses a business view-data source pair to retrieve table data.

Text search indices exist as folders on a file system, so text search indices must be accessible using a path name to both the enterprise server and the web server. Administrators must designate the locations of these folders by specifying the base folder in Text Search Properties.

Defining Text Search Indices

This section provides an overview of text search indices and discusses how to:

- Designate data sources for a business view.
- Define media objects for a text search index.
- Define languages for a text search index.

Understanding Text Search Indices

To create a text search index, define the following items:

- Business view

To be able to perform a text search over a business view, the developer must select the Text Search option on the business view's properties form in OMW. Otherwise, the business view is not available for a text search.

See *EnterpriseOne Tools 8.94 PeopleBook: Development Tools: Tables and Business Views*.

- Data source

The data source tells Verity where to search for the data defined in the business view. If you do not select a data source, Verity searches the default data source defined in the OCM mapping.

- **Media objects**

To associate media objects with a business view-data source pair, use the Text Search Index Media Object Queue Revisions form. If no queues are specified, then all queues will be scanned.

- **Languages**

To build the index for any languages other than your base language, enter the language on the Text Search Index Language Revisions form.

Forms Used to Define Text Search Indices

Form Name	Form ID	Navigation	Usage
Work With Text Search Indices	W95800B	Text Search Administration menu (GH9077), Text Search Indices	View and select text search business views with the associated data sources. Build, clear, and optimize text search indices.
Text Search Index Revisions	W95800A	On Work with Text Search Indices, select a business view.	Edit data sources for each business view.
Text Search Index Media Object Queue	W95800E	On Work with Text Search Indices, highlight a data source, then select Media Object Queues from the Row menu.	Edit text search indices for media object queues
Text Search Index Language Revisions	W95800F	On Work with Text Search Indices, highlight a data source, then select Languages from the Row menu.	Edit text search indices for language.

Designating Data Sources for a Business View

Access the Text Search Index Revisions form.

Text Search Business View Displays the business view selected using the Work with Text Search Indices form.

Text Search Data Source The text search data source defined for the Text Search business view.

Defining Media Objects for a Text Search Index

Access the Text Search Index Media Object Queue Revisions form.

Text Search Business View The business view selected using the Work with Text Search Indices form.

Text Search Data Source The data source selected using the Work with Text Search Indices form.

Media Object Queue Name The name of the media object queue from the table F98MOQUE.

Defining Languages for a Text Search Index

Access the Text Search Index Language Revisions form.

Text Search Business View	The business view selected using the Work with Text Search Indices form.
Text Search Data Source	The data source selected using the Work with Text Search Indices form.
Language	The user defined code indicating the language.
Description	The name of the language.

Building Text Search Indices

There are four types of builds you can perform:

- Full
- Incremental
- Optimize
- Clear

A full build indexes all the data referenced by a business view and creates a new text search index or replaces an existing text search index. You should schedule full builds regularly, depending on the frequency with which the data changes.

Some applications automatically perform incremental builds. An incremental build takes data entered since the last full build and adds it to the end of the text search index. This makes the data available for searching, but each time an incremental build runs, it decreases the efficiency of the text search index. To optimize the efficiency of the text search index, you need to run an optimize build.

An optimize build takes the data entered since the last full build and re-indexes it. This increases text search efficiency and ensures that text searches cover recently added data. An optimize build is not as resource-intensive as a full build, so you can schedule it more frequently.

A clear build removes all data from the text search index. Under normal circumstances you would not clear a text search index, except to free file system storage. Before you can search again, you need to do a full build. However, if you do a search after a clear build, there is no data in the index to return.

You can perform builds manually or schedule them to occur automatically. The manual Build options are off the Report and Row menus. Schedule builds using the EnterpriseOne Scheduler by running the following UBEs:

- R958001 — XJE001 (Full Build).
- R958001 — XJDE002 (Optimize).
- R958001 — XJDE003 (Clear).

Defining Text Search Properties

This section provides an overview of text search properties and discusses how to:

- Add a new text search business view-data source pair.
- Define stop words.
- Define synonyms.
- Define topics.

Understanding Text Search Properties

There are three properties you can define for a Verity search:

- **Stop Words**

Stop words are words that are too common to search for. For example, if every service ticket uses the word “broken”, you would not search on “broken”. Similarly, if you only sold automobiles, searching sales receipts for the words “automobile” or “car” would be useless. Instead, you might search for specific makes and models of automobiles. By making “car” and “automobile” stop words, if you entered the search “1998 Ford Mustang Car”, the system would only search for “1998 Ford Mustang”, taking out the common word, “car”. Stop words reduce the required file system storage for text search indices and improve search performance.

- **Synonyms**

Synonyms are words that mean the same thing. For example, in a motorcycle dealership, the words “bike”, “chopper”, and “hog” all refer to a motorcycle. Motorcycle is the thesaurus word, that is the word all the synonyms point to. “Bike”, “chopper”, and “hog” are the synonyms. When a user enters the search word “chopper”, all records containing “motorcycle”, and any of its synonyms are returned.

- **Topics**

To define topics you need Verity software not provided with EnterpriseOne. Please reference the documentation Verity provides for more information on topics and topic outline files.

Verity has predefined common stop words and synonyms for each language supported. You only need to define those that are specific to your business.

You can define synonyms and stop words globally or for specific business view-data source pairs.

Forms Used to Define Text Search Properties

Form Name	Form ID	Navigation	Usage
Work with Text Search Properties	W95820A	Text Search Administration menu (GH9077), Text Search Properties	View, add, and select text search business views-data source pairs and define maximum results and base folders.
Text Search Properties Revisions	W95820B	From Work with Text Search Properties, click Add.	Add a new text search business view-data source pair and define maximum results and base folder.
Work with Text Search Stop Words	W95820E	From Work with Text Search Properties, select Stop Words from the Row or Form menu.	When entered from the Row menu, view the stop words defined for a text search business view-data source pair or global stop words. When entered from the Form menu, view and edit stop words already set up in the system.
Work with Text Search Synonyms	W95820C	From Work with Text Search Properties, select Synonyms from the Form or Row menu.	When entered from the Row menu, view the synonyms defined for a text search business view-data source pair, or global synonyms. When entered from the Form menu, view and edit synonyms already set up in the system.
Work with Text Search Topics	W95820I	From Work with Text Search Properties, select Topics from the Form or Row menu.	When entered from the Row menu, view the topics defined for a text search business view-data source pair, or global topics. When entered from the Form menu, view and edit topics already set up in the system.

Adding a New Text Search Business View-Data Source Pair

Access the Text Search Properties Revisions form.

Text Search Business View	The name of the business view of the business view-data source pair from which to build the text search indices.
Data Source	The name of the data source of the business view-data source pair from which to build the text search indices.
Base Folder	The folder to contain the text search index. This folder must be accessible to both the enterprise server and the web server.

Max Results The maximum number of matches to be returned from this text search index.

Defining Stop Words

Access the Work with Text Search Stop Words form.

Global This option defines stop words for all business view-data source pairs.

Business View/Data Source Specific This option defines stop words for only one business view-data source pair.

Text Search Business View The business view used to build the text search index.

Text Search Data Source The database used to build the text search index.

Language The language defined for the text search index.

Defining Synonyms

Access the Work with Text Search Synonyms form.

Global This option defines synonyms for all business view-data source pairs.

Business View/Data Source Specific This option defines synonyms for only one business view-data source pair.

Text Search Business View The business view used to build the text search index.

Text Search Data Source The database used to build the text search index.

Language The language defined for the text search index.

Defining Topics

Access the Work with Text Search Topics form.

Global This option defines topics for all business view-data source pairs.

Business View/Data Source Specific This option defines topics for only one business view-data source pair.

Text Search Business View The business view used to build the text search index.

Data Source The database used to build the text search index.

Language The language defined for the text search index.

CHAPTER 24

Using the Universal Table Browser

This chapter provides an overview of the Universal Table Browser and discusses how to:

- View the data in tables.
- View column properties in a table.

Understanding the Universal Table Browser

To view the data in tables in different databases, use the Universal Table Browser. This tool lets you verify the existence of data in a table, as well as determine the structure of the table. The Universal Table Browser uses JDEBASE APIs to retrieve data from the database, making it independent of the database that you access.

Viewing the Data in Tables

In PeopleSoft Solution Explorer, access the Application Development (GH902) menu, select Object Management, and then double-click Universal Table Browser.

Note. All column and row security that you set up using Security Workbench applies to the Universal Table Browser.

To view the data in tables:

1. On Universal Table Browser, select Open Table from the File menu.
2. On Table and Data Source Selection, complete these required fields:
 - Table
 - Data Source
3. Select the Format Data option.

The query by example (QBE) feature functions as in any other EnterpriseOne application. For example, you can enter *>50* in the ABAN8 column QBE to display records with an address book number that is greater than 50. You can enter *F** in the ABALPH column QBE to display records with an alpha name that begins with the letter F.

The column sequence and column width features function as in any other EnterpriseOne application. You can rearrange the columns. For example, you might want to move a column that you use often from the end to the beginning, or move a column next to an associated column. You also can size columns.

Data Source

A valid data source in which the table resides. This default value is obtained from the OCM settings in the current environment. Use the visual assist to enable the data search form, and select any EnterpriseOne data source.

Format Data

Indicates whether you want the Universal Table Browser to format portions of the data (default) or whether you want to view raw data.

Formatted: The Universal Table Browser displays the data according to the specifications of the EnterpriseOne data dictionary item. For example, assume that the data item PROC is a numeric field of size 15, with four display decimals. For a value of 56.2185, the Universal Table Browser displays a formatted value (using the data dictionary editing) as 56.2185, even though this value is stored in the database as 562185.

Nonformatted: The Universal Table Browser displays the data according to the specification of the database and the data item type (such as numeric) from which the data came. For example, assume the table data item, PROC, is a numeric field stored in the database. Depending on the database, this field might have a default value size of 32 with a precision of 15 being a numeric data type. Because EnterpriseOne does not store the decimals in the database, a value 56.2185 would be stored and displayed in the database as 562185.0000000000000000.

Viewing Column Properties in a Table

In PeopleSoft Solution Explorer, access the Cross Application Development Tools (GH902) menu, and then choose Universal Table Browser.

To view column properties in a table

1. On Universal Table Browser, view a table as described in the previous task.
2. Right-click a desired column and choose Column Properties.

If you are viewing a formatted table, the data dictionary properties are displayed in the upper-right portion of the Column Properties form. If you are viewing an unformatted table, the data dictionary properties are not displayed.

CHAPTER 25

Working with Flat File Encoding

This chapter provides an overview of flat file encoding, an example of how to set up a flat file encoding record, and discusses how to:

- Add a flat file encoding record.
- Activate a flat file encoding file.

Understanding Flat File Encoding

Because PeopleSoft EnterpriseOne software uses Unicode and not all third-party software does, there is a preprocessing and postprocessing intercept of all flat files. During the intercept, the software converts the flat file into the Unicode character set or back into the original character set. You can assign the conversion character set applied to a flat file—based on the user or role, the program ID, the program version, and the environment—by adding and activating a flat file encoding record.

Using Unicode Flat File Encoding Configuration (P93081), you create records for a table that specifies what character sets are used for programs. The character sets are based on the user or role, the program ID, program version, and the environment. When the pre- or post-processing intercept occurs, the intercept program calls the table, searches it, and applies the record. The search is from more specific records to less specific records.

The primary users of Unicode Flat File Encoding Configuration are power users and system administrators. The business manager can provide the character set that is used to encode the third-party flat file.

Before setting up a flat file encoding record, you need to know the encoding of the flat file being transferred. You also need to know the user or role, program, program version, and environment that is calling the flat file.

To ensure that all files are encoded to the primary character set, set up a default flat file encoding record for the primary character set, and then add any exceptions. The system applies the more specific records before the more general records, so the default record is only used if no other records apply to the incoming flat file. If you do not add and activate a flat file encoding record, the default record is UCS2, UTF16_BE/UTF16_LS, which is a Unicode character set.

This table displays the character sets, from user defined code H95/FE, that are currently supported:

Code	Description	.ini Setting
BIG5	Chinese, Traditional	TC_BIG5
CP1250	WIN-Latin2, Central Europe	EE_CP1250
CP1251	WIN-Cyrillic	RS_CP1251
CP1252	WIN-Latin 1, Western European	WE_ISO88591

Code	Description	.ini Setting
CP1253	WIN-Greek	GR_CP1253
CP1254	WIN-Latin5, Turkish	TK_CP1254
CP1256	Win-Arabic	AR_CP1256
GB2312	Chinese, Simplified	SC_GB
IBM-1123	EBCDIC-Cyrillic	RS-EBCDIC
IBM-420	EBCDIC-Arabic	AR_EBCDIC
IBM-933	EBCDIC-Korean	KO_EBCDIC
IBM-935	EBCDIC-Simplified Chinese	SC_EBCDIC
IBM-937	EBCDIC-Traditional Chinese	TC_EBCDIC
IBM-939	EBCDIC-Japanese	JA_EBCDIC
IBM-37	EBCDIC-Latin 1 or Western Euro	US_EBCDIC
KSC-5601	Korean	KO_KSC
SHIFT_JIS	WIN-Japanese	JA_SJIS
UCS2	UTF16_BE/UTF16_LE	
UTF-16LE	UTF16_LE	
UTF-16BE	UTF16_BE	
UTF8	UTF8	
IBM-858	# PC Latin 1 with Euro	

Example: Setting Up Flat File Encoding Records

The example company primarily uses the flat file encoding character set CP1252, WIN-Latin 1, Western European. However, the Sales Order Entry program (P4210) uses the UTF8, Unicode character set, except when the user JL5534221 runs version JDE0001 in the PDEVCLA environment; then the program uses the CP1250, WIN-Latin2, Central Europe character set. The same program occasionally, but not currently, uses the character set CP1254, WIN-Latin5, Turkish for environment PDEVASD2.

The following table presents the information for the encoding records that the example company needs in the flat file encoding table:

User/Role	Application Name	Application Version Name	Environment	Encoding Name	Status
All	All	All	All	CP1252	Active
All	P4210	All	All	UTF8	Active
JL5534221	P4210	JDE0001	PDEVCLA	CP1250	Active
All	P4210	All	PDEVASD2	CP1254	Inactive

These steps provide instructions on how to set up flat file encoding records for the previous example:

1. From the System Administration Tools (GH9011) menu, select Unicode Flat File Encoding Configuration.
2. On Work With Flat File Encoding, click Add.
3. On Flat File Encoding Revisions, complete these fields, and then click OK:

- User / Role

**PUBLIC* includes all users and roles.

- Environment

**ALL* includes all environments.

- Program ID

**DEFAULT* includes all programs.

- Version

**DEFAULT* includes all program versions.

- Encoding Name

Enter the following value: *CP1252*.

4. Repeat step 3 to add the following records to the table:

User/Role	Environment	Program ID	Version	Encoding Name
*PUBLIC	*ALL	*DEFAULT	*DEFAULT	CP1252
*PUBLIC	*ALL	P4210	*DEFAULT	UTF8
JL5534221	PDEVCLA	P4210	JDE0001	CP1250
*PUBLIC	PDEVASD2	P4210	*DEFAULT	CP1254

5. Click Cancel to return to Work With Flat File Encoding.
6. Click Find to display all of the flat file encoding records.
7. Select the first record and from the Row menu, choose Change Status to activate the recode.
8. Repeat step 7 to activate the currently active records.

This table displays the final configuration:

User/Role	Environment	Program ID	Version	Encoding Name	Status
*PUBLIC	*ALL	*DEFAULT	*DEFAULT	CP1252	AV
*PUBLIC	*ALL	P4210	*DEFAULT	UTF8	AV
JL5534221	PDEVCLA	P4210	JDE0001	CP1250	AV
*PUBLIC	PDEVASD2	P4210	*DEFAULT	CP1254	NA

Forms Used to Work with Flat File Encoding

Form Name	Form ID	Navigation	Usage
Work With Flat File Encoding	W93081A	System Administration Tools (GH9011), Unicode Flat File Encoding Configuration	Access the form to add a flat file encoding record. Locate the defined flat file encoding files.
Flat File Encoding Revisions	W93081B	On Work With Flat File Encoding, click Add.	Enter the information for a flat file encoding record.

Adding a Flat File Encoding Record

To define the character set that is applied to a flat file during the pre- or post-processing intercept, add a flat file encoding record. You can apply a flat file encoding file based on the user, the user role, the program ID, the program version, and the environment.

After you add the flat file encoding record, you must activate it.

Access the Work With Flat File Encoding form.

To add a flat file encoding record:

1. On Work With Flat File Encoding, click Add.
2. On Flat File Encoding Revisions, complete these fields, and then click OK:

- User / Role

The default user/role is **PUBLIC*, which includes all users. By specifying a user or role, you can limit flat file encoding to only programs running under that user or role.

- Environment

The default environment is **ALL*, which applies the character set encoding to all environments. By specifying an environment, you can limit the flat file encoding to only programs running under that environment.

- Program ID

The program ID identifies the batch or interactive application to which to apply the flat file encoding. The default value, **DEFAULT*, applies flat file encoding to all programs.

- Version

A version is a set of user defined specifications that determines how a batch or interactive application runs. A program version identifies the batch or interactive application version to which to apply the flat file encoding. The default version, **DEFAULT*, applies the flat file encoding file to all versions.

- Encoding Name

The encoding name identifies the character set used by the incoming or outgoing flat file. You must specify an encoding name.

Activating a Flat File Encoding Record

After adding a flat file encoding record, you must activate it before it will be applied to incoming and outgoing flat files.

Access the Work With Flat File Encoding form.

To activate or deactivate a flat file encoding file:

1. On Work With Flat File Encoding, click Find to display the defined flat file encoding files.
2. Select the flat file encoding file to activate or deactivate.
3. From the Row menu, select Change Status.

The status of the flat file encoding becomes active (*AV*) or inactive (*NA*).

CHAPTER 26

Understanding Naming Conventions

This chapter provides an overview of naming conventions and discusses:

- Path codes
- Data sources
- Package names
- Server names
- Workstation names

Naming Conventions Overview

This section provides information about the naming conventions that PeopleSoft suggests that you use when you set up the configuration. You should use alphanumeric characters for the names. Depending on the server platform, some characters might not be allowed.

Path Codes

The naming conventions for a path code are as follows:

- Limited to 10 characters.
- Letters must be uppercase only.

Data Sources

The naming conventions for a data source are as follows:

- Limited to 30 characters.
- Case-sensitive.

Specific naming convention exceptions for the Client Access data source are as follows:

- Limited to 32 characters.
- Must begin with an alphabetic character.

- You cannot use the following characters:

- { }
- []
- ()
- ?
- *
- =
- !
- @
- ;

Note. You must type the data source name before you can use the Client Access ODBC driver to access iSeries data.

Data Source Description

Limited to 80 characters.

Package Names

The naming conventions for a package are as follows:

- Limited to 10 characters.
- Uppercase only.
- You cannot use the following characters:
 - /
 - \
 - :
 - *
 - ?
 -
 - <
 - >
 - |

Server Names

The naming conventions for a server depend on the specific platform. For example, an HP9000 and an iSeries allow you to enter different characters when you define the server name. EnterpriseOne limits the number of characters that you can use to name a server to 15, regardless of the platform.

Workstation Names

The naming conventions for a workstation are as follows:

- Limited to 15 characters.
- Each workstation requires a unique name.

When you add a workstation to a Windows Server domain, you must use the name created for the computer by the network administrator.

If the workstation name does not have a computer account in the domain, you cannot sign in to the domain or access any domain user accounts.

CHAPTER 27

Understanding the Jde.ini File Settings

This section provides a listing of the settings within the jde.ini file (on the iSeries, it is known as the INI file) and discusses:

- Jde.ini file location.
- Workstation jde.ini settings.
- iSeries server jde.ini settings.
- UNIX/Linux server jde.ini settings.
- Windows enterprise server jde.ini settings.
- Server jde.ini settings for WebSphere.
- Web server jas.ini settings.
- Web server jdbj.ini settings.

Jde.ini File Overview

The jde.ini file is an initialization file that provides runtime settings for EnterpriseOne. Specific versions of the file must reside on every workstation and enterprise server in the installation.

The jde.ini is divided into sections with informational headings. Each section heading is enclosed in square brackets, such as [JDENET]. Each section contains one or more keys. The key name is on the left side of the equal (=) sign; the value of the key is on the right side.

The workstation jde.ini file can be accessed three ways:

- Access Windows Explorer, locate the jde.ini file, and double-click it to open it.
Use Notepad to view the file.
- Click the Windows Start button, and select Run from the list of options.
Type *jde.ini* in the Open field.
- Type *jde.ini* in the Fast Path field of PeopleSoft Solution Explorer.

How to Use This Section

The sections, such as [CLUSTER], in this section are alphabetized. The settings within the sections are presented in the order in which they appear in the jde.ini file.

Locating the Jde.ini File

You can locate the jde.ini file in various places, depending on the platform.

Workstation Jde.ini Settings

This section discusses the settings found in the client-side workstation jde.ini file. Information is organized by section—for example, [DEBUG]. Sections are alphabetized, but settings found within sections are listed in the order in which they are found in the software.

The jde.ini file is located in the default Windows directory of the workstation. This directory might have a variety of names, depending on the type of operating system being used. If you are using Windows 2000, the default directory might be called Win2000.

[ACTIVE DIRECTORY]

The ACTIVE DIRECTORY settings are:

Setting	Value	Purpose
JdenetSCP	Variable	The value is the name of the Service Connection Point object in Active Directory. The SCP allows the workstation to connect to a server that has PeopleSoft EnterpriseOne running on it. Typically, the name is the name of the EnterpriseOne service running on the server, such as: PeopleSoft_ERP_810_SP1. JdenetSCP is the connection port parameter.
SecurityServerSCP	Variable	Same as previous. SecurityServerSCP is the security server parameter.
LockManagerSCP	Variable	Same as previous. LockManagerSCP is the Lock Managerkadol parameter
UnifiedLogonServerSCP	Variable	Same as previous. UnifiedLogOnServer SCP is the unified logon server parameter.

[DB SYSTEM SETTINGS]

The settings in this section contain information about the default environment and path code. A directory must reside on the workstation that has the same name as the default path code shown in its jde.ini file. The name of the server can also be found in this section:

Setting	Value	Purpose
Version=	43	A version number to prevent mismatch of the jde.ini file with the running version of EnterpriseOne.

Setting	Value	Purpose
Default User=	JDE	The user account name for the database bootstrap tables.
Default Env=	ADEVCLA	The default environment on the workstation or the enterprise server.
Default PathCode=	PROD	The name of a subdirectory under \810 that the software uses to find specifications to display sign-in information before an environment is selected.
Base Datasource=	System - 810	The data source representing the database from which logon information is retrieved.
Object Owner=	Object/owner	The owner of the system database tables.
Server=	Server name	The server on which the database resides
Database=		The name of the Oracle connect string or the ODBC datasource name for iSeries.
Load Library=		The PSFT driver that is used to access the database that stores the system tables. This value is set dynamically by EnterpriseOne runtime.
Decimal Shift=	N (default) Y	A flag to indicate if decimal shifting is used for numeric data.
Julian Dates=	N (default) Y	A flag to indicate if dates are stored in Julian or database-specific format.
Use Owner=	N (default) Y	A flag to indicate that table names are to be qualified by owner.
Secured=	N (default) Y	Indicates whether the database is a secured database that requires a user and password login.
Type=	A (default) O I L W M S	A single character denoting the type of database holding the system tables. These characters can be O (Oracle), A (MS Access), I (Client Access, iSeries), L (SQL Server OLEDB), W (DB2 UDB for Windows/Unix), S (SQL Server), M MSDE/OLEDB OR N (MSDE/ODBC).

Setting	Value	Purpose
DatabaseName2=		ODBC name for the SQL Server database or iSeries library database name
DatabaseInstance=		Name of the SQL Server database instance if using multiple instances. Leave this setting blank if using a single instance.
ServerPort=		The port number of the SQL Server database port
UnicodeFlag=	N (default) Y	Indicates whether Unicode is used on the datasource. Set this to Y if using Unicode.
LOBFlag=	Y	For Oracle and iSeries. Indicates that LOBs are used in the datasource instead of BLOBs. This value should always be Y.
Default Pwd=		The default password.
Default Journal=	OW_JRNL	iSeries only. The name of the default journal. Journaling is required on the iSeries for rollback recovery. The two components to journaling are: <ul style="list-style-type: none"> • The journal • The journal receiver Both before and after images of a database transaction can be recorded by journaling. Journaling can be set to any character string of 10 characters or fewer.
Default Journal LIBRARY=	Journal library	iSeries only. The library name where the journal is stored, which can be set to any valid library name. The library name changes for each release.
Default Journal Receiver	OW_JRNL000	iSeries only. The name of the journal receiver, which can be set to any character string of 10 characters or fewer.
Default Journal Receiver LIBRARY=	Journal library	iSeries only. The library name where the journal receiver is stored, which can be set to any valid library name. The library name changes for each release.
Size of Journal Receiver=		iSeries only.

Setting	Value	Purpose
ThousandsSeparator=	,	<p>Sets the default character for ThousandsSeparator; the default can be set to any character except a number. This value should match the ThousandsSeparator that is specified by the client operating system.</p> <p>Note. The INI file does not support the use of a space. If a space or non-blocking space must be specified, use the strings SPACE or NB_SPACE instead.</p>
DecimalSeparator=	.	<p>Sets the default character for DecimalSeparator; the default can be set to any character except a number. This value should match the DecimalSeparator that is specified by the client operating system.</p> <p>Note. The INI file does not support the use of a space. If a space or non-blocking space must be specified, use the strings SPACE or NB_SPACE instead.</p>

[DB SYSTEM SETTINGS - SECONDARY]

This section is used for workstations only. The settings are used for a secondary data source to start PeopleSoft EnterpriseOne if the primary data source is unavailable. These settings should be the same as the values in the F98611 table for the secondary data source:

Setting	Typical Value	Purpose
Base Datasource=	Access32	The data source representing the database from which logon information is retrieved.
Object Owner=		The database owner of the system tables.
Server=	Server name	The server on which the database that stores the system tables resides.
Database=	Access32	The name of the database that stores the system tables.
Load Library=	JDBODBC.DLL (default)	The JDE driver that is used to access the database holding the system tables.
Decimal Shift =	N (default) Y	A flag to indicate if decimal shifting is used for numeric data.
Julian Dates=	N (default) Y	A flag to indicate if dates are stored in Julian or database-specific formats.
Use Owner=	N (default) Y	A flag to indicate that table names are to be qualified by owner.

Setting	Typical Value	Purpose
Secured=	N (default) Y	A flag to indicate whether database is securing, requiring user and password login.
Type=	A (default) O S I	A single character denoting the type of database that stores the system tables. These characters can be: O (Oracle), A (MS Access), S (SQL Server), or I (Client Access, iSeries).
Library List=		iSeries only. Database server that stores the system tables.
Library=		iSeries only. Database library that stores the system tables.

[DEBUG]

The settings in this section determine the location of the jde.log and jdedebug.log. The settings are also used to turn the jdedebug.log on and off:

Setting	Typical Value	Purpose
TAMMultiUserOn=	0	
Output=	None	Controls the status of the jdedebug file. Valid values are: <ul style="list-style-type: none"> • NONE. No trace information is written to jdedebug.log. • FILE. Database and runtime trace information are written to the file that is specified by the DebugFile= parameter in the [DEBUG] section. • EXCFIL. Runtime trace information is written to the file that is specified by the DebugFile= parameter in the [DEBUG] section. • BOTH. Trace information is written to both jde.log and jdedebug.log.
ServerLog=	0 (default) 1	Valid values are: <ul style="list-style-type: none"> • 0. Disables the workstation requesting the business function JDE.LOG and JDEDEBUG.LOG entries from the server. • 1. Enables workstation requesting business function JDE.LOG and JDEDEBUG.LOG entries from the server.

Setting	Typical Value	Purpose
LEVEL=	BSFN,EVENTS	<p>Controls the debug level. You can specify any combination of allowable values using commas as delimiters. The default setting is LEVEL=BSFN,EVENTS. Valid values are:</p> <ul style="list-style-type: none"> EVENTS. Traces the starting and stopping of events. BSFN. Traces when business functions are entered and when they return. SF_x. Traces when system functions execute. The x variable is any allowable system function value. Valid values are: <ul style="list-style-type: none"> SF_GRID SF_PARENT_CHILD SF_GENERAL SF_MESSAGING SF_WORKFLOW SF_WORKFLOW_ADMIN SF_MEDIA_OBJ SF_CONTROL <p>For example, LEVEL=SF_CONTROL. In addition, you can specify multiple system functions by separating them with commas. For example, LEVEL=SF_GRID,SF_CONTROL.</p>
DebugFile=	c:\jdedebug.log	The location and name of the jdedebug.log file.
JobFile=	c:\jde.log	The location and name of the jde.log file.

[EVEREST]

The EVEREST setting is:

Setting	Typical Value	Purpose
ShowAlias=	0 (default for PROD packages) 1 (default for APPL packages)	This setting disables (0) or enables (1) the ability to right-click a data dictionary item and display its alias.

[INSTALL]

The settings in this section contain directory paths and general installation information:

Setting	Typical Value	Purpose
DefaultSystem=	System	The name of the subdirectory under \810 that contains the foundation code and tools.
ClientPath=	EnterpriseOne Client Install	The name of the directory on the deployment server that contains the Workstation Installation program and other files that are used during deployment.
PackagePath=	Package	The name of the subdirectory on the deployment server under a path code that contains the packages that were built for that path code.
DataPath=	Data	The name of the subdirectory on the deployment server under the path code that contains the Access database that is delivered for all packages for that path code.
HOSTS=	Hosts	The name of the directory on the deployment server that contains all of the types of host files. Used in the host configuration generate application.
HP9000=	hp9000	The name of the directory on the deployment server that contains HP9000 files. Used in the host configuration generate application.
RS6000=	rs6000	The name of the directory on the deployment server that contains RS/6000 files. Used in the host configuration generate application.
AS400=	as400	The name of the directory on the deployment server that contains iSeries files. Used in the host configuration generate application.
SUN=	Sun	The name of the directory on the deployment server that contains Sun files. Used in the host configuration generate application.
LocalCodeSet=	WE_ISO88591	A setting that is used to determine alternate language usage. See the appropriate EnterpriseOne PeopleTools 8.11 Upgrade document for other language values.
ActiveConsole	0 1	If this setting is 0, the package build does not add the entry to the package.inf file. If this setting is 1, an ActivEra Console shortcut is added to the package build .inf file. When the package is installed to a workstation, the shortcut is added to the desktop.
WebAdmin=	0 1	A setting of 1 gives the user administrative rights to the Java & HTML Generator so that the administrator can generate any Java serialized object publicly. A setting of 0 means that the user can only generate personal forms and menus using the Java & HTML Generator.

[JDE_CG]

The JDE_CG section settings are:

Setting	Typical Value	Purpose
STDLIBDIR=	\$(COMP)\VC98\lib	The path to the lib directory that is used by the MSVC compiler. This value is updated by a workstation installation that is based on the user's deployment preferences.
TPLNAME=	EXEFORM2	
ERRNAME=	CGERR	
TARGET=	Debug (default) Release	Used by the code generator and global build program to determine the type of build. Customer should only build under release, as conflicts with the release build of the tools occur if they build under debug.
INCLUDES=	\$(COMP)\VC98\include;\$ (SYSTEM)\include; \$(SYSTEM)\cg; \$(APP)\include; \$(SYSTEM)\includev	The path to the include (header files) directory that is used by the MSVC compiler. This value is updated by a workstation installation, based on the user's deployment preferences.
LIBS=	\$(COMP)\VC98\lib; \$ (SYSTEM)\lib32; \$(APP)\lib32; \$(SYSTEM)\libv32	The path to the library directory that is used by the MSVC compiler and PeopleSoft EnterpriseOne Foundation. This value is updated by a workstation installation, based on the user's deployment preferences.
MAKEDIR=	\$(COMP)\VC98\bin; \$(COMP) \Common\MSDev98\Bin	The path to the make directory that is used by the MSVC compiler. This value is updated by a workstation installation, based on the user's deployment preferences.
USER=	User name	The user ID of the person who performed the workstation installation.

[JDEMAIL]

The JDEMAIL settings are:

Setting	Typical Value	Purpose
ClientType=	Windows HTML	Defines whether the application shortcut that is attached to an external email message contains a Windows application shortcut or a URL for an HTML application shortcut. The default value is Windows.

Setting	Typical Value	Purpose
mailProfile=	Default Profile	The name of the profile to be used for external mail systems that are accessed through PeopleSoft EnterpriseOne Work Center. Examples of external mail servers include Microsoft Exchange Server and Lotus Domino Mail Server.
mailServer=	owsmtp.peoplesoft.com	The domain name of the SMTP server to be accessed for sending server mail messages.

[JDENET]

The JDENET section settings are:

Setting	Typical Value	Purpose
serviceNameListen=	6005	Specifies the communications service port on the TCP/IP network. The software uses this port address to listen for requests on the network.
serviceNameConnect=	6005	Specifies the communications service port on the TCP/IP network. The software uses this port address to connect to the network. OCM determines on which server a business function runs. If you run multiple instances of EnterpriseOne on the same server, each instance runs on a different port. The serviceNameConnect parameter value determines the EnterpriseOne instance that handles the business function request.
maxLenInlineData=	1024	For internal use only.
maxLenFixedData=	4096	For internal use only.
maxFixedDataPackets=	1024	For internal use only.
netTrace=	0	Turns netTrace on or off. The default setting of 0 means that netTrace is off. A setting of 1 - 4 enables JDENET debug to log messages. You can increase the level of detail by increasing this number, and you can use these log messages for debugging.
kernelDelay=	0	For internal use only.

[JDENET_KERNEL_DEFX]

The JDENET_KERNEL_DEFX settings are:

Setting	Typical Value	Purpose
bOneUserOnly=	0	<p>Parameter value of 1 allows the client workstation to get its own kernel process on the server. For the setting to work, a corresponding parameter, bAllowOneUserOnly, with a value of 1, must be added to the [JDE_KERNEL_DEFX] section of the server jde.ini file.</p> <p>Specify the kernel process that the user will have on the server by adding the number of the kernel definition section:</p> <p>[JDENET_KERNEL_DEF6]</p> <p>bOneUserOnly=1</p> <p>This setting allows a client workstation to have its own CallObject kernel process on the server.</p>

[LOCK MANAGER]

The LOCK MANAGER settings enable transaction processing.

Note. Enable transaction processing on the server before you enable it on the workstation. If you try to set up the workstation jde.ini file before you set up the server jde.ini, you could be requesting a service on the server that is not yet available, which generates an error.

The LOCK MANAGER settings are:

Setting	Typical Value	Purpose
Server=	Server name	This setting indicates the lock manager server to be used to process records. For example, a server name might be intelnta. The value for this setting is the name of the server that is acting as the lock manager.
RequestedService=	NONE	<p>This setting indicates the type of service that the client requests from the server. Valid values are:</p> <ul style="list-style-type: none"> • TS Time stamp service. • NONE No service is requested.

[MAILMERGE]

The MAILMERGE setting is:

Setting	Purpose
FileLocation=	The location on the workstation of the mailmerge file.

[NETWORK QUEUE SETTINGS]

The settings in this section contain the name of the queue that is used when running batch jobs on the server. The settings also show the workstation's UBE priority, and whether to hold the jobs in a spool file or immediately send them to a printer:

Setting	Typical Value	Purpose
UBEQueue=	QBATCH	The batch name that the client submits for the UBE or package installation to the server.
UBEPriority=	5	The priority that is set when the UBE is submitted. For workstations, valid values are 1 to 5, where 1 is the highest priority setting. The priority setting is relative to other UBE jobs that are submitted by the software.
PrintImmediate=	FALSE (default) TRUE	EnterpriseOne servers hold the UBE spool files submitted from a workstation unless the jde.ini file on the workstation has the PrintImmediate=TRUE setting (which is case-sensitive) in the [NETWORK QUEUE SETTINGS] section. On the iSeries, the spool file is created with the HOLD(*YES) attribute as a default. If the setting PrintImmediate=TRUE is set in the jde.ini file on the workstation, upon submission of the UBE to the EnterpriseOne server, the spool file is released once it is placed on the appropriate outqueue and closed.
SaveOutput=	TRUE (default) FALSE	A setting that lists whether the user wants to save the log files that are generated by the UBE.
InstallSpecs=	Y	A setting that lists whether the user wants to install specifications when submitting UBEs.
JDENETTimeout=	60	The timeout value, listed in seconds, for clients to attempt to connect to the server.

[OBJECT LIBRARIAN]

The OBJECT LIBRARIAN section settings are:

Setting	Value	Purpose
OLTLogMode=	YES (default) NO APPEND	<p>This setting specifies if and how the Object Management Workbench Transaction log (OLT.log) is generated. Valid values are:</p> <ul style="list-style-type: none"> • YES. The OLT.log is generated for each transaction. If the log exists before a transaction, its contents are overwritten. • NO. No OLT.log is generated during Object Management Workbench object transactions. • APPEND. The information for a transaction is appended to the OLT.log. <p>When the size of the log reaches the maximum size allowed (2 MB), the user is prompted to rename the existing file. If the user chooses not to rename it, the existing contents of the log are overwritten by the information that is generated by the new transaction.</p>
OLTLogContents=	GENERAL (default) DETAIL	<p>Specifies if detail information about specification records will be generated in the OLT.log. Valid values are:</p> <ul style="list-style-type: none"> • GENERAL. No detail information about specification records will be generated. • DETAIL. Detail information will be generated.

[OFFLINE DB SYSTEM SETTINGS]

The settings in this section are used only for running PeopleSoft EnterpriseOne in detached mode. If you have not installed the workstation with the detached mode option, this section does not appear in the workstation jde.ini file. The following settings are the same as in the section [DB SYSTEM SETTINGS] listed previously in this chapter, although the values are different:

Setting	Value	Purpose
Version=	43	A version number to prevent mismatch of the jde.ini file with the running version of EnterpriseOne.
Default User=	JDE	The user account name for the database bootstrap tables.
Default Env=	DEMO810	The default environment on the workstation or the enterprise server.

Setting	Value	Purpose
Default PathCode=	APPL_PGF	The name of a subdirectory under \810 that the software uses to find specifications to display sign-in information before an environment is selected.
Base Datasource=	System Local	Data source representing the database from which logon information is retrieved.
Object Owner=		The owner of the system database tables.
Server=		The server on which the database resides.
Database=	System Local	The name of the Oracle connect string or the ODBC datasource name for iSeries.
Load Library=		The PSFT driver that is used to access the database that stores the system tables. This value is set dynamically by EnterpriseOne runtime.
Decimal Shift=	N	A flag to indicate if decimal shifting is used for numeric data.
Julian Dates=	N	A flag to indicate if dates are stored in Julian or database-specific format.
Use Owner=	N	A flag to indicate that tables names are qualified by owner.
Secured=	N	Indicates whether this database is secured, requiring a user and password login.
Type=	A (default) O I L W M S	A single character denoting the type of database holding the system tables. These characters can be O (Oracle), A (MS Access), I (Client Access, iSeries), L (SQL Server OLEDB), W (DB2 UDB for Windows/Unix), S (SQL Server), M MSDE/OLEDB OR N (MSDE/ODBC).
DatabaseName2=		ODBC name for the SQL Server database or iSeries library database name.
DatabaseInstance=		Name of the SQL Server database instance if using multiple instances. Leave this setting blank if using a single instance.
ServerPort=		The port number of the SQL Server database port.

Setting	Value	Purpose
UnicodeFlag=	N (default) Y	Indicates whether Unicode is used on the datasource. Set this to Y if using Unicode.
LOBFlag=	Y	For Oracle and iSeries. Indicates that LOBs are used in the datasource instead of BLOBs. This value should always be Y.
LibraryList=		iSeries only. Database server that stores the system tables.
Default Pwd=		The default password.

[SECURITY]

The SECURITY settings are:

Setting	Typical Value	Purpose
SecurityServer=	Server name	
RowSecurity=	DEFAULT	
DataSource=	ORACLE PVC	
DefaultEnvironment=	Environment name	This setting defines a valid environment in which the path code defines F98OWSEC.
UnifiedLogon=	0 (default) 1	This setting specifies whether the unified logon feature is on or off. When off, EnterpriseOne uses the standard logon functionality. Enter 0 (or leave blank) to set unified logon to off, or 1 to set it to on.
UnifiedLogonServer=	server name	This setting specifies where the unified logon server resides. If no server is present, the default is the EnterpriseOne security server.
ShowUnifiedLogon=	0 1 (default)	This setting determines whether the EnterpriseOne environment selection form appears when the unified logon feature is used. Valid values are: <ul style="list-style-type: none"> • 0: The environment selection form is not displayed. • 1: The environment selection form is displayed.

[SVR]

The settings in this section contain environment and subdirectory information:

Setting	Typical Value	Purpose
EnvType=	1	Used by JDEKRNL.
EnvironmentName=		
SpecPath=	spec	This line and all of the following lines in this section specify the path names that enable other EnterpriseOne source programs to locate files. For instance, if spec is changed to specifications, changing SpecPath would allow this change immediately. This value is not updated by any program or process. The only reason to change this value is aesthetic. This line is the subdirectory under the path code that is used to store the set of specification files on the workstation.
SourcePath=	source	On the client workstation, the subdirectory under the path code that is used to store the business function source files.
ObjectPath=	obj	On the client workstation, the subdirectory under the path code that is used to store the business function object files.
HeaderPath=	include	On the client workstation, the subdirectory under the path code and system directory that is used to store the business function and system header files.
HeaderVPath=	includev	On the client workstation, the subdirectory under the system directory that is used to store the foundation code header files.
BinPath=	bin32	On the client workstation, the subdirectory under the path code and system directory that is used to store the set of business functions, and application and foundation code dlls.
LibPath=	lib32	On the client workstation, the subdirectory under the path code and system directory that is used to store the business function and system lib files.
LibVPath=	libv32	On the client workstation, the subdirectory under the path code and system directory that is used to store the third-party libraries.
MakePath=	make	On the client workstation, the subdirectory under the path code that is used to store the set of business function make files. This value is not updated by any program or process. We recommend that you do not change the name of this directory.

Setting	Typical Value	Purpose
WorkPath=	work	On the client workstation, the subdirectory under the path code that is used to store the set of application temp files that are created during a build. This value is not updated by any program or process. We recommend that you not change the name of this directory.
CodeGeneratorPath=	cg	On the client workstation, the subdirectory under the system directory that is used to store the templates for interactive application form types. These templates are used at runtime and are created during a build of applications.
ResourcePath=	res	On the client workstation, the subdirectory under the path code that is used to store the set of bitmaps.
IconPath=	res\icons	On the client workstation, the subdirectory under the path code that is used to store the set of icons.
FontPath=	res\font	On the client workstation, the subdirectory under the path code that is used to store the set of fonts.
HelpPath=	helps	The path to the location that stores the client-accessible set of help files, if any. This path can point to a server and is specified in User Profiles.
TreeBmpPath=	res\treebmps	On the client workstation, the subdirectory under the path code that is used to store the tree bit map files.
ModelPath=	models	On the client workstation, the subdirectory under the path code that is used to store the models files.
LocalePath=	locale	The base directory for the National Language Support (NLS) conversion tables.
Iconvpath=	locale\Iconv	The directory for the NLS conversion map.

[UBE]

The settings in this section determine whether the jdedebug.log is on or off. This setting also determines the level of debugging:

Setting	Typical Value	Purpose
UBEException	0 1 (default)	Disable (0) or enable (1) exception handling. 0 allows the system to exit gracefully on an error. 1 brings up a debug log.
UBEChkMem	0 1 (default)	Disable (0) or enable (1) calls to jdeCheckMemory, which allows memory traces on business functions.

Setting	Typical Value	Purpose
UBESubsystemLimit	3	Used to specify the number of subsystem jobs per report version.
UBESaveLogFile	0 (default) 1	Delete (0) or save (1) UBE log file (delete only works when DebugLevel=0).
UBEDBOutputLocation		Used to define the location for database output or mapping.
UBETabOpt=	1 0	Not delivered in the default jde.ini file. The system automatically performs row data selection optimization. However, use this setting if you want to disable row data selection optimization. The values are enabled (1) or disabled (0). If you want to re-enable optimization, you can change the value back to 1 or simply delete the UBETabOpt setting.
UBEDebugLevel=	0 (default) 1- 6	Used to specify what level of debugging information will be provided when using UBE debug logging. The highest level of logging information is 6. Valid values are: <ul style="list-style-type: none"> • 0: Error messages only • 1: Informative messages • 2: Section-level messages • 3: Object-level messages • 4: Event rules messages • 5: SQL statements • 6: UBE function messages
UBEShowPDFLink	0 (default) 1	Type 1 to show a box around PDF links.
UBEPrintDataItems	0 (default) 1	Used to specify whether to print the associated data item description in the .pdf file as metadata for third-party vendors. Valid values are: <ul style="list-style-type: none"> • 0: No, do not print. • 1: Yes, do print.
UBESSDebug	0 (default) 1	Disable (0) or enable (1) printing the subsystem key.
UBEVCDebug	0 (default) 1	Auto-attach VC when starting UBE in process (NT only).

Setting	Typical Value	Purpose
UBETHread	0 1 (default)	Run UBE as a process (0) or a thread (1).
WebServer	0 (default) 1	This setting specifies whether the system enables the UBE feature from the web server and identifies the EnterpriseOne kernel as a web kernel to meet the special needs of the web. If you leave this value blank, the calls from the business functions or the error message handling from the kernel do not work properly. Valid values are: <ul style="list-style-type: none"> • 0: Disabled • 1: Enabled

[WORKFLOW]

The WORKFLOW settings are:

Setting	Value	Purpose
Asynchronous Workflow=	FALSE	Used to activate or deactivate asynchronous workflow. The default value is FALSE.

iSeries Server Jde.ini Settings

This section describes the settings found in the PeopleSoft EnterpriseOne iSeries server INI. Information is organized by section—for example, [DEBUG]. Sections are alphabetized, but settings within sections are listed in the order in which they are found in the software.

[AS400]

The AS400 settings are:

Setting	Value	Purpose
CRTMOD=	CRTMOD MODULE(%s /%s) SRCFILE(%s/%s) SRCMBR(%s) OUTPUT(*PRINT) DBGVIEW(*NONE) OPTIMIZE(40)	The string used by the package install to compile business functions. Note that CRTMOD and CRTMOD2 are concatenated and used by the software to compile business functions.
CRTMOD2=	DEFINE(JDENV_ AS400MUTEX PRODUCTION_ VERSION NO _SIGNALS) TGTRLS(V4R3M0)	The concatenated string that is used by the package install for declaring additional definitions for compiling business functions.

Setting	Value	Purpose
CRTSRVPGM=	CRTSRVPGM SRVPGM(%s/%s) MODULE(%s/*ALL) BNDSRVPGM(JDELIB JDEKRNL OWVER) EXPORT(*ALL) OPTION(*DUPPROC *DUPVAR *UNRSLVREF) ALWLIBUPD(*YES) TGTRLS(V4R3M0)	The string that is used by the package install for binding business function modules to create the PeopleSoft EnterpriseOne service programs (*SRVPGM).
CRTDBPGM1=	CRTPGM PGM(%s/%s) MODULE(DBDRVAG DBDRV_AC DBDRV_CC DBDRV_CN	The concatenation of CRTDBPGM* settings is used to create the database programs JDB_*. These database programs are automatically created by EnterpriseOne at startup. The SENTINEL job creates them at startup time, and then monitors and creates additional programs as needed during runtime. The status of the programs and their usage are maintained in the user space JDEPGMCTL in the CONTROL library.
CRTDBPGM2=	DBDRV_CH DBDRV_CP DBDRV_RQ DBDRVSQ DBMONCTL DBDRVDLI	See purpose for CRTDBPGM1.
CRTDBPGM3=	DBSQL DBSQL_A DBSQL_D DBSQL_I DBSQL_M DBSQL_S DBSQL_U DBSQL_X	See purpose for CRTDBPGM1.
CRTDBPGM4=	BNDSRVPGM(JDEKRNL JDELIB JDEIPC) ACTGRP(%s) OPTION(*DUPPROC	See purpose for CRTDBPGM1.
CRTDBPGM5=	*DUPVAR) ALWLIBUPD (*YES) AUT(*ALL) TGTRLS(V4R3M0)	See purpose for CRTDBPGM1.
PrintUBEJoblog=	FALSE (default) TRUE	If true, indicates that the software always writes the iSeries JOBLOG for the batch application (UBE) to a spool file.
PrintUBEJoblogOn Error=	FALSE (default) TRUE	If true, indicates that the software writes the iSeries JOBLOG for the batch application (UBE) to a spool file if an error occurs—for example, if a UBE fails.

[BSFN BUILD]

The BSFN BUILD settings are:

Setting	Value	Purpose
Build Area=	/psft810/packages	The location on the server where the package will be built.
Optimization Flags=	(40)	Machine dependent. These compile flags are used when building business functions in Release mode. You should not change these flags.
DebugFlags=	*ALL	Machine dependent. These compile flags are used when building business functions in Debug mode. You should not change these flags.
InliningFlags=	Y (default, yes) N (no)	Valid values are: <ul style="list-style-type: none"> • Yes: Turns on inlining on the iSeries. • No: Turns inlining off. This entry is blank for non-iSeries servers.
DefineFlags=	JDENV_ASS\$))MUTEX PRODUCTION_VERSION JDBDB2400 AS400V3R6	
CompilerFlags=	*EXPMAC *NOSHOWINC	This setting determines whether to compile listings when building a server package. Valid values are: <ul style="list-style-type: none"> • *PRINT: Listings are compiled. • *NONE: Listings are not compiled.
CompileOutput=	*PRINT blank	Machine dependent. Valid compiler flags. The spill flag sets the stack space when business functions are compiled. The default value of 1024 is adequate to compile the delivered business functions. While values other than 1024 might be valid on various host platforms, this value is the only one validated by EnterpriseOne.
OSReleaseLevel=	V4R3M0	The release level to which you are compiling. You should not change this setting.
LinkFlags=	*DUPROC *DUPVAR * UNRSLVREF	Machine dependent. These flags are used when linking business functions. You should not change these flags.
LinkLibraries=	JDELIB JDEKRNL JDENET JDEIPC OWVER	Libraries to which business functions are linked (Windows and iSeries servers only).

Setting	Value	Purpose
SimultaneousBuilds=	0 (default) any integer	Indicates the number of DLLs that can be built at a time. 0 (zero) means that all DLLs are built simultaneously.
QName=	as400 batch jobq name	The job queue name to which all package builds will be submitted. If left blank, QName uses the default JOBQ as specified in the user profile that is doing the submitting.

[DB SYSTEM SETTINGS]

The settings in this section contain information about the default environment and path code:

Setting	Value	Purpose
Version=	43	A version number to prevent mismatch of the jde.ini file with the running version of EnterpriseOne.
Default User=	PSFT	The user account name for the database bootstrap tables.
Default Pwd=	PSFT	The user account password for the database bootstrap tables.
Default Env=	810APP	The default data source on the workstation or the enterprise server.
Default PathCode=	810APP	The subdirectory under \SPKG under which the business function code is stored.
Base Datasource=	DB2	The data source representing the database from which logon information is retrieved.
Object Owner=		The owner of the system database tables.
Server=	server name	The server on which the database resides.
Database=	database name	The name of the database where the system tables reside.
Load Library=	DBDR (default)	The PSFT driver that is used to access the database that stores the system tables. This driver depends on the database to be used and the type of system running EnterpriseOne.
Decimal Shift=	Y (default) N	A flag to indicate if decimal shifting is used for numeric data.
Julian Dates=	Y (default) N	A flag to indicate if dates are stored in Julian or database-specific format.

Setting	Value	Purpose
Use Owner=	Y N (default)	A flag to indicate that tables names are to be qualified by owner.
Secured=	Y (default) N	Indicates whether this is a secured database requiring a user and password login.
Type=	I	A single character denoting the type of database holding the system tables. These characters can be O (Oracle), A (MS Access), I (Client Access, iSeries), L (SQL Server OLEDB), W (DB2 UDB for Windows/Unix), S (SQL Server), M MSDE/OLEDB OR N (MSDE/ODBC).
Library=	database library	iSeries only. The database library that stores the system tables.
DatabaseName2=		ODBC name for the SQL Server database or iSeries library database name.
DatabaseInstance=		Name of the SQL Server database instance if using multiple instances. Leave this setting blank if using a single instance.
ServerPort=		The port number of the SQL Server database port.
UnicodeFlag=	N (default) Y	Indicates whether Unicode is used on the datasource. Set this to Y if using Unicode.
LOBFlag=	Y	For Oracle and iSeries. Indicates that LOBs are used in the datasource instead of BLOBs. This value should always be Y.
DatabaseProgramMax=	-1 (default)	iSeries only. The maximum number of database connection programs to allow. The value -1 means no limit.
DatabaseProgramInitial=	10 (default)	iSeries only. The number of database connection programs to start initially when EnterpriseOne is started.
DatabaseProgramThreshold=	3 (default)	iSeries only. The threshold for starting new database connection programs. If the number of database connection programs not in use drops below this limit, start new ones.
DatabaseProgramAdditional=	10 (default)	iSeries only. The number of new database connection programs to start when the threshold number is reached.

Setting	Value	Purpose
DatabaseProgramCheckIntervalSeconds=(default)		iSeries only. The length, in seconds, before the software idles after the database connection programs are created.
Default Journal=	OW_JRNL	<p>iSeries only. The name of the default journal. Journaling is required on the iSeries for rollback recovery. The two components to journaling are:</p> <ul style="list-style-type: none"> • The journal • The journal receiver <p>Both before and after images of a database transaction can be recorded by journaling. This value can be set to any character string that is 10 characters or fewer.</p>
Default Journal LIBRARY=	journal library	iSeries only. The library name where the journal is stored. This name can be set to any valid library name. The library name changes for each release.
Default Journal Receiver	OW_JRNL000	iSeries only. The name of the journal receiver. This can be set to any character string that is 10 characters or fewer.
Default Journal Receiver LIBRARY=	journal library	iSeries only. The library name where the journal receiver is stored. This can be set to any valid library name. The library name changes for each release.
Size of Journal Receiver=	6000	<p>iSeries only. This setting specifies a storage space threshold value (in KB) for the journal receiver. If the threshold value is exceeded during journaling, one of the following occurs:</p> <ul style="list-style-type: none"> • The message CPF7099 is sent to the journal message queue if the journal has the MBGRCV(*USER) attribute. • The system attempts to create and attach a new receiver if the journal has the MBGRCV(*SYSTEM) attribute. <p>When the old receiver is detached, the message CPF7020 is sent to the journal message queue. If the attempt fails due to lock conflicts, the system sends the message CPI70E5 and then tries again every ten minutes until the change journal operation is successful.</p> <p>When the system cannot determine if the journal has the MBGRCV(*SYSTEM) attribute, or if the attempt to create and attach a new journal receiver fails because of something other than a lock conflict, the message CPI70E3 is sent.</p>

[DEBUG]

The settings in this section determine the location of the jde.log and jdedebug.log. The settings are also used to turn the jdedebug.log on and off.

Setting	Typical Value	Purpose
Output=	FILE	Controls the status of the jdedebug log file. Valid values are: <ul style="list-style-type: none"> NONE: No trace information is written to jdedebug.log. FILE: Database and runtime trace information is written to the file that is specified by the DebugFile= parameter in the [DEBUG] section.
Trace=	TRUE	Writes additional trace information to the log files to aid in debugging.
DebugFile=	psft810/jdedebug	Location of the jdedebug log. The default value is jdedebug. No processes update this value. The names of the resulting files are path/jdedebug_#####.log, where ##### represents the iSeries job number that is associated with the job that created the file. <p>Note. The software does not create the path to these files. The path must exist prior to the logging process. The path resides in the Integrated File System (IFS) on the iSeries. You can use the iSeries WRKLNK command to see a list of directories and files and navigate between the IFS directories. EnterpriseOne contains a command called DSPSTMF that enables you to view these log files. In addition, you can set up Client Access to more easily view some of the smaller log files.</p> <p>See Using iSeries Integrated File System Logging Support in the EnterpriseOne Tools 8.94 PeopleBook: Server & Workstation Administration documentation for details about how to set up client access to view log files.</p>
JobFile=	psft810/jde.log	Location of the jde log. PeopleSoft ships the software with this value set to the jde.log. No processes update this value. Examine the log files jde.log, and jdedebug for information that can be used to assist in problem analysis and resolution. The names of the resulting files is path/jde_#####.log where ##### is the iSeries job number that is associated with the job that created the file. <p>See Using iSeries Integrated File System Logging Support in the EnterpriseOne Tools 8.94 PeopleBook: Server & Workstation Administration documentation for details about how to set up client access to view log files.</p>

Setting	Typical Value	Purpose
JDETSFile=	/psft810/JDETS.LOG	Specifies the location of the lock manager trace file on the iSeries.
ClientLog=	1 (default) 0	Valid values are: <ul style="list-style-type: none"> • 1: enables servicing CALLOBJ server trace to workstation. • 0: disables servicing CALLOBJ server trace to workstation.
LogErrors=	1 (default) 0	The action for error messages. Valid values are: <ul style="list-style-type: none"> • 0 or FALSE: Indicates that no error messages will be written to JDE.LOG. • 1 or TRUE: Indicates that error messages will be written to JDE.LOG.
KeepLogs=	1	Valid values are: <ul style="list-style-type: none"> • 1: Indicates that the logs will be saved after printing. • 0: Indicates that the logs will not be saved.
RunBatchDelay=	0	Specifies the time that runbatch waits upon startup, in seconds. This setting enables developers to start debugging the job or process.
TAMTraceLevel=	0 (default)	Specifies the level of TAM tracing, where 0 is off and 9 provides the greatest amount of tracing detail.

[ENTERPRISE TIMEZONE ADJUSTMENT]

The setting in this section contains information for properly adjusting the Enterprise Portal time for single signon.

Setting	Purpose
EntNode=	Enables you to enter the difference, in minutes, between Greenwich Mean Time (GMT) and Enterprise Portal Node time when setting up single signon between Enterprise Portal and PeopleSoft EnterpriseOne. You should change this setting whenever daylight savings time changes to reflect the difference between GMT time and the Enterprise Portal Node time.

[INSTALL]

The settings in this section contain directory paths and general installation information:

Setting	Typical Value	Purpose
DefaultSystem=	E810SYS	The name of the system library.
ClientPath=	810APP	The name of a valid path code on the deployment server that contains the workstation installation program and other files that are used during deployment.
810=		Should be left blank on the iSeries.
LocalCodeSet=	US_EBCDIC	A setting that is used to determine alternate language usage. See the appropriate EnterpriseOne PeopleTools 8.11 Upgrade document for other language values.
WebAdmin=	1	This setting specifies whether the system generates all of the Java objects for the default user. This setting includes overriding Java objects that were previously generated. If you leave this value blank, the system generates all the Java objects for the current user.
EnvCreation=	1 (default) to 5	This setting determines the number of environments that can be processed (loaded) at the same time.

[INTEROPERABILITY]

The INTEROPERABILITY settings are:

Setting	Typical Value	Purpose
RegisteredEvents=	RTSOOUT	Names of EventTypes. An event is an EnterpriseOne business transaction running on an enterprise server. To enable real-time generation of events, you must register each event that you want to generate in realtime.
FilteredEvents=	*ALL	The value of this parameter defines the events that you want to create in realtime. A value of *ALL generates all registered events. *NONE disables event generation. You can also enter a subset of registered events.

[JDEIPC]

The JDEIPC settings are:

Setting	Typical Value	Purpose
maxNumberOfResources=	1000	The total number of IPC resources that are available.

Setting	Typical Value	Purpose
startIPCKeyValue	2101	On NT, this value is used to uniquely name the IPC Shared memory. On all other systems, this value is the value of the IPC ID, which JDEIPC used for its shared memory. This value, plus the maxNumberOfResources, defines the range of IPC IDs that PeopleSoft EnterpriseOne will use on the system. System administrators should ensure that this range of IDs is not used by any other software. Although JDEIPC will not use an existing ID in its range, this situation might not be true of other software.
avgResourceNameLength	15	PeopleSoft Internal. Increase this value if you get an IPC error String table full.
maxMsgqEntries=	1024	
mazMsgqBytes=	65536	
ipcTrace=	0	Controls the level of interprocess communications (IPC) messages written to the jdedebug.log. Valid values are: <ul style="list-style-type: none"> • 0 (default): Writes no messages to the debug log. • 1: Writes only general trace messages. • 2: Writes IPC handle state trace messages. • 3: Writes both general and IPC handle state trace messages.

[JDEITDRV]

The JDEITDRV settings are:

Setting	Typical Value	Purpose
DrvCount=	3	The number of event drivers that is used for processing messages from event generators, either Z file or real-time.
Drv1=	Z:ZDRV	The directory location of the Z file event driver.
Drv2=	RT:RTDRV	The directory location of the real-time event driver.
Drv3=	JDENET:JDETRDRV	The directory location of the JDENET driver.

[JDEMAIL]

The JDEMAIL settings are:

Setting	Typical Value	Purpose
mailServer=	owsmtp.peoplesoft.com	The domain name of the SMTP server that is accessed for sending server mail messages.

[JDENET]

The JDENET settings are:

Setting	Typical Value	Purpose
serviceNameListen=	jde_server	Specifies the communications service port on the TCP/IP network. EnterpriseOne uses this port address to listen for requests on the network.
serviceNameConnect=	jde_server	Specifies the communications service port on the TCP/IP network. EnterpriseOne uses this port address to connect to the network.

Setting	Typical Value	Purpose
maxNetProcesses=	<p>Depends on the maximum number of concurrent EnterpriseOne users that the system is expected to handle, as well as the processing and memory power of the server.</p> <p>If you only need one process, then maxNetProcesses=1. However, if you need two or more processes, note that the first process is used exclusively to handle new connections and distribute them evenly among the other processes. In this case, you must add an extra process to act as a broker. To determine the number of processes that you need, you must first determine the maximum number of connections that you need and the number of connections a single process can handle. The formula for the number of connections allowed for each process is:</p> $\frac{(\text{maxNetConnections} / (\text{maxNetProcesses} - 1)) + 2}{2}$ <p>Each process requires two extra connections for listening (one for TCP and another for UDP), and an extra process is dedicated to handling incoming connections.</p>	Defines the maximum number of JDENET_N processes that can be running. You can increase the value for a server that is expecting heavy JDENET message flow.
maxNetConnections=	Depends on the maximum number of concurrent EnterpriseOne users that the system is expected to handle, as well as the processing and memory power of the server.	The total number of connections that all JDENET_N processes can handle. This value is platform-specific. You can increase the value for a server that is expecting to handle larger number of workstations at the same time.
netShutdownInterval=	15	

Setting	Typical Value	Purpose
maxKernelProcesses=	<p>Depends on several factors:</p> <p>Total of the individual kernel type maximums. The value should be at least that large, but it can be increased as needed.</p> <p>The number of one-user-only kernels you want to allow. Any number above the individual kernel maximum total will be allocated to one-user-only kernels.</p> <p>The room that you want to allow for dynamic increase of kernel processes from the Server Administration Workbench.</p>	The maximum number of JDENET_K processes that can be running. The value should be greater than all of the values added together in maxNumberOfProcesses for all the dedicated servers.
maxKernelRanges=	20	The number of dedicated servers and types.
kernelDelay=	0	For internal use only.
maxLenInlineData=	1024	For internal use only.
maxLenFixedData=	4096	For internal use only.
maxFixedDataPackets=	1024	For internal use only.
netTrace=	0	For internal use only.
krnlCoreDump=	0	For internal use only.
newProcessThreshold Connects=	0	
MaxIPCQueueMsgs	12	For internal use only.
InternalQueueTimeout	30	For internal use only.

[JDENET_KERNEL_DEFx]

This section defines internal dedicated server processes for JDENET. The sections are numbered JDENET_KERNEL_DEF1 to JDENET_KERNEL_DEF20. The settings in these sections should not be changed except where noted:

Setting	Value	Purpose
bAllowOneUserOnly=	1	<p>Parameter value of 1 (default) means that one-user-only kernel processes are allowed on client workstations. Add the setting only for CallObject kernel processes:</p> <p>[JDENET_KERNEL_DEF6]</p> <p>bAllowOneUserOnly=1</p> <p>Setting must be added with adding a [JDENET_KERNEL_DEFx]</p> <p>bOneUserOnly=1 section to the client workstation jde.ini file.</p>

Setting	Value	Purpose
krnlName	DEF1: JDENET RESERVED KERNEL	DEF1: Used for internal purposes and testing.
	DEF2: UBE KERNEL	DEF2: Processes EnterpriseOne batch process requests.
	DEF3: REPLICATION KERNEL	DEF3: Processes data replication requests.
	DEF4: SECURITY KERNEL	DEF4: Processes security server requests.
	DEF5: LOCK MANAGER KERNEL	DEF5: Processes transaction manager and lock manager requests.
	DEF6: CALL OBJECT KERNEL	DEF6: Processes requests for remote master business functions (MBF).
	DEF7: JDBNET KERNEL	DEF7: Processes JDBNet server-to-server requests.
	DEF8: PACKAGE INSTALL KERNEL	DEF8: Processes package installation request.
	DEF9: SAW KERNEL	DEF9: Processes SAW application requests.
	DEF10: SCHEDULER KERNEL	DEF10: Processes Scheduler application requests.
	DEF11: PACKAGE BUILD KERNEL	DEF11: Processes package build requests.
	DEF12: UBE SUBSYSTEM KERNEL	DEF12: Processes UBE subsystem requests.
	DEF 13: WORKFLOW KERNEL	DEF13: Processes workflow requests.
	DEF 16: XML LIST KERNEL	DEF16: Processes and returns request for data in XML document format.
	DEF 19: EVENT NOTIFICATION KERNEL	DEF19: Processes real-time events and XML documents generated by the Interoperability Event Observer, as well as Z file events. Publishes all EnterpriseOne events to subscribers.
	DEF 20: INTEROPERABILITY EVENT OBSERVER KERNEL	DEF20: Processes information from business functions calling real-time APIs and uses that information to create an XML or a Z file that is publishable to subscribers by the Event Notification Kernel.
	DEF 22: XML DISPATCH KERNEL	DEF22: Kernel for routing XML messages to their proper kernel.
	DEF 23: XTX KERNEL	DEF23: Kernel for transforming XML messages from one type to another.
	DEF 24: XML SERVICE KERNEL	DEF24: Processes inbound XAPI messages

Setting	Value	Purpose
dispatchDLLName=	DEF1: JDENET DEF2: JDEKRNL DEF3: JDEKRNL DEF4: JDEKRNL DEF5: JDEKRNL DEF6: JDEKRNL DEF7: JDEKRNL DEF8: JDEKRNL DEF9: JDESAW DEF10: JDEKRNL DEF11: JDEKRNL DEF12: JDEKERNL DEF13: JDEKRNL DEF16: XMMLIST DEF19: JDEIE DEF20: JDEIEO DEF22: XMLDISPATCH DEF23: XJSKERNEL DEF24: XMLSERVICE	Identifies the name of the JDENET service program.

Setting	Value	Purpose
dispatchDLLFunction=	DEF1: JDENET_Dispatch Message DEF2: JDEK_ DispatchUBEMessage DEF3: DispatchRepMessage DEF4: JDEK_ DispatchSecurity DEF5: TM_ DispatchTransactionManager DEF6: JDEK_ DispatchCallObject Message DEF7: JDEK_ DispatchJDBNETMessage DEF8: JDEK_ DispatchPkgInstallMessage DEF9: JDEK_ DispatchSAWMessage DEF10: JDEK_ DispatchScheduler DEF11: JDEK_ DispatchPkgBuildMessage DEF12: JDEK_ DispatchUBESBSMessage DEF13: JDEK_WFServerProcess DEF16: JDEK_XMLListDispatch DEF19: JDEK_DispatchITMessage DEF20: JDEK_DispatchIEOMessage DEF22: XMLDispatch DEF23: JDEK_ DISPATCHXTSMessage DEF24: XMLServiceDispatch	The name of the JDENET function for handling JDENET messages. The dispatchDLLName and dispatchDLLFunction entries are platform-specific.

Setting	Value	Purpose
maxNumberOfProcesses=	Depends on the number of concurrent users and kernel types. For example, CallObject kernels should be configured to start five to ten concurrent users per kernel.	The maximum number of kernel processes that can be run on this server for each kernel type. The user can modify this setting to tune performance. The default value is 1 for all JDENET_KERNEL_DEF sections.
numberOfAutoStartProcesses=	Variable	<p>The number of kernel processes that will automatically start for each kernel type. If this number is 0, then no processes start automatically for that kernel type. This number must be less than the maximum number of processes for that kernel type. The user can modify this setting to tune performance. The default value is 0 for all JDENET_KERNEL_DEF sections.</p> <p>The decision on assigning a value to this parameter should be based on when the user wants the overhead of starting a kernel process to occur: either when EnterpriseOne services start or when the first message for kernel type is received.</p>

[LOCK MANAGER]

The LOCK MANAGER section enables transaction processing and includes the following settings:

Setting	Typical Value	Purpose
Server	server name	This setting specifies the name of the lock manager server to be used to process records—for example, a server name might be <code>intelna</code> .
AvailableService=	NONE	<p>This setting indicates the service that the lock manager server is offering. It is also used to indicate whether the lock manager server is on or off. Valid values are:</p> <ul style="list-style-type: none"> • TS Time stamp service. • NONE No service is available. <p>Note. This setting only applies to servers.</p>
RequestedService=	NONE	<p>This setting indicates the type of service that the workstation requests from the server. The service that is currently being provided by servers is time stamping (TS) only. Valid values are:</p> <ul style="list-style-type: none"> • TS • NONE

[LREngine]

The LREngine settings are:

Setting	Typical Value	Purpose
System=	/E810SYS_X (you must use the integrated file system (IFS)).	The directory location of the List-Retrieval Engine, a database that is used to manage access to XML repository files.

[NETWORK QUEUE SETTINGS]

The settings in this section contain the name of the queue that is used when running batch jobs on the server. The settings also show the workstation's UBE priority, and whether to hold the jobs in a spool file or immediately send them to a printer:

Setting	Typical Value	Purpose
DefaultPrinterOUTQ=	QGPL/ONEWORLD_A	The default printer to which batch applications are routed.
UBEQueue	QBATCH	The batch name that the client submits for the UBE or package installation to the server.
JDENETTimeout=	60	The timeout value, listed in seconds, for clients to attempt to connect to the server. A server can act as a client when it uses JDBNET, submits UBEs to another server, calls a business function on another server, uses a Lock Manager on another server, or when it makes security server requests to another server.

[SAMPLE_EVENT]

The SAMPLE_EVENT settings are:

Setting	Typical Value	Purpose
DS1=	D4202150B	Defines the data structure for each real-time event registered in the [INTEROPERABILITY] section. Replace [SAMPLE_EVENT] with an event name, such as RTSOOUT, and then enter the values that define the data structure of the event.
DS2=	D4202150C	
DS3=	D34A1050C	

[SECURITY]

The SECURITY settings are:

Setting	Typical Value	Purpose
DataSource=		

Setting	Typical Value	Purpose
User=	JDESVR	This value must be a valid EnterpriseOne user ID and database user ID. Accordingly, this means that the user ID and password pair in the [SECURITY] section must be a valid EnterpriseOne user ID and password and database user ID and password.
Password=	JDESVR	This value must be the correct password for the EnterpriseOne user ID specified in the User setting of the [SECURITY] section. Accordingly, this means that the user ID and password pair in the [SECURITY] section must be a valid EnterpriseOne user ID and password and database user ID and password.
DefaultEnvironment=	P810ASD1	Defines a valid environment in which the path code defines the F98OWSEC table.
SecurityServer=	security server name	
ServerPswdFile=	TRUE	<p>The setting of this parameter determines whether EnterpriseOne uses special password handling for batch reports running on the server. Set the value to TRUE to instruct the software to enable special handling of passwords. Set the value to FALSE to disable special handling.</p> <p>When the software runs a batch report on the server, it runs the report by using a string of line commands and parameters that includes the user password. Under some operating systems, the status of a job can be queried and the parameters that were used to start the process can be viewed.</p> <p>As a security measure, you can enable special handling by EnterpriseOne. When enabled, the software does not include the user password in the parameter list for a batch process. Instead, it includes the name of a file that contains the user password. The software instructs the operating system to destroy this file as soon as the batch report reads the password.</p>
History=	0	

Setting	Typical Value	Purpose
SecurityMode=	0 (default) 1 2	This setting controls whether EnterpriseOne uses the standard logon procedure, unified logon, or both. Valid values are: <ul style="list-style-type: none"> • 0: Accepts only the standard logon. • 1: Accepts only the unified logon. • 2: Accepts both.
AllowedUsers=	group or user names	This setting for the unified logon feature enables you to specify users or groups who are allowed to use EnterpriseOne. If no users or groups are specified, all of the users who have logged on to the proper domains are authenticated by the unified logon server.

[SVR]

The settings in this section contain environment and subdirectory information:

Setting	Typical Value	Purpose
SpecPath=		This line and all of the following lines in this section specify the path names that enable source programs to locate files. This value is not updated by any program or process. The only reason to change this value is aesthetic.
PackedSpecPath=	/810APP	

[TCENGINE]

The TCENGINE settings are:

Setting	Typical Value	Purpose
TraceLevel=	0 (default)	The level of table conversion logging to perform. Valid values are 0-9, where 9 generates the most logging, and 0 generates no logging.
StopAfterRow=	0 (default)	The number of rows to process during table conversion. This setting is useful for debugging. The value 0 indicates that the table conversion processes all rows. Enter a number to indicate the number of rows after which to stop proceeding.
ForceRowByRow=	0 (default) 1	Valid values are: <ul style="list-style-type: none"> • 0: Allows inserts from selects. • 1: Forces table conversions to convert one row at a time, regardless of whether an insert could be used.

[UBE]

The settings in this section determine whether the jdedebug.log is on or off. This setting also determines the level of debugging:

Setting	Typical Value	Purpose
UBEException	0 1 (default)	Disable (0) or enable (1) exception handling. 0 allows the system to exit gracefully on an error. 1 brings up a debug log.
UBEChkMem	0 1 (default)	Disable (0) or enable (1) calls to jdeCheckMemory, which allows memory traces on business functions.
UBESubsystemLimit	3	Used to specify the number of subsystem jobs per report version.
UBESaveLogFile	0 (default) 1	Delete (0) or save (1) UBE log file (delete only works when DebugLevel=0).
UBEDBOutputLocation		Used to define the location for database output or mapping.
UBETabOpt=	1 0	Not delivered in the default jde.ini file. The system automatically performs row data selection optimization. However, use this setting if you want to disable row data selection optimization. The values are enabled (1) or disabled (0). If you want to re-enable optimization, you can change the value back to 1 or simply delete the UBETabOpt setting.
UBEDebugLevel=	0 (default) 1- 6	Used to specify what level of debugging information will be provided when using UBE debug logging. The highest level of logging information is 6. Valid values are: <ul style="list-style-type: none"> • 0: Error messages only • 1: Informative messages • 2: Section-level messages • 3: Object-level messages • 4: Event rules messages • 5: SQL statements • 6: UBE function messages
UBEShowPDFLink	0 (default) 1	Type 1 to show a box around PDF links.

Setting	Typical Value	Purpose
UBEPrintDataItems	0 (default) 1	Used to specify whether to print the associated data item description in the .pdf file as metadata for third-party vendors. Valid values are: <ul style="list-style-type: none"> • 0: No, do not print. • 1: Yes, do print.
UBESSDebug	0 (default) 1	Disable (0) or enable (1) printing the subsystem key.
UBEVCDebug	0 (default) 1	Auto-attach VC when starting UBE in process (NT only).
UBETHread	0 1 (default)	Run UBE as a process (0) or a thread (1).
WebServer	0 (default) 1	This setting specifies whether the system enables the UBE feature from the web server and identifies the EnterpriseOne kernel as a web kernel to meet the special needs of the web. If you leave this value blank, the calls from the business functions or the error message handling from the kernel do not work properly. Valid values are: <ul style="list-style-type: none"> • 0: Disabled • 1: Enabled

[WORKFLOW]

The WORKFLOW settings are:

Setting	Value	Purpose
Asynchronous Workflow=	FALSE	Used to activate and deactivate asynchronous workflow. The default value is FALSE.

[WORLD ENVIRONMENT MAP]

The WORLD ENVIRONMENT MAP settings are:

Setting	Value	Purpose
OneWorldEnvironmentName= (for example, APPLJDEDC2)	WorldEnvironment Name (for example, QA810COMP)	The string used by the special business function code to set up PeopleSoft World library lists from within EnterpriseOne. The library lists call PeopleSoft World software from PeopleSoft EnterpriseOne. The functions associated with these settings might not be used by application developers.

[XML Dispatch]

The XML Dispatch setting is:

Setting	Typical Value	Purpose
PollIntervalMillis=	3000	The number of milliseconds that the XML Dispatch kernel sleeps during inactivity when it is waiting on responses from other XML kernels (such as the XML Call Object kernel). The lower this value is, the more CPU cycles the XML Dispatch kernels use when waiting for responses from other XML kernels.

[XTS]

The XTS setting is:

Setting	Typical Value	Purpose
ResponseTimeout=	600	The number of seconds that the XML Dispatch kernel waits for a response from other XML kernels (such as XML Call Object kernel) before giving up on the response.

UNIX/Linux Server Jde.ini Settings

This section describes the settings found in the UNIX and Linux server jde.ini file. In these environments, there is an environment variable called JDE_BASE that defines the directory in which the jde.ini is found. Some settings might differ between server platforms. Information is organized by section, such as [DEBUG]. Sections are alphabetized, but settings found within sections are generally listed in the order in which they are found in the software.

[BSFN BUILD]

The BSFN BUILD settings are:

Setting	Typical Value	Purpose
Build Area=	/usr/PeopleSoft/810/packages	The location on the server where the package will be built.
Optimization Flags=	+01 (default for HP-UX) -02 (default for AIX) -0 (default for Solaris)	Machine dependent. These compile flags are used when building business functions in Release mode. You should not change these flags.

Setting	Typical Value	Purpose
DebugFlags=	-g -y -D_DEBUG -DJDEDEBUG (default for HP-UX) -g -qfulpath -qdbextra -D_DEBUG -DJDEDEBUG (default for AIX) -g -D_DEBUG -DJDEDEBUG (default for Solaris or Linux)	Machine dependent. These compile flags are used when building business functions in Debug mode. You should not change these flags.
InliningFlags=	blank (default)	This entry is blank for non-iSeries servers.
DefineFlags=	-DKERNEL -DPRODUCTION_VERSION -DNATURAL_ALIGNMENT -D_HPUX_SOURCE (default for HP) -D_SUN-SOURCE (default for Solaris) -D_GNU_SOURCE (default for Linux)	These definitions are passed to the compiler. The first three are common on all platforms. The remaining definitions are platform-specific.
CompilerFlags=	-Aa +w1 +z -c (default for HP-UX) -qalign=natural -qflag=I:I -c (default for AIX) -qspill=1024 (AIX only) -xCC -Xa -misalign -KPIC -c (default for Solaris) -fPIC -Wall -c (default for Linux)	Machine dependent. Valid compiler flags. The spill flag sets the stack space when business functions are compiled. This flag is not set by default, but may be needed for some older AIX compilers.
OSReleaseLevel=	+DAportable (for HP-UX only)	The release level to which you are compiling. You should not change these flags.

Setting	Typical Value	Purpose
LinkFlags=	-b -z -B symbolic -ljdesaw -L/usr/ PeopleSoft/810/system/lib (default for HP-UX) -bM:SRE -bexpall -brtl -lc -lm -bnoentry -L. -L/usr//PeopleSoft/810 /system/lib -ljdelib -lcallobj -lerror -lgtext -ljdb -ljde_erk -ljdecache -ljdeddapi -ljdeknet -ljderepl -ljdeschr -ljdesec -ljdespec -ljdetam -llanguage -lmisc -lpackage -lport -lqueeknl -lruntime -lsrc -ltransmon -lube -lworkflow -ljdesaw -ljdenet -lowver -ljdeunicode -lv_verify -bloodmap:loadmap -ljdesaw (default for AIX) -dy-G -L/usr/PeopleSoft/810 /system/lib -ljdesaw (default for Solaris) -shared -L/usr/PeopleSoft/810 /system/lib -ljdesaw (default for Linux)	<p>Machine dependent. These flags are used when linking business functions, including linking them to the jdesaw system that is the shared library. In general, you should not have to change these flags.</p> <p>The -B symbolic setting tells the HP linker to always resolve symbols (calls to functions) in the same library from where they are referenced, if possible. This action prevents a call from one library going to another library of the same name in a different path code.</p>
LinkLibraries=	blank (default)	Libraries to which business functions are linked (Windows and iSeries servers only).
SimultaneousBuilds=	0 (unlimited) (default) any integer (number of simultaneous builds)	Indicates the number of business functions libraries that can be built simultaneously. A value of 0 means that all libraries can be built simultaneously.

[CLUSTER]

The CLUSTER settings are:

Setting	Typical Value	Purpose
Primary Node=	host name	<p>When clustering is used with EnterpriseOne, this setting specifies either a primary server where the software will run or a floating IP address name. This setting can also be used to specify a "virtual" host name that overrides the actual host name. This can be useful for some load balancing applications.</p> <p>This setting is delivered commented out.</p>

[DB SYSTEM SETTINGS]

The settings in this section contain information about the default environment and path code used during the bootstrap process. A directory must reside on the server that has the same name as the default path code shown in its jde.ini file:

Setting	Value	Purpose
Version=	43	A version number to prevent a mismatch of the jde.ini file with the running version of EnterpriseOne.
Default User=	PSFT	The user account name for the database bootstrap tables.
Default Pwd=		The user account password for the database bootstrap tables. This is usually left blank.
Default Role=	*ALL	The role that is used for the bootstrap initialization (usually *ALL).
Default Env=	PD9	The default data source on the enterprise server.
Default PathCode=	PD9	The business function directory that is used for initialization.
Base Datasource=	host - B9 Server Map	The data source representing the database from which sign-in information is retrieved.
Object Owner=	SVM9	The owner of server map database tables.
Server=	server name	The server on which the database resides.
Database=	jde9	The database connect string (Oracle) or database alias name (DB2 UDB) where the server map tables reside.
Load Library=	(blank)	The EnterpriseOne driver library that is used to access the database that stores the server map tables. Beginning in PeopleSoft EnterpriseOne 8.9, this value is automatically determined.
Decimal Shift=	Y (default) N	A flag to indicate if decimal shifting is used for numeric data.
Julian Dates=	Y (default) N	A flag to indicate if dates are stored in Julian or database-specific format.
Use Owner=	Y (default) N	A flag to indicate that table names are qualified by owner.
Secured=	Y (default) N	Indicates whether this database is a secured, requiring a user and password login.

Setting	Value	Purpose
Type=	O W	A single character denoting the type of database holding the server map tables. This character can be O (Oracle) or W (DB2 UDB for Windows/Unix). Other values may be valid for accessing databases on other platforms.
JDBNetUse=	N (default) Y	Indicates whether JDBNet is being used to access the bootstrap tables.
UnicodeFlag=	N (default) Y	Indicates whether the database is enabled for Unicode data.
LOBFlag=	N (default) Y	Indicates whether the server map bootstrap tables contain BLOB data.

[DEBUG]

The settings in this section determine the location of the jde.log and jdedebug.log files. The settings are also used to turn the jdedebug.log on and off:

Setting	Typical Value	Purpose
Output=	FILE	Controls the status of the jdedebug file. Valid values are: <ul style="list-style-type: none"> NONE: No trace information is written to jdedebug.log. FILE: Database and runtime trace information is written to the file that is specified by the DebugFile= parameter in the [DEBUG] section.
ClientLog=	1 (default) 0	Valid values are: <ul style="list-style-type: none"> 1: Enables servicing of business functions JDE.LOG and JDEDEBUG.LOG entries from the server to the workstation. 0: Disables this service.
DebugFile=	/u01/PeopleSoft/810/log /jdedebug.log	The location and name of the jdedebug.log file.
JobFile=	/u01/PeopleSoft/810/log /jde.log	The location and name of the jde.log file.
LogErrors=	1	This setting controls whether messages are logged to the jde.log files. Changing this setting to 0 causes all logging to be turned off.
JDETSFile=	/u01/PeopleSoft/810/log /JDETS.log	Specifies the location of the lock manager trace file.

Setting	Typical Value	Purpose
RepTrace=	1	Enables replication of log messages.
TAMTraceLevel=	0	Set the level of logging for spec (or TAM) file operations.

[ENTERPRISE TIMEZONE ADJUSTMENT]

The setting in this section contains information for properly adjusting the Enterprise Portal time for single signon.

Setting	Purpose
EntNode=	Enables you to enter the difference, in minutes, between Greenwich Mean Time (GMT) and Enterprise Portal Node time when setting up single signon between Enterprise Portal and PeopleSoft EnterpriseOne. You should change this setting whenever daylight savings time changes to reflect the difference between GMT time and the Enterprise Portal Node time.

[INSTALL]

The settings in this section contain directory paths and general installation information:

Setting	Typical Value	Purpose
DefaultSystem=	system	The name of the subdirectory under /810 that contains the foundation code and tools.
ClientPath=	client	The name of the directory on the deployment server that contains the Workstation install program and other files that are used during deployment.
PackagePath=	package	The name of the subdirectory on the deployment server under a path code that contains the packages that were built for that path code.
DataPath=	data	The name of the subdirectory on the deployment server under the path code that contains the Access database that is delivered for all packages for that path code.
810=	/usr//PeopleSoft/810	Base path of the PeopleSoft EnterpriseOne installation.
Double_Byte=	0	
LocalCodeSet=	WE_ISO88591	A setting that is used to determine alternate language usage. See the appropriate EnterpriseOne PeopleTools 8.11 Upgrade document for other language values.

[INTEROPERABILITY]

The INTEROPERABILITY settings are:

Setting	Typical Value	Purpose
RegisteredEvents=	RTSOOUT	Names of EventTypes. An event is an EnterpriseOne business transaction running on an EnterpriseOne enterprise server. To enable real-time generation of events, you must register each event that you want to generate in realtime.
FilteredEvents=	*ALL	The value of this parameter defines the events that you want to create in realtime. A value of *ALL generates all registered events. *NONE disables event generation. You can also enter a subset of registered events.

[JDEIPC]

The JDEIPC settings are:

Setting	Typical Value	Purpose
ipcTrace=	0	Set to 1 to enable IPC logging messages. Important! This setting can cause the log files to grow very fast.
maxNumberOfSemaphores=	200	This setting defines the size of the semaphore array that EnterpriseOne creates. Changing this setting may require you to update kernel settings on Solaris or Linux platforms.
MaxNumberOfResources	1000	Not delivered in the default jde.ini file. This setting should only be added or changed if the EnterpriseOne system is reporting IPC resource allocation errors.
startIPCKeyValue	7999	Delivered commented out. On UNIX, this setting is the value of the IPC ID that EnterpriseOne uses for its shared memory. This value, plus the maxNumberOfResources, defines the range of IPC IDs that EnterpriseOne will use on the system. The default range is from 5000 to 5999. You should change this value only if there is a conflict with other software running on the server.

[JDEITDRV]

The JDEITDRV settings are:

Setting	Typical Value	Purpose
DrvCount=	3	The number of event drivers that are used for processing messages from event generators, either Z file or real-time.
Drv1=	Z:libzdrv.so (Sun and AIX) Z;libzdrv.sl (HP9000)	The directory location of the Z file event driver.
Drv2=	RT:librtdrv.so (Sun and AIX) RT:librtdrv.sl (HP9000)	The directory location of the real-time event driver.
Drv3=	JDENET:libjdetdrv.so (Sun and AIX) JDENET:libjdetdrv.sl (HP9000)	The directory location of the JDENET driver.

[JDEMAIL]

The JDEMAIL setting is:

Setting	Typical Value	Purpose
mailServer=	mail.peoplesoft.com	The name of the SMTP server to access for sending server mail messages.

[JDENET]

The JDENET settings are:

Setting	Typical Value	Purpose
serviceNameListen=	6012	The port number or service name that is used by EnterpriseOne to communicate with clients and other servers.
serviceNameConnect=	6012	The port number or service name that is used by EnterpriseOne to communicate with clients and other servers.

Setting	Typical Value	Purpose
maxNetProcesses=	5	<p>Defines the maximum number of jdenet_n processes that can be running. You can increase the value for a server that is expecting a large number of concurrent users.</p> <p>If you need two or more processes, note that the first process is used exclusively to handle new connections and distribute them evenly among the other processes. In this case, you must add an extra process to act as a broker. Thus, the number of connections each jdenet_n process will handle is defined by the formula:</p> $(\text{maxNetConnections}) / (\text{maxNetProcesses} - 1)$ <p>If you increase the maxNetConnections setting, you should also increase the maxNetProcesses setting accordingly. In general, allow at least one jdenet_n process per 250 concurrent users.</p>
maxNetConnections=	1000	The total number of connections that all jdenet_n process can handle. This value is site-specific. You can increase the value for a server that is expecting to handle larger number of concurrent users.
maxKernelProcesses=	50	The maximum number of jdenet_k processes that can be running. The value should be greater than the sum of all maxNumberOfProcesses settings for the dedicated servers.
maxKernelRanges=	24	The number of dedicated server types
netTrace=	0	Enables JDENET log messages. This setting should be turned off (set to 0) unless specifically needed for debugging, as it can impact performance of the EnterpriseOne system even when debug logging is not enabled.
HandleKrnISignals=	1	<p>Not delivered in default jde.ini file. Used for debugging purposes.</p> <p>Turns on and off the handling of signals that are delivered to the process. Kernel processes read the setting on startup. A value of 1 turns on handling, which means that the kernel process handles the signal, performs some cleanup tasks, and exits. A value of 0 turns off signal handling. With a value of 0, when signals are delivered to a process, the process writes out a core file. The core file contains data that developers can use to determine the cause and location of the signal. Use the value of 0 for debugging purposes.</p> <p>Once EnterpriseOne service has started, only processes started after you make a change to this setting are affected.</p>

Setting	Typical Value	Purpose
netCoreDump=	0	For internal use only. Not delivered with the RS/6000.
netTemporaryDir=	temporary file directory	Not delivered in default jde.ini file. Use this setting to change the directory to use for EnterpriseOne temporary files. Without this setting, most temporary files are created in the system default directory (usually /tmp). Some parts of the EnterpriseOne system may use the Unix environment variable TMPDIR to determine the location for temporary files.

[JDENET_KERNEL_DEFx]

This section defines internal dedicated server processes for EnterpriseOne. The sections are numbered JDENET_KERNEL_DEF1 to JDENET_KERNEL_DEF24. The settings in these sections should not be changed except as noted:

Setting	Value	Purpose
krnlName	DEF1: JDENET RESERVED KERNEL DEF2: UBE KERNEL DEF3: REPLICATION KERNEL DEF4: SECURITY KERNEL DEF5: LOCK MANAGER KERNEL DEF6: CALL OBJECT KERNEL DEF7: JDBNET KERNEL DEF9: SAW KERNEL DEF10: SCHEDULER KERNEL DEF11: PACKAGE BUILD KERNEL DEF12: UBE SUBSYSTEM KERNEL DEF 13: WORKFLOW KERNEL DEF 14: QUEUE KERNEL DEF 15: XML TRANS KERNEL DEF 16: XML LIST KERNEL DEF 19: EVENT NOTIFICATION KERNEL DEF 20: INTEROPERABILITY EVENT OBSERVER KERNEL DEF 22: XML DISPATCH KERNEL DEF 23: XTX KERNEL DEF 24: XML SERVICE KERNEL	<ul style="list-style-type: none"> Value should not be changed. DEF1: Used for internal purposes and testing. DEF2: Processes batch process requests. DEF3: Processes data replication requests. DEF4: Processes security server requests. DEF5: Processes transaction manager and lock manager requests. DEF6: Processes requests for remote master business functions (MBF). DEF7: Processes JDBNet server-to-server requests. DEF9: Processes SAW application requests. DEF10: Processes Scheduler application requests. DEF11: Processes package build requests. DEF12: Processes UBE subsystem requests. DEF13: Processes workflow requests. DEF14: Processes job queue messages. DEF15: Processes XML transactions. DEF16: Processes and returns request for data in XML document format. DEF19: Processes real-time events and XML documents that are generated by the Interoperability Event Observer, as well as Z file events. Publishes all EnterpriseOne events to subscribers. DEF20: Processes information from business functions calling real-time APIs and uses that information to create an XML or a Z file that is publishable to subscribers by the Event Notification Kernel. DEF22: Kernel for routing XML messages to their proper kernel. DEF23: Kernel for transforming XML messages from one type to another. DEF24: Processes inbound XAPI messages.

Setting	Value	Purpose
dispatchDLLName=	DEF1: libjdenet.{ext} DEF2: libjdeknet.{ext} DEF3: libjderepl.{ext} DEF4: libjdeknet.{ext} DEF5: libtransmon.{ext} DEF6: libxmlcallobj.{ext} DEF7: libjdeknet.{ext} DEF9: libjdesaw.{ext} DEF10: libjdeschr.{ext} DEF11: libjdeknet.{ext} DEF12: jdekernel.{ext} DEF13: libworkflow.{ext} DEF14: libqueueknl.{ext} DEF15: libxmltransactions. {ext} DEF16: libxmllist.{ext} DEF19: libjdeie.{ext} DEF20: libjdeieo.{ext} DEF22: libxmldispatch. {ext} DEF23: libxtskrnl.{ext} DEF24: libxmlservice.{ext}	<p>Values should not be changed.</p> <p>Identifies the name of the library loaded by the given kernel type. The library extension {ext} is .sl for HP-UX, and .so for the other Unix platforms.</p>

Setting	Value	Purpose
dispatchDLLFunction=	DEF1: JDENET_Dispatch Message DEF2: JDEK_ DispatchUBEMessage DEF3: DispatchRepMessage DEF4: JDEK_ DispatchSecurity DEF5: TM_ DispatchTransactionManager DEF6: JDEK_ DispatchCallObject Message DEF7: JDEK_ DispatchJDBNETMessage DEF9: JDEK_ DispatchSAWMessage DEF10: JDEK_ DispatchScheduler DEF11: JDEK_ DispatchPkgBuildMessage DEF12: JDEK_ DispatchUBESBSMessage DEF13: JDEK_ DispatchWFServer Process DEF 14: DispatchQueueMessage DEF16:XMLListDispatch DEF19: JDEK_ DispatchITMessage DEF20: JDEK_ DispatchIEOMessage DEF22: XMLDispatch DEF23: JDEK_ dispatchXTSMessage DEF24: XMLServiceDispatch	The name of the main function for handling messages of the give type. The dispatchDLLName and dispatchDLLFunction entries are platform-specific.

Setting	Value	Purpose
maxNumberOfProcesses=	1	The maximum number of kernel processes that can be run on this server for each kernel type. Some settings may need to be changed based on user count.
numberOfAutoStartProcesses=	0	The number of kernel processes that automatically start for each kernel type. If this number is 0, then no processes start automatically for that kernel type. This number must be less than the maximum number of processes for that kernel type. The user can modify this setting to tune performance. The default value is 0 for all JDENET_KERNEL_DEF sections.

[LOCK MANAGER]

The LOCK MANAGER section enables transaction processing and includes the following settings:

Setting	Typical Value	Purpose
Server=	server name	This setting specifies the name of the lock manager server to be used to process records—for example, a server name might be <code>intelna</code> .
AvailableService=	TS	<p>This setting indicates the service that the lock manager server is offering. It is also used to indicate whether the lock manager server is on or off. Valid values are:</p> <ul style="list-style-type: none"> • TS Time stamp service. • NONE No service is available. <p>Note. This setting only applies to servers.</p>
RequestedService=	TS	<p>This setting indicates the type of service that the workstation requests from the server. The service that is currently being provided by servers is time stamping (TS) only. Valid values are:</p> <ul style="list-style-type: none"> • TS • NONE

[LREngine]

The LREngine setting is:

Setting	Typical Value	Purpose
System=	/owdisk2/810/bdev/output	The directory location of the List-Retrieval Engine, a database that is used to manage access to XML repository files.

[NETWORK QUEUE SETTINGS]

The settings in this section contain the name of the queue that is used when running batch jobs on the server. The settings also show the workstation's UBE priority, and whether to hold the jobs in a spool file or immediately send them to a printer:

Setting	Typical Value	Purpose
OutputDirectory=	directory name	Not delivered in the default jde.ini file. This is the directory where you want to create the PrintQueue directory. The default value is the install location found in the [INSTALL] section of the jde.ini.
JDENETTimeout=	60	The timeout value, listed in seconds, for clients to attempt to connect to the server. A server can act as a client when it uses JDBNET, submits UBEs to another server, calls a business function on another server, uses a Lock Manager on another server, or when it makes security server requests to another server.
QKOnIdle	300	If the queue kernel is idle for this amount of time, it does a check of each of its queues and performs any necessary cleanup activities. The time is in seconds.

[SAMPLE_EVENT]

The SAMPLE_EVENT settings are:

Setting	Typical Value	Purpose
DS1=	D4202150B	Defines the data structure for each real-time event registered in the [INTEROPERABILITY] section. Replace [SAMPLE_EVENT] with an event name, such as RTSOOUT, and then enter the values that define the data structure of the event.
DS2=	D4202150C	
DS3=	D34A1050C	

[SECURITY]

The SECURITY settings are:

Setting	Typical Value	Purpose
User=	PSFT	This value must be a valid EnterpriseOne user ID and database user ID. Accordingly, this means that the user ID and password pair in the [SECURITY] section must be a valid EnterpriseOne user ID and password and database user ID and password.
Password=	PSFT	This value must be the correct password for the EnterpriseOne user ID specified in the User setting of the [SECURITY] section. Accordingly, this means that the user ID and password pair in the [SECURITY] section must be a valid EnterpriseOne user ID and password and database user ID and password.
Default Role=	*ALL	The role that is used for the security data source (usually *ALL).
DefaultEnvironment=	PD9	Defines a valid environment in which the path code defines table F98OWSEC.
DataSource=	System B9	The name of the data source that contains the security tables.
SecurityServer=	server name	The name of the server that provides security services. Usually this corresponds to the current host.
ServerPswdFile=	TRUE	The setting of this parameter determines whether the software uses special password handling for batch reports running on the server. Set the value to TRUE to instruct the software to enable special handling of passwords. Set the value to FALSE to disable special handling. (Typically, this is only done for debugging purposes.)
History=	0	

[SERVER ENVIRONMENT MAP]

The SERVER ENVIRONMENT MAP settings are:

Setting	Typical Value	Purpose
environmentName=	environment name	Allows one environment name to be translated to another name and be treated by the server accordingly.

[SVR]

The settings in this section contain environment and subdirectory information:

Setting	Typical Value	Purpose
EnvType=	1	Used by JDEKRNL.
EnvironmentName=	PD9	Default EnterpriseOne startup environment.
SpecPath=	spec	This line and all of the following in this section specify the path names so that other EnterpriseOne source programs know where to look for files. For instance, if spec were ever to be changed to specifications, changing SpecPath would allow changes to be made quickly. This value is not updated by any program or process. The only reason to change this setting is aesthetic. This setting is the subdirectory under the path code user to store the replicated set of specification files on the workstation.
SourcePath=	source	
ObjectPath=	obj	
HeaderPath=	include	
HeaderVPath=	includev	
BinPath=	bin32	
LibPath=	lib32	
LibVPath=	libv32	
MakePath=	make	
WorkPath=	work	
CodeGeneratorPath=	cg	
ResourcePath=	res	
HelpPath=	helps	
NextIDPath=	nextid	
LibraryListName=	PD9	Default EnterpriseOne startup environment.

[WORKFLOW]

The WORKFLOW settings are:

Setting	Value	Purpose
Asynchronous Workflow=	FALSE	Used to activate and deactivate asynchronous workflow. The default value is FALSE.

[XML Dispatch]

The XML Dispatch setting is:

Setting	Typical Value	Purpose
PollIntervalMillis=	3000	The number of milliseconds that the XML Dispatch kernel sleeps during inactivity when it is waiting on responses from other XML kernels (such as the XML Call Object kernel). The lower this value is, the more CPU cycles the XML Dispatch kernels use when waiting for responses from other XML kernels.

[XTS]

The XTS setting is:

Setting	Typical Value	Purpose
ResponseTimeout=	600	The number of seconds that the XML Dispatch kernel waits for a response from other XML kernels (such as XML Call Object kernel) before giving up on the response.

Windows Enterprise Server Jde.ini Settings

This section describes the settings found in the Windows enterprise server jde.ini file. Information is organized by section, such as [DEBUG]. Sections are alphabetized, but settings found within sections are listed in the order in which they appear in the software. For cases when defaults for Intel and Compaq AlphaServer processors differ, the two values are labeled.

[ACTIVE DIRECTORY]

The setting in this section is used when Active Directory is installed:

Setting	Value	Purpose
SCPToPublish	Variable. Typically, use a version of PeopleSoft EnterpriseOne running on the server—for example, PeopleSoft_ERP_810_SP1.	<p>Identifies the Service Connection Point (SCP) object in Active Directory. When a user signs in to EnterpriseOne, the software searches Active Directory for an SCP object with a service name that matches the parameter value in the [ACTIVE DIRECTORY] section of the workstation jde.ini file. The software chooses an SCP object with a status of <i>running</i> and retrieves the server name and port number, thus enabling the workstation to make a connection to the server.</p> <p>If you move EnterpriseOne service from one server to another or change the service port number, no changes to the workstation jde.ini file are needed, as long as the name of the SCP object in Active Directory and the parameter values of the [ACTIVE DIRECTORY] section of the workstation jde.ini file match.</p>

[BSFN BUILD]

The BSFN BUILD settings are:

Setting	Value	Purpose
DoCompression=	0	<p>Used to compress server packages for redeployment to other servers of the same platform type. This setting saves you from having to build a package on each server. Valid values are:</p> <ul style="list-style-type: none"> • 0: Do not use compression. • 1: Use compression.
BuildArea=	Z: \PeopleSoft\810\ddp\packages	The location on the server where the Package Name directory will be created and the package built.
DebugFlags=	/Gz /Od /Zi /MDd /Yd /W4 /GX /Gy /D_DEBUG	Machine dependent. These compile flags are used when building business functions in debug mode. You should not change these flags.
OptimizationFlags=	/Gz /O2 /MD /W4 /GX /Gy	Machine dependent. These compile flags are used when building business functions in release or optimize mode. You should not change these flags.
OSReleaseLevel=	5.0	The Windows server release level to which you are compiling. You should not change this flag.
DefineFlags=	/D WIN32 /D _WINDOWS /D IAMASERVER /D KERNEL	Machine dependent. These compile flags are used when linking business functions. You should not change these flags.
CompilerFlags=	/nologo /c	Machine dependent. These compile flags are used when linking business functions. You should not change these flags.

Setting	Value	Purpose
LinkFlags=	/DLL /DEBUG /SUBSYSTEM:windows /FORCE:MULTIPLE /FORCE:UNRESOLVED /INCREMENTAL:YES /VERBOSE /MAP	Machine dependent. These flags are used when linking business functions. You should not change these flags.
LinkLibraries=	jdekrm.lib, jdel.lib, jdenet.lib, jdeipc.lib	Libraries to which business functions are linked.
SimultaneousBuilds=	0	Indicates the number of processes that are started for the business function build. 0 means to run as many build processes as possible.

[BSFN Builder]

The settings in this section are for PeopleSoft internal use only:

Setting	Value	Purpose
User=	JDE	User ID used to run BSFNBuilder.exe.
Pwd=	JDE	User password used to run BSFNBuilder.exe.
PathCode=	appl_pgf	Pathcode under which BSFNs are built.
Build Area=	z: \PeopleSoft\810\ddp	The path to the parent directory of the pathcode for the business functions that you are building. This setting is typically the same as the base installation directory.
DBSFNFlags=	/Gz /Od /Zi /MDd /Yd /W4 /GX /Gy /Fp\$(PRECOMPHDR) /D WIN32 /D _DEBUG /D _WINDOWS /D IAMASERVER /D KERNEL /nologo /c	Machine-dependent compiler flags that are used to create debug builds.
RBSFNFlags=	/Gz /O2 /MD /W4 /GX /Gy /Fp\$(PRECOMPHDR) /D WIN32 /D NDEBUG /D _WINDOWS /D IAMASERVER /D KERNEL /nologo /c	Machine-dependent compiler flags that are used to create release builds.

Setting	Value	Purpose
DLinkFlags=	/DLL /DEBUG /SUBSYSTEM:windows /out:\$(DLLTARGET) /PDB:\$(PDB) /IMPLIB:\$(LIBRARY) /FORCE:MULTIPLE /FORCE:UNRESOLVED /INCREMENTAL:YES /VERBOSE /MAP	Machine-dependent link flags for debug builds.
RLinkFlags=	/DLL /DEBUG /SUBSYSTEM:windows /out:\$(DLLTARGET) /PDB:\$(PDB) /IMPLIB:\$(LIBRARY) /FORCE:MULTIPLE /FORCE:UNRESOLVED /VERBOSE /MAP:\$ (MAPTARGET)/OPT:REF	Machine-dependent link flags for release builds.
KeepMake=	0	The status of make files after the build. Valid values are: <ul style="list-style-type: none"> • 0: The default setting; do not keep. • 1: Keep.
BFDDir=	bsfnerr	Subdirectory under path code that will contain build error logs. The default value is bsfnerr.

[DB SYSTEM SETTINGS]

The settings in this section contain information about the default environment and path code. A directory must reside on the enterprise server that has the same name as the default path code shown in its jde.ini file:

Setting	Value	Purpose
Version=	43	A version number to prevent a mismatch of the jde.ini file with a running version of EnterpriseOne. The only valid value is 43.
Default User=		The EnterpriseOne user ID that is used to access the bootstrap tables, F986101 and F98611.
Default Pwd=		The user password that is used to access the bootstrap tables.
Default Env=	P810HPO1	The environment that is used in situations where an environment is not specified.
Default PathCode=	PROD	The default path code. The specification files for the bootstrap tables are then read from the spec subdirectory of this pathcode folder.

Setting	Value	Purpose
Server=	hp9000a	The server where the bootstrap tables are located. This value is ignored except when jdbnet is used.
Type=	O A S I	The database type where the bootstrap tables reside. Valid values are: <ul style="list-style-type: none"> • O (Oracle) • A (MS Access) • S (SQL Server) • I (Client Access)

[DEBUG]

The settings in this section determine the location of the jde.log and jdedebug.log. The settings are also used to turn logging on and off:

Setting	Typical Value	Purpose
DebugFile=	z: \peoplesoft\810\ddp\log\jdedebug.log	The path and name of the log file that are used to write debug tracing information. The process ID is added before the period in this file name.
JobFile=	z: \peoplesoft\810\ddp\log\jde.log	The path and name of the log file that are used to write job error and warning information. The process ID is added before the period in this file name.
Output=	FILE	Controls how tracing information is written. Valid values are: <ul style="list-style-type: none"> • NONE: The default setting; no trace information is written to DebugFile. • FILE: Database and runtime information is written to DebugFile. • AUX: Tracing information is written to the program debugger output window. • BOTH: Tracing information is written to both DebugFile and the program debugger output window.
JDETSFile=	z: \peoplesoft\810\ddp\log\jdetts.log	The path and name of the log file that is used to write lock manager tracing information.

Setting	Typical Value	Purpose
KeepLogs=	1	<p>Keeps logs for UBEs in the Print Queue directory. Valid values are:</p> <ul style="list-style-type: none"> • 1: Keeps the logs created when UBEs are run. • 2: Delete the UBE logs when the UBE is finished processing. <p>Regardless of this setting, logs are kept if an error occurs when processing the UBE.</p>
TAMTraceLevel=	0	<p>Controls the amount of TAM information that is logged to the jdedebug.log. Valid values are:</p> <ul style="list-style-type: none"> • 0-10, with higher numbers increasing the amount of information being logged. • 0: Default setting; no information output.
TAMTrace=	0	<p>Controls TAM file trace information. Valid values are:</p> <ul style="list-style-type: none"> • 0: Do not write TAM trace information to the debug file. • 1: Write TAM trace information to the debug file.
ClientLog=	0	<p>Sends log information to the client and merges it with the client's jde.log and jdedebug.log files. Valid values are:</p> <ul style="list-style-type: none"> • 0: Do not send log information to the client. • 1: Send log information to the client.
QKLog=	0	<p>Controls JDE Queue Kernel tracing information. Valid values are:</p> <ul style="list-style-type: none"> • 0: Do not write Queue Kernel message information to the debug file. • 1: Write Queue Kernel message information to the debug file.
TraceRowSecurityFetch=	FALSE	<p>Controls row level security tracing. Valid values are:</p> <ul style="list-style-type: none"> • FALSE (default): Deactivate tracing. • TRUE: Activate tracing.
WTSLogs=	FALSE	<p>Creates logs in the User Profile directory for TSE installations. Valid values are:</p> <ul style="list-style-type: none"> • FALSE (default): Set the log file paths by the JobFile and DebugFile. • TRUE: Write the log files to c:\WTSRV\Profiles\%Userid%\Windows.

Setting	Typical Value	Purpose
jdelibFatal=	FALSE	Determines whether message boxes are supported. Valid values are: <ul style="list-style-type: none"> FALSE (default): Message boxes are not supported. TRUE: Message boxes are supported.
TAMMultiUserOn=	0	Determines whether multiuser access to TAM files is allowed. Valid values are: <ul style="list-style-type: none"> 0 (default). -1: Do not allow multiuser access. 1: Allow multiuser access.
TAMErrorMsgBox=	0	Controls whether TAM error messages open a message box. Valid values are: <ul style="list-style-type: none"> 0 (default): Do not write fatal error messages to a message box. 1: Write fatal error messages to a message box.

[ENTERPRISE TIMEZONE ADJUSTMENT]

The setting in this section contains information for properly adjusting the Enterprise Portal time for single signon.

Setting	Purpose
EntNode=	Enables you to enter the difference, in minutes, between Greenwich Mean Time (GMT) and Enterprise Portal Node time when setting up single signon between Enterprise Portal and PeopleSoft EnterpriseOne. You should change this setting whenever daylight savings time changes to reflect the difference between GMT time and the Enterprise Portal Node time.

[INSTALL]

The settings in this section contain directory paths and general installation information:

Setting	Typical Value	Purpose
B9=	\peoplesoft\810\ddp	The path to the EnterpriseOne base installation directory.

Setting	Typical Value	Purpose
LocalCodeSet=	WE_ISO88591	Determines the character code set used by the software. Valid values are: <ul style="list-style-type: none"> WE_ISO88591 (1252) - English JA_SJIS (932) - Japanese TC_BIG5 (950) - Traditional Chinese SC_GB (936) - Simplified Chinese KO_KSC (949) - Korean
StartServicePrefix	psft810	Uniquely identifies EnterpriseOne services to a single installation. The prefix tags EnterpriseOne services when running parallel releases on a single server. The default value is PSFT810.
DefaultSystem	system	The name of the system directory. The default value is system. Do not change this value.
Double_Byte	0	Indicates if this installation is a double-byte installation. Valid values are: <ul style="list-style-type: none"> 0 (default): No, not a double-byte installation. 1: Yes, a double-byte installation.
POSTSCRIPT_ONLY	0	Used with double-byte to force postscript only. Valid values are: <ul style="list-style-type: none"> 0 (default): Do not force. 1: Force.
	1	Used to retrieve the code page for the current process. Valid values are: <ul style="list-style-type: none"> 1 (default): Use the 1252 English code set. <0: Use 1252 (English). =0: Use the code page found in [INSTALL] LocalCodeSet in the jde.ini file. >0: Use the code page already in effect.

[INTEROPERABILITY]

The INTEROPERABILITY settings are:

Setting	Typical Value	Purpose
RegisteredEvents=	RTSOOUT	Names of EventTypes. An event is an EnterpriseOne business transaction running on a enterprise server. To enable real-time generation of events, you must register each event that you want to generate in realtime.
FilteredEvents=	*ALL	The value of this parameter defines the events that you want to create in realtime. A value of *ALL generates all registered events. *NONE disables event generation. You can also enter a subset of registered events.

[JDE_CG]

The JDE_CG settings are:

Setting	Typical Value	Purpose
TARGET=	RELEASE	The type of build that is used to compile objects. Valid values are: <ul style="list-style-type: none"> RELEASE (default): Build using release mode. DEBUG: Build using debug mode.
INCLUDES=	c:\msdev\devstudio\vc\include	The path to Microsoft Visual C++, system, and EnterpriseOne pathcode include (header) files.
LIBS=	c:\msdev\devstudio\vc\lib	The path to Microsoft Visual C++, EnterpriseOne system, and EnterpriseOne pathcode library files.
MAKEDIR=	c:\msdev\devstudio\vc\bin	The path to the directories of Microsoft Visual C++ programs.
STDLIBDIR=	c:\msdev\devstudio\vc\lib	The path to directories of Microsoft Visual C++ libraries.
ServerPackage Sleep=	60	The wait time, in seconds, between status checks of server package builds. The default value is 60.

[JDEIPC]

The JDEIPC settings are:

Setting	Typical Value	Purpose
ipcTrace=	0	Controls the number of interprocess communications (IPC) written to the jdedebug.log. Valid values are: <ul style="list-style-type: none"> • 0 (default): Write no messages to the log. • 1: Write only general trace messages to the log. • 2: Write IPC handle state trace messages to the log. • 3: Write both general and IPC handle state trace messages to the log.
startIPCKeyValue=	7001	An integer offset that is used to separate globally shared memory when running multiple instances of EnterpriseOne. The values of these keys for each instance must differ by at least the value of maxNumberOfResources. The default value is 5000.
maxNumberOfResources=	1000	The maximum number of IPC resources that the EnterpriseOne instance will use. When this value is reached, no more IPC resources can be created. The default value is 1000.
maxNumberOfSemaphores=	100	The maximum number of semaphore resources that EnterpriseOne will use. When this value is reached, no more semaphore resources can be created. On Windows NT, two semaphore resources are used to implement each message queue. The default value is 100.
maxMsgqMsgBytes=	2048	The maximum number of bytes in a message to be put on a message queue. The default value is 2048 (2K).
maxMsgqEntries=	1024	The maximum number of messages that can be on a message queue at one time. The default value is 1024.
maxMsgqBytes=	65536	The maximum number of bytes that can be on a message queue at one time. The default value is 65536 (64K).

[JDEITDRV]

The JDEITDRV settings are:

Setting	Typical Value	Purpose
DrvCount=	3	The number of event drivers that is used for processing messages from event generators, either Z file or real-time.

Setting	Typical Value	Purpose
Drv1=	Z:zdrv.dll	The directory location of the Z file event driver.
Drv2=	RT:rtdrv.dll	The directory location of the real-time event driver.
Drv3=	JDENET:jdetdrv.dll	The directory location of the JDENET driver.

[JDEMAIL]

The JDEMAIL settings are:

Setting	Typical Value	Purpose
ClientType=	Windows HTML	Defines whether the application shortcut that is attached to an external email message will contain a Windows application shortcut or a URL for an HTML application shortcut. The default value is Windows.
mailServer=	owsmtjp.jdedwards.com	The domain name of the SMTP server to access for sending server mail messages.
RuleN=	HANDLER: DATA	The SMTP email configuration rules that are taken from the F90005 table. Any empty or invalid entry is considered at the end of the list. N is a positive integer starting at 1.

[JDENET]

The JDENET settings are:

Setting	Typical Value	Purpose
serviceNameListen=	6003 jde_server	The TCP/IP port number that is used for receiving communications packets. If this value is an integer, that number is used as the port. If this value is a character string, it will be translated using the file c:\winnt\system32\drivers\etc\services into a port number and transport protocol. The default value is 6003.
serviceNameConnect=	6004 jde_server	The TCP/IP port number that is used for sending communications packets. If this value is an integer, that number is used as the port. If this value is a character string, it will be translated using the file c:\winnt\system32\drivers\etc\services into a port number and transport protocol. The default value is jde_server.

Setting	Typical Value	Purpose
maxNetProcesses=	<p>1</p> <p>If you only need one process, then maxNetProcesses=1. However, if you need two or more processes, note that the first process is used exclusively to handle new connections and distribute them evenly among the other processes. In this case, you must add an extra process to act as a broker. To determine the number of processes that you need, you must first determine the maximum number of connections that you need, and the number of connections that a single process can handle. The formula for the number of connections allowed for each process is:</p> $\frac{(\text{maxNetConnections} / (\text{maxNet Processes} - 1)) + 2}{2}$ <p>Each process requires two extra connections for listening (one for TCP and another for UDP), and an extra process is dedicated to handling incoming connections.</p>	Defines the maximum number of JDENET_N processes that can be running. You can increase the value for a server that is expecting heavy JDENET message flow.
maxNetConnections=	100	The maximum number of connections for all jdesnet and jdenet_n processes that are running. The default value is 100.
maxKernelProcesses=	50	The maximum number of JDENET_K processes that can be running. The value should be greater than all of the values added together in maxNumberOfProcesses for all the dedicated servers.
maxKernelRanges=	20	The number of dedicated server types
NetHostName=		The IP address to use if multiple network cards are used on the server.
netTrace=	1	Enables JDENET log messages.

Setting	Typical Value	Purpose
ServiceControlRefresh	1	The rate in seconds at which the Jdesctrl program refreshes its status of the services. Jdesctrl can be used instead of the Services applet to start, stop, pause, and continue EnterpriseOne net and queue services on Windows NT enterprise servers. The default value is 1.
EnablePredefinedPorts=	0	Allows EnterpriseOne net to use a predefined range of TCP/IP ports. This setting is required to permit the EnterpriseOne Java server outside a firewall. This port range starts at the port number that is specified by serviceNameListen and ends at the port that is calculated by the equation $\text{serviceNameListen} = \text{maxNetProcesses} - 1$. The default value, 0, means do not use a predefined range of ports. Set the value at 1 and restart the server if you set the server up behind a firewall.
PreConnectHosts=	0	The number of enterprise servers that will be initialized. This initialization allows the enterprise servers that are listed in the keys PreConnectHost1, PreConnectHost2, and so on, to load their bootstrap tables, thereby improving response time when task requests are actually sent to the servers.
PreConnectHostN	EntServer1	The name of enterprise servers that will be initialized. N is a positive integer, starting with 1.
NetTemporaryDir=	Variable	Allows the Server Administration Workbench (SAW) to create, transfer, and remove temporary log files larger than 5 MB. The variable should be the name of the temporary director that SAW uses to accomplish these tasks.
MaxIPCQueueMsgs	12	For internal use only.
InternalQueueTimeout	30	For internal use only.

[LOCK MANAGER]

The LOCK MANAGER section enables transaction processing and includes the following settings:

Setting	Typical Value	Purpose
Server=	server	This setting specifies the name of the lock manager server to be used to process records—for example, a server name might be intelna.

Setting	Typical Value	Purpose
RequestedService=	TS	<p>This setting indicates the type of service that the workstation requests from the server. The service that is currently being provided by servers is time stamping (TS) only. Valid value are:</p> <ul style="list-style-type: none"> • NONE (default) No service is available. • TS Time stamp service.
AvailableService=	NONE	<p>This setting indicates the service that the lock manager server is offering. It is also used to indicate whether the lock manager server is on or off. Valid values are:</p> <ul style="list-style-type: none"> • NONE (default) • TS <p>Note. This setting only applies to servers.</p>
LogServices=	0	<p>Controls lock manager tracing information. Valid values are:</p> <ul style="list-style-type: none"> • 0 (default): Do not write messages to the file specified in [DEBUG] JDETSFile. • 1: Write messages to this file.

[LREngine]

The LREngine settings are:

Setting	Typical Value	Purpose
System=	P:\Builds\BDEV_WF\output	The directory location of the List-Retrieval Engine, a database that is used to manage access to XML repository files.

[MQSI]

The settings in this section are for the header information on the message that is required for Commerce Integrator. If the adapter is being used without Net Commerce/Commerce Integrator, the create header is *No*; the following jde.ini settings are blank, except for the OWHostName:

Setting	Typical Value	Purpose
QMGRName=	JDE_QMGR	MQ Series queue manager.
QInboundName=	INBOUND.Q	MQ Series inbound message queue name. This queue is used to place incoming MQ Series messages.

Setting	Typical Value	Purpose
QErrorName=	DEFRES.Q	MQ Series default response queue name. This queue is used if a success and failure destination is not provided in the incoming message.
QOutboundName=	OUTBOUND.Q	MQ Series outbound queue name. This queue is used to place outbound MQ Series messages.
TimeoutWaitInterval=	15	Timeout wait interval for the kernel processing.
MaxBufferLength=	10240	The maximum buffer length of an MQ Series message.
CreateHeader=	YES	Create special header information in MQ Series message for Commerce Integrator.
AppGroup=	NNJDE	Used with create header.
JDEOrderStatusCode=	JDESOOUT	Used with create header. Transaction type for EnterpriseOne sales order status.
JDECustomerCode=	JDEAB	Used with create header. Transaction type for EnterpriseOne customer add and update.
JDEItemPriceCode=	JDEPRICE	Used with create header. Transaction type for EnterpriseOne price update.
JDEItemQtyCode=	JDEIL	Used with create header. Transaction type for EnterpriseOne product quantity update.
NCOrderStatusCode=	JDE.IC.F4201Z1	Used with create header. Net commerce order status code.
NCCustomerCode=	JDE.IC.F0101Z2	Used with create header. Net commerce customer add and update code.
NCProductPriceCode=	JDE.IC.F4106NC	Used with create header. Net commerce product quantity update code.
NCProductQtyCode=	JDE.IC.F41021Z1	Used with create header. Net commerce product quantity update code.
OWHostName=		EnterpriseOne host name. Used to create outbound net message. The OWHostName creates the net message to trigger the Outbound Adapter. This setting is the name of the server on which PeopleSoft EnterpriseOne is installed.

[NETWORK QUEUE SETTINGS]

The settings in this section contain information for starting batch queues:

Setting	Typical Value	Purpose
QEnv=	P810HPO1	The environment for starting batch queues.
QUser=	JDE	The EnterpriseOne user ID for starting batch queues.
QPassword=	JDE	The EnterpriseOne user password for starting batch queues.
QName=	QBATCH	The default queue name if not specified in UBEQueueN, PKGQueueN, or SPCQueueN.
QueueDelay=	30	The time, in seconds, between which the batch queues search for jobs in table F986110. The default value is 5.
JDENETTimeout=	60	The timeout value, listed in seconds, for clients to attempt to connect to the server. A server can act as a client when it uses JDBNET, submits UBEs to another server, calls a business function on another server, uses a Lock Manager on another server, or when it makes security server requests to another server.
UBEQueues=	1	The total number of batch queues that are devoted to handling UBE requests. Set the value at 2 if you launch a subsystem UBE to run on the server. This value allows the subsystem UBE to run in one queue while normal UBEs can run in a separate queue. This setting is necessary because the subsystem UBE goes into a permanent processing mode and consumes all other UBEs in the queue.
UBEQueueN=	QBATCH	The names of the UBE batch queues. <i>N</i> ranges from 1 to the value of UBEQueues.
SpecInstallQueues=	1	The total number of batch queues that are devoted to handling spec file installation requests. The default value is 1.
SpcQueues=	QBATCH	The names of the specification installation queues. <i>N</i> ranges from 1 to the value of SpcQueues.
KillImmediate=	1	The action of the shutdown process. Valid values are: <ul style="list-style-type: none"> • 0: Allows batch queue processes to finish their current task after receiving a shutdown request. • 1 (default): Stop queue processes immediately upon receiving a shutdown request.
OutputDirectory=	z: \peoplesoft\810 \ddp	The parent directory for the PrintQueue directory where job files (in .pdf format) are located.

[SAMPLE_EVENT]

The SAMPLE_EVENT settings are:

Setting	Typical Value	Purpose
DS1=	D4202150B	Defines the data structure for each real-time event that is registered in the [INTEROPERABILITY] section. Replace [SAMPLE_EVENT] with an event name, such as RTSOOUT, and then enter the values that define the data structure of the event.
DS2=	D4202150C	
DS3=	D34A1050C	

[SECURITY]

The SECURITY settings are:

Setting	Typical Value	Purpose
SecurityServer=	server1	This value must be a valid EnterpriseOne user ID and database user ID. Accordingly, this means that the user ID and password pair in the [SECURITY] section must be a valid EnterpriseOne user ID and password and database user ID and password.
User=	JDE	This value must be the correct password for the EnterpriseOne user ID specified in the User setting of the [SECURITY] section. Accordingly, this means that the user ID and password pair in the [SECURITY] section must be a valid EnterpriseOne user ID and password and database user ID and password.
Password=	JDE	The database account password that is used to access security table F98OWSEC.
DefaultEnvironment=	JDEOPT32	The default environment in which the security kernel runs.
DataSource=	System - 810	The data source where security table F98OWSEC can be found. The default value is System - 810.
SecurityMode=	0, 1, or 2	Controls whether the software accepts a standard logon, unified logon, or both. Valid values are: <ul style="list-style-type: none"> • 0 (default): Accept only the standard logon. • 1: Accept only the unified logon. • 2: Accept both.
AllowedUsers=	EnterpriseOne _users, Bowens	A comma-delimited list of user accounts, groups of user accounts, or both, that are permitted to sign in to EnterpriseOne using unified logon. This setting allows the users to bypass the EnterpriseOne client sign-in screen.

Setting	Typical Value	Purpose
NumServers=	1	The total number of servers running security services that can validate a connection. The security server request is sent to each security server in turn until one answers the request or no more security servers are listed. The default value is 1.
History=	0	Turns on the signon security history logging. This information is stored in table F9312.

[SERVER ENVIRONMENT MAP]

The SERVER ENVIRONMENT MAP settings are:

Setting	Typical Value	Purpose
ENV1=	ENV2	Maps one environment name to another. Wherever ENV1 is to be used on the enterprise server, it is replaced by ENV2. Multiple environment mappings can be specified.

[SVR]

The settings in this section specify path names so that other programs can find source, headers, specifications, and other information:

Setting	Typical Value	Purpose
SpecPath=	spec	The path to TAM files. Do not change.
SourcePath=	source	The path to business function source files. Do not change.
ObjectPath=	obj	The path to business function object files. Do not change.
HeaderPath=	include	The path to business function header files. Do not change.
HeaderVPath=	includev	The path to third-party vendor header files. Do not change.
BinPath=	bin32	The path to system and business function executables and DLLs. Do not change.
LibPath=	lib32	The path to system and business function library files. Do not change.
LibVPath=	libv32	The path to third-party vendor library files. Do not change.

Setting	Typical Value	Purpose
MakePath=	make	The path to business function make files. Do not change.
WorkPath=	work	The path to work files. Do not change.
FontPath=	res\fonts	The path to font files. This setting can be used in creating batch reports.
SysFontPath=	winnt\fonts	The path to Windows NT system font files. This setting can be used in creating batch reports.

Server Jde.ini Settings for WebSphere

This section details the settings that are found in the enterprise server jde.ini file as needed to run WebSphere third-party software. The information in this section supplements the information for the platform-specific sections. Information is organized by section, such as [JDENET]. Sections are alphabetized, but settings found within sections are generally listed in the order they are found in the software.

[JDENET]

The JDENET settings are:

Setting	Typical Value	Purpose
maxKernelRanges=	13	The maximum number of kernel types and ranges that will be used. Verify that this number is updated to the next number.

[JDENET_KERNEL_DEF13]

This section defines JDENET internal dedicated server processes.

Setting	Typical Value	Purpose
krnlName=	MQSI Kernel	
beginningMsgTypeRange=	5513	The beginning message of the range for each kernel type.
endingMsgTypeRange=	6001	The ending message of the range for each kernel type.
dispatchDLLName=	mqsadapt.dll	This setting determines the .DLL that is used for kernel processes.
dispatchDLLFunction=	_JDEK_DispatchMQ SeriesProcess@28	The name of the kernel function for handling kernel request messages.

Setting	Typical Value	Purpose
maxNumberOfProcesses=	1	The maximum number of kernel processes that can be run on this server for each kernel type.
numberOfAutoStartProcesses=	1	The number of kernel processes that automatically start for each kernel type. Verify that this value is 1.

[MQSI]

The settings in this section are for the header information on the message that is required for Commerce Integrator. If the adapter is being used without Net Commerce/Commerce Integrator, the create header is No and the following jde.ini settings would be blank, except for the OWHostName:

Setting	Typical Value	Purpose
QMGRName=	JDE_QMGR	MQ Series queue manager.
QInboundName=	INBOUND.Q	MQ Series inbound message queue name. This queue is used to place incoming MQ Series messages.
QErrorName=	DEFRES.Q	MQ Series default response queue name. This queue is used if a success and failure destination is not provided in the incoming message.
QOutboundName=	OUTBOUND.Q	MQ Series outbound queue name. This queue is used to place outbound MQ Series messages.
TimeoutWaitInterval=	15	Timeout wait interval for the kernel processing.
MaxBufferLength=	10240	The maximum buffer length of an MQ Series message.
CreateHeader=	YES	Create special header information in MQ Series message for Commerce Integrator.
AppGroup=	NNJDE	Used with create header.
JDEOrderStatusCode=	JDESOOUT	Used with create header. Transaction type for sales order status.
JDECustomerCode=	JDEAB	Used with create header. Transaction type for customer add and update.
JDEItemPriceCode=	JDEPRICE	Used with create header. Transaction type for price update.
JDEItemQtyCode=	JDEIL	Used with create header. Transaction type for product quantity update.
NCOrderStatusCode=	JDE.IC.F4201Z1	Used with create header. Net commerce order status code.

Setting	Typical Value	Purpose
NCCustomerCode=	JDE.IC.F0101Z2	Used with create header. Net commerce customer add and update code.
NCPProductPriceCode=	JDE.IC.F4106NC	Used with create header. Net commerce product quantity update code.
NCPProductQtyCode=	JDE.IC.F41021Z1	Used with create header. Net commerce product quantity update code.
OWHostName=		EnterpriseOne host name. Used to create outbound net message. The OWHostName creates the net message to trigger the Outbound Adapter. This setting is the name of the server on which EnterpriseOne is installed.

Web Server Jas.ini Settings

The jas.ini file defines the startup Object Configuration Manager and other web server-specific properties for the web server to communicate back to the enterprise environment. It is also the key to the installation. If any critical settings are incorrect or left blank, the web server does not run. The critical settings are listed in a separate table for each of the following sections.

The jas.ini file is automatically updated during web server installation using the Java Server Installer. However, you can modify the jas.ini settings after installation by using a text editor. The jas.ini file is functionally similar to the jde.ini file on the enterprise server.

Note. Many of the settings in the jas.ini file are located in a file called jdbj.ini.

See [Chapter 27, “Understanding the Jde.ini File Settings,” Web Server Jdbj.ini Settings, page 395.](#)

To configure the jas.ini file, the supply server must:

- Add server names that are specific for your installation to parameters in the [SECURITY] and [SERVER] sections.
- Verify the path names for various settings that are path-name-specific.
If you follow the recommendations, you should not need extensive modifications to these paths.
- Verify the port numbers for the TCP/IP connections.

Note. A good practice is to add a comment line to the .ini files to include such information as:

The current JAS package version (as labeled on the CD).

The date when you manually updated the file.

The person’s name who performed the updates.

The following table summarizes the jas.ini settings that are used by the Java server:

Setting	Description
[DB SYSTEM SETTINGS]	<p>This optional section is not delivered as part of the standard jas.ini.</p> <p>This section contains settings that enable load balancing for multiple JAS instances by using the Redirector functionality.</p>
[SECURITY]	This section contains EnterpriseOne security information.
[OWWEB]	This section contains PeopleSoft EnterpriseOne web server-specific settings. Modify for the environment.
[PORTAL CONFIGURATION]	<p>This section contains optional settings for the Portal. The settings in this section are the default settings and are not required to be included as part of the jas.ini. That is, if no value is specified in the jas.ini, the Portal automatically uses the default setting that is listed in this section.</p> <p>However, for sites that need to modify any values that can be read from the jas.ini, the values must be entered and modified as appropriate for that custom installation.</p> <p>Note. Future installations might not preserve the custom modifications, so saving a copy of the jas.ini before doing an upgrade is important.</p>
[CACHE]	This section contains HTTP session settings.
[DB CONNECTION POOL]	Starting with PeopleSoft EnterpriseOne 8.9, this section was renamed and moved to the jdbj.ini file.
[JDBC URL]	Starting with PeopleSoft EnterpriseOne 8.9, this section was renamed and moved to the jdbj.ini file.
[JDBC DRIVERS]	Starting with PeopleSoft EnterpriseOne 8.9, this section was renamed and moved to the jdbj.ini file.
[SERVER COMPONENTS]	This section loads Java server packages. Do not modify this section.
[JDENET]	This section specifies values for the Java server to communicate with the PeopleSoft EnterpriseOne enterprise server.
[SERVER]	This section specifies values for the Java server to retrieve data dictionary error descriptions from the enterprise server.
[LOGIN]	This section contains settings for login and the Local Director.
[LOGS]	This section turns on debug logging and specifies the location of log files.
[TRANSACTIONS]	This section contains configuration settings to configure transaction processing within JAS.
[JAS Instance]	<p>This optional section is not delivered as part of the standard jas.ini.</p> <p>This section contains settings to define multiple JAS instances by using the Redirector functionality. Multiple instances can be defined to improve performance and to scale installations for large user bases. The default mechanism for allocating users among multiple JAS instances is round robin or sequential selection.</p>

Setting	Description
[JAS Weight]	This optional section is not delivered as part of the standard jas.ini. This section contains settings that enable load balancing for multiple JAS instances by using the Redirector functionality.
[Redirector]	This optional section is not delivered as part of the standard jas.ini. This section specifies the location to which the Redirector will redirect if no web server is available. Typically, this location is an HTML page that provides an explanation.
[ERPINTERACTIVITY]	This section is used to activate and configure the Interactive HTML settings.
[WEB GUI]	This section is used to configure the web GUI interface.

[CACHE]

The values that are specified for these keys are in milliseconds. For example, 60000ms is equal to 1 minute.

Many of the settings that were in this section before PeopleSoft EnterpriseOne 8.9 have been moved.

See [Chapter 27, “Understanding the Jde.ini File Settings,” Web Server Jdbj.ini Settings, page 395](#).

Parameter	Recommended Setting	Description
UserSession=	2400000	<p>The time in milliseconds before an inactive user session cache is cleaned up.</p> <p>Note. This value must be greater than the Invalidate Time setting in WebSphere to prevent the Java server from timing out before WebSphere. To check the Invalidation Timeout setting in WebSphere, open the WebSphere Administrative Console, expand the node to the Application Server (AS_JDEdwards_1), click the Services, select Session Manager Services, and then click the Advance tab. Verify that Invalidation Timeout is enabled and set to an appropriate value (in minutes).</p> <p>Default value: 12000000.</p> <p>TheUserSession value must always be greater than the HTTP session timeoutInvalidate Timeout setting in WebSphere.</p> <p>Effect of Change: When theHTTP Session timeout value is reached, JAS receives notification to remove the UserSession from cache. Changing theUserSession value does not effect change, as long as this value greater than theHTTP session timeout value in WebSphere.</p>
CacheCheck=	300000	<p>The time in milliseconds to check the status of all the objects stored in cache.</p> <p>Default value: 300000.</p> <p>Note. We strongly recommend that you use the default value.</p> <p>Minimum value: 60000. If a lower value than 60000 is used, CacheManager checks the value stored in cache too frequently, which creates more overhead on the JAS server.</p> <p>Maximum value: 600000. Do not use a greater value than 600000 because the CacheManager is not able to check the status of cached objects often, and invalid objects remain in cache even after they expire.</p> <p>Relationship: This value does not depend on any other parameters in the jas.ini file.</p> <p>Effect of Change: If you decrease this value, CacheManager checks the value that is stored in cache very frequently, which creates overhead in the JAS server. If you increase this value too much, then CacheManager does not check the status of cached objects often, and invalid objects remain in cache even after they expire.</p>

[JAS PREFERENCE]

The settings for the JAS PREFERENCE section are:

Setting	Typical Value
JasServer=	ownts1
Port=	80
Servlet=	/jde/servlet/html.login

[JDENET]

Use this section only if you are running business functions and launching UBEs without the JOWProxy service:

Parameter	Recommended Settings	Description
serviceNameConnect		The TCP port on which the enterprise server is listening. Modify for the environment.
enterpriseServerTimeout=	90000	The time in milliseconds before a timeout condition can occur.
MaxPoolSize=	50	The maximum number of connections to the enterprise server. This setting is hidden.
TempFileDir=	c:\810\internet (Windows) /tmp (iSeries and UNIX)	A temporary directory for jdenet. This entry must be a valid directory on the system.

[LOGS]

This section is used to set system-dependent values for various logging functions that are related to the PeopleSoft EnterpriseOne Java server:

Parameter	Recommended Setting	Description
Debug=	FALSE	TRUE: Debug logging is enabled. FALSE: Debug logging is disabled.
Log=	Site-dependent variable	The name and location of the jas.log file. The directory in the path must exist on the system.
Debuglog=	Site-dependent variable	The name and location of the jasdebug.log file. The directory in the path must exist on the system.
JdbcTrace=	FALSE	TRUE: Trace logging of JDBC statements is included in the standard output log file. FALSE: No trace logging is performed.

Parameter	Recommended Setting	Description
stderr=	Site-dependent variable	<p>Specifies the WebSphere log directory for input errors.</p> <p>The stderr and stdout keys must point to the same directory that was supplied for the stderr and stdout fields when defining the WebSphere application server, typically the directory under /810. The default path is:</p> <p>iSeries: /PeopleSoft/810/stderr.log</p> <p>Windows: c:\WebSphere\AppServer\logs\stderr.log</p> <p>Unix: /u01/PeopleSoft/810/stderr.log</p>
stdout=	Site-dependent variable	<p>Specifies the WebSphere log directory for output errors. The stderr and stdout keys must point to the same directory supplied for the stderr and stdout fields when defining the WebSphere application server, typically the directory under /810. The default path is:</p> <p>iSeries: /PeopleSoft/810/stdout.log</p> <p>Windows: c:\WebSphere\AppServer\logs\stdout.log</p> <p>Unix: /u01/PeopleSoft/810/stdout.log</p>

[OWWEB]

The OWWEB settings are:

Parameter	Recommended Setting	Description
PathCodes=	('PS810','DV810','PY810','PD810')	<p>This parameter must be a valid path code for EnterpriseOne.</p> <p>The default environment is listed by path code. If this value is empty, all of the available environments are available to a particular user or group. Each path code is single quoted and separated by commas.</p>
MO QUEUE=	x:\peoplesoft\810\ internet\jdewww\ moqueue (For Windows machines)	<p>Specifies the path that is used by the web server to cache the media object files. These fields are the actual files that are used by the web browser. This path <i>must</i> translate into virtual path /jde/moqueue/ ' for the web browser.</p> <p>The web server process must have write and create authority to this path.</p>
FtpPort=	21	<p>Specifies the default port to be used for FTP.</p> <p>(Unix and iSeries only)</p>

Parameter	Recommended Setting	Description
FtpUsr=	anonymous	Specifies the user ID to use for FTP access to the media object file server. (Unix and iSeries only)
FtpPwd=	anonymous	Specifies the password to be used for FTP access to the media object file server. (Unix and iSeries only)
F0005Prefix=	DR	Column prefix for table F0005.
F0004Prefix=	DT	Column prefix for table F0004.
MaxUser=	100	The maximum number of EnterpriseOne (internet) users.
UseProxyServer=	FALSE	Defines whether the Java server uses ProxyServer functionality. Valid values are: <ul style="list-style-type: none"> FALSE: This value sends JDENET messages directly from the JAS server and does not employ any proxy server functionality. TRUE: This value sends JDENET messages through the JOWProxy process of the PeopleSoft EnterpriseOne client. This value is not valid for PeopleSoft EnterpriseOne 8.9.
UseMOWinNTShare=	TRUE (Windows) FALSE (iSeries and UNIX)	Specifies the sharing method that the web server uses to fetch the media object files from their location into the cached location of the web server. Valid values are: <ul style="list-style-type: none"> TRUE: This value specifies the Windows UNC share. FALSE: This value specifies an FTP server.
PrintImmediate=	FALSE	When set to FALSE, the enterprise server generates a .pdf file only. When set to TRUE, the enterprise server generates a .pdf file and converts the .pdf file to PostScript, PDL, or Line output for the UBE job.
KeepUBE=	TRUE	When set to FALSE, the JDE.LOG and JDEDEBUG.LOG files are deleted when the UBE job is completed. When set to TRUE, the JDE.LOG and JDEDEBUG.LOG are kept when the UBE job is completed.
UBEQueue=	QB810	The batch queue to which UBE jobs are submitted.
VirtualClientTimeOut	30000	The time in milliseconds before a virtual client is timed out.

Parameter	Recommended Setting	Description
SystemDateFormat=	MDE	Specifies the system data format.
SystemDateSeparator=	/	Specifies the system data separator.
HelpPath=	/jde/owhelp/	<p>This setting specifies the directory path for the help files. The syntax of the setting is:</p> <p>http://[machine]/[path]/</p> <p>If you do not specify a setting for HelpPath or use the default setting, /jde/owhelp/, the web server builds a help path that is based on the current instance of the JAS server.</p> <p>For example, if the URL for the PeopleSoft EnterpriseOne web server is:</p> <p>http://machinename:82/</p> <p>then the PeopleSoft EnterpriseOne web server assumes that the URL for the help path is:</p> <p>http://machinename:82/jde/owhelp</p>
OWJRNL=	OWJRNL	<p>This setting is only applicable to PeopleSoft EnterpriseOne web servers running on iSeries platforms. If you have manual commit turned on to update the iSeries DB2 database records, this setting allows the EnterpriseOne web server to activate the JOURNAL for the applicable iSeries tables.</p> <p>The value that you specify for this setting must be the name of the library name on the iSeries for the STRJOURNAL stored procedure.</p>
AutoPilotIDs=	FALSE	<p>This setting controls whether the Java server generates IDs that are useful for scripting HTML client actions by using the PeopleSoft AutoPilot tool. Valid values are:</p> <ul style="list-style-type: none"> FALSE: The Java server does not generate any AutoPilot IDs. TRUE: The Java server generates AutoPilot IDs.
AnonAccess=	TRUE	Enables anonymous user access.
DefaultEnvironment=	Site-dependent variable	Default environment for sign-in. Used with basic authentication.
InitialLanguageCode=	EN	ISO language code for initial user language.
LogoutProcessTimeout=	90	Number of seconds after sign-out that a business function that is activated by the user continues to run.

[PORTALCONFIGURATION]

This section contains optional settings for the PeopleSoft EnterpriseOne Portal.

If you are using a load balancer such as a Cisco LocalDirector, you must specify the `localhost` setting.

If you are using the Portal Component Importer, you must specify the `backup`, `jde`, and `servlet` settings.

With the exception of the previous settings, all of the settings that are shown in this section are the default settings and are not required to be included as part of the `jas.ini`. That is, if no value is specified in the `jas.ini`, the Portal automatically uses the default settings, as listed in this section.

However, for sites that need to modify any values that can be read from the `jas.ini`, the values must be entered and modified as appropriate for that custom installation.

Note. Future installations might not preserve the custom modifications, so saving a copy of the `jas.ini` before doing an upgrade is very important.

Parameter	Recommended Setting	Description
admin (for SP 13.1 and above)	Site-dependent-variable; no default value is used.	This setting specifies a list of user IDs separated by the character. These users can administer all of the components and workspaces, regardless of relationship.
backup	Windows: x:\temp\backup iSeries and Unix: /backup	A location where files that are about to be overwritten by the Component Importer are saved. This parameter provides a backup of the overwritten files.
cache_workspace_purge	3600000	The time in milliseconds to retain a workspace in cache without being accessed before being deleted. If set to zero, the system never purges workspaces from the cache. Changing this value can drastically affect Portal performance. Use caution when changing this value.
cache_workspace_expire	900000	For expirable components, the time in milliseconds, in addition to the last loaded timestamp before a workspace is deleted. To make a component expirable, implement <code>public long getLastLoadedTimestamp()</code> . A workspace does not expire unless a user accesses it. If set to zero, the system never expires workspaces from the cache. Changing this value can drastically affect Portal performance. Use caution when changing this value.

Parameter	Recommended Setting	Description
cache_workspace_timeout	300000	<p>The interval in milliseconds that the system should wait before checking cache for items to purge or expire. The lower the number, the better the memory conservation; but the slower the cache. If set to zero, the system never expires or purges workspaces from the cache.</p> <p>Changing this value can drastically affect Portal performance. Use caution when changing this value.</p>
cache_workspace_refresh	0	<p>The time in milliseconds before the system deletes all of the workspaces from the cache.</p> <p>Changing this value can drastically affect portal performance. Use caution when changing this value.</p>
cache_component_purge	3600000	<p>The time in milliseconds to retain a component in cache without being accessed before being deleted. If set to zero, the system never purges components from the cache.</p> <p>Changing this value can drastically affect Portal performance. Use caution when changing this value.</p>
cache_component_expire	900000	<p>For expirable components, the time in milliseconds, in addition to the last loaded timestamp before a component is deleted. To make a component expirable, implement <code>public long getLastLoadedTimestamp()</code>. A component does not expire unless a user accesses it. If set to zero, the system never expires components from the cache.</p> <p>Changing this value can drastically affect Portal performance. Use caution when changing this value.</p>
cache_component_timeout	300000	<p>The interval in milliseconds that the system should wait before checking cache for items to purge or expire. The lower the number, the better the memory conservation; but the slower the cache. If set to zero, the system never expires or purges components from the cache.</p> <p>Changing this value can drastically affect Portal performance. Use caution when changing this value.</p>

Parameter	Recommended Setting	Description
cache_component_refresh	0	<p>The time in milliseconds before the system deletes all components from the cache.</p> <p>Changing this value can drastically affect Portal performance. Use caution when changing this value.</p>
cache_itrust_purge	60000	<p>The time in milliseconds to retain an inherited trust session in cache without being accessed before being deleted. If set to zero, the system never expires or purges inherited trust session from the cache.</p> <p>Changing this value can drastically affect Portal performance and security. Use caution when changing this value.</p>
cache_itrust_expire	0	<p>For expirable components, the time in milliseconds, in addition to the last loaded timestamp before an inherited trust session is deleted. To make a component expirable, implement <code>public long getLastLoadedTimestamp()</code>. An inherited trust session does not expire unless a user accesses it.</p> <p>You should not change this setting unless instructed to do so by PeopleSoft.</p>
cache_itrust_timeout=	30000	<p>The interval in milliseconds that the system should wait before checking cache for items to purge or expire. The lower the number, the better the memory conservation; but the slower the cache. If set to zero, the system never expires or purges inherited trust sessions from the cache.</p>
cache_itrust_refresh	0	<p>The time in milliseconds before the system deletes all of the inherited trust sessions from the cache.</p>
cache_entbutton_purge	3600000	<p>The time in milliseconds to retain an Enterprise Navigation Bar button in cache without being accessed before being deleted. If set to zero, the system never purges Enterprise Navigation buttons from the cache.</p> <p>Changing this value can drastically affect Portal performance. Use caution when changing this value</p>

Parameter	Recommended Setting	Description
cache_entbutton_expire	0	For expirable components, the time in milliseconds in addition to the last loaded timestamp before an Enterprise Navigation Bar button is deleted. To make a component expirable, implement <code>public long getLastLoadedTimestamp()</code> . If set to zero, the system never expires Enterprise Navigation buttons from the cache.
cache_entbutton_timeout	900000	The interval in milliseconds that the system should wait before checking cache for items to purge or expire. The lower the number, the better the memory conservation; but the slower the cache. If set to zero, the system never expires or purges Enterprise Navigation Bar buttons from the cache.
cache_entbutton_refresh	0	The time in milliseconds before the system deletes all of the Enterprise Navigation Bar buttons from the cache.
pagegreeting	Welcome to your Portal	Default page greeting when adding a new workspace. This setting has a blank default value.
localhost	Site-dependent variable	If you are using a Cisco LocalDirector router, you must include this setting. If the port of the web server is other than 80, you must specify the port. The syntax is: <code>ip_address:port</code> , where <code>ip_address:port</code> refers to the local PeopleSoft EnterpriseOne Java server machine (not the Cisco LocalDirector machine). This information is required to enable the portal code to determine the origin of machine requests so that responses can be routed accordingly. For example: 10.0.110.79:85
styleurl	/jde/owportal/portal.css	URL of portal style sheet. Both relative and fully qualified URLs are valid.
hlpimg	/jde/owportal/images/help2.gif	Name of help image in component tool bar. Both relative and fully qualified URLs are valid.

Parameter	Recommended Setting	Description
perimg	/jde/owportal/images/ edit2.gif	Default personalize icon file path and name, such as: /jde/images/edit2.gif. Both relative and fully qualified URLs are valid.
maximg	/jde/owportal/images/ maximize2.gif	Default expand icon file path and name, such as: /jde/images/maximize2.gif. Both relative and fully qualified URLs are valid.
minimg	/jde/owportal/images/ minimize2.gif	Default contract icon file path and name, such as: /jde/images/minimize2.gif Both relative and fully qualified URLs are valid.
resimg	/jde/owportal/images/ restore2.gif.	Default restore icon file path and name, such as: /jde/images/restore2.gif. Both relative and fully qualified URLs are valid.
retimg	/jde/owportal/images/ return.gif.	Default return icon file path and name, such as: /jde/images/return.gif. Both relative and fully qualified URLs are valid.
servlet	x:\Program Files\JDEdwards\JAS\EA_JAS_80.ear\webclient.war\classes (windows) /JDEdwards/JAS/EA_JAS_80.ear/webclient.war/classes (UNIX and iSeries)	The directory where Portal servlets reside. The Component Importer/Exporter uses the directory to find and write servlets. The JAS administrator uses this directory; the administrator must create and configure it to be included in the web application's class path.
ShowCurrentEnvironmentRole	FALSE	Environment display. When set to TRUE, the system displays the current environment in the Workspace Navigation bar.
ShowSignin	TRUE	Shows the regular login link on the Workspace Navigation Bar when the user logs in anonymously.
corplogourl	/jde/owportal/images/jdelogo.gif	The URL of the default corporate logo. This image is used when the current workspace does not specify an image. Both relative and fully qualified URLs are valid.

Parameter	Recommended Setting	Description
corplogolinkurl		<p>The URL of the default corporate logo link. This link is used when the current workspace does not specify a link.</p> <p>This setting has no default value.</p> <p>Both relative and fully qualified URLs are valid.</p>
DataMigrationHasOccurred	This is a system setting; do not modify this setting or add it to the jas.ini file.	True, if 810 pristine component and workspace data have been updated.
DefaultWorkspace		<p>The workspace to display when no other workspace is specified or when DefaultWorkspaceOnly is set to TRUE. Use uppercase letters to set this parameter.</p> <p>This setting has no default value.</p>
DefaultWorkspaceOnly	FALSE	Allows access to the default workspace only.
edting	/jde/owportal/images/edit2.gif	<p>The URL of the default edit icon. The edit icon is used for buttons that enable the user to alter an object.</p> <p>Both relative and fully qualified URLs are valid.</p>
jde	<p>x:\Program Files \JDEdwards\JAS\EA_JAS_80.ear\webclient.war (Windows)</p> <p>/JDEdwards/JAS/EA_JAS_80.ear/webclient.war (UNIX and iSeries)</p>	The jdewww directory that is created at JAS install time. The Component Importer/Exporter uses the directory to find and write HTML resources such as .html, .gif, and .jpg files.
NumberOfIcons	34	Number of enterprise navigation bar icons override.
colorscheme1	<p>Default #FFFFFF #00009C #0063CE #080029 #CECECE #FFFFFF #636363 #FFFFFF background.jpg </p> <p>/jde/owportal/owportal.css</p>	Delimited string for color schemes. String consists of name, background color, tool bar color, tool bar tools color, fixed area color, border color, text color, menu color, greeting color, top background image color, and style sheet URL.
colorscheme2	<p>Springtime #FFFFFF #218C7B #84BDB5 #006B63 #CECECE #FFFFFF #FF6B29 #FFFFFF springtimebkgd.gif </p> <p>/jde/owportal/portal.css</p>	Delimited string for color schemes. String consists of name, background color, toolbar color, tool bar tools color, fixed area color, border color, text color, menu color, greeting color, top background image color, and style sheet URL.

Parameter	Recommended Setting	Description
colorscheme3	Bluedot #FFFFFF #4A5A9C #849CC6 #001873 #CECECE #FFFFFF #737BB5 #FFFFFF bluedotbkgd.gif /jde/owportal/portal.css	Delimited string for color schemes. String consists of name, background color, toolbar color, tool bar tools color, fixed area color, border color, text color, menu color, greeting color, top background image color, and style sheet URL.
colorscheme4	Techno #FFFFFF #006363 #739C9C #004242 #CECECE #FFFFFF #B5C6C6 #FFFFFF technobkgd.gif /jde/owportal/portal.css	Delimited string for color schemes. String consists of name, background color, toolbar color, tool bar tools color, fixed area color, border color, text color, menu color, greeting color, top background image color, and style sheet URL.
colorscheme5	Cityscape #FFFFFF #FF9C00 #FFC66B #000063 #CECECE #FFFFFF #636363 #FFFFFF cityscapebkgd.gif /jde/owportal/portal.css	Delimited string for color schemes. String consists of name, background color, toolbar color, tool bar tools color, fixed area color, border color, text color, menu color, greeting color, top background image color, and style sheet URL.

[SECURITY]

Confirm the following settings for the [security] section. These settings are unique to the JAS security server:

Parameter	Recommended Setting	Description
DefaultEnvironment=	JPD810	Specifies the default PeopleSoft EnterpriseOne environment.
NumServers=	1	Specifies the total number of EnterpriseOne security servers that are defined as being available to users who sign in to this EnterpriseOne web server. If this parameter is missing or has a value of blank, the default value is 1; the sign-in is handled by the primary security server that is defined by theSecurityServer= parameter in the [SECURITY] section of the jas.ini.
SecurityServer=	Site-dependent variable	Specifies the name of the security server that is defined for the EnterpriseOne enterprise server installation.

Parameter	Recommended Setting	Description
SecurityServer <i>N</i> =	Site-dependent variable	<p>Specifies the name of the secondary server. You can define multiple security servers if you want sign-in to fail over to valid secondary servers if users cannot sign in to the primary server.</p> <p>Valid values for <i>N</i> are numeric values from 1 to <i>n</i> where:</p> <p>Defines the first secondary security server</p> <p>Defines the second secondary security server</p> <p><i>N</i> defines any number of sequentially accessed security server</p>
UserLogonCookie=	FALSE	<p>Defines whether user sign-in information is saved in an encrypted cookie on the HTML client machine. This information includes user name, password, and environment. Valid values are:</p> <ul style="list-style-type: none"> • TRUE: User information is saved in an encrypted cookie that automatically populates the login screen. • DIRECT: Enables users to access login information in the cookie and bypass the login screen. • FALSE: User information is not saved in an encrypted cookie. <p>You must use this setting when using the JAS Redirector.</p>
CookieLifeTime unit is	"day"	Specifies the unit of time used by theCookieLifeTime= parameter.
CookieLifeTime=	7	Specifies the amount of time before a cookie expires, measured by the value of theCookieLifeTime unit is parameter.

[SERVER]

Use this section only if you are running business functions and launching UBEs without the JOWProxy service:

Parameter	Recommended Setting	Description
GlossaryTextServer=	machinename:port	Specifies the enterprise server and the port number on which EnterpriseOne is listening. This provides glossary text information for the EnterpriseOne web server.
codePage=	1252	The code page for displaying the glossary text information.

[SERVER COMPONENTS]

The [SERVER COMPONENTS] section of the jas.ini is used by the Java server to set environment variables. Do not modify this section unless you are instructed to do so by PeopleSoft.

Confirm the following settings within this section:

```
[SERVER COMPONENTS]
com.jdedwards.jas.UserManager
com.jdedwards.jas.JDBCProxy
com.jdedwards.jas.JDEORB
com.jdedwards.jas.DDValidaton
com.jdedwards.jas.security.SecruityBroker
com.jdedwards.jas.UDCJDBC
com.jdedwards.jas.JDEUDCtext
com.jdedwards.jas.JDEUpdates
com.jdedwards.jas.JDEQueries
com.jdedwards.jas.JDEOWDirect
com.jdedwards.jas.MenuServer
com.jdedwards.jas.ServerQuery
com.jdedwards.jas.JDESignon
com.jdedwards.runtime.virtual.VCServlet
```

Note. This last entry, `com.jdedwards.runtime.virtual.VCServlet`, is required for Multiple Application Framework (MAF) to function correctly. If this setting is missing, EnterpriseOne applications do not launch under MAF.

See Also

For the most up-to-date jas.ini and jdbj.ini settings (these settings can change with each service pack release), see the *EnterpriseOne PeopleTools 8.11 Web Server Installation*

EnterpriseOne Tools 8.94 PeopleBook: Interoperability, “Understanding Interoperability”

EnterpriseOne Tools 8.94 PeopleBook: Workflow Tools, “Creating a Workflow Process”

Web Server Jdbj.ini Settings

The jdbj.ini file contains configuration information for JDBj, which allows the web server to access EnterpriseOne databases. The parameters in this file are only used for accessing EnterpriseOne data and are ignored for standalone database access.

The critical parameters of the jdbj.ini file are automatically updated during the installation of the web server using the Java Server Installer. However, you can modify these settings after installation using a text editor. The jdbj.ini file is functionally similar to the jde.ini file on the EnterpriseOne enterprise server.

Note. In general, it is a good practice to add a comment line to the .ini files to include such information as:

The current JAS package version (as labeled on the CD).

The date that you manually updated the file.

The person's name who performed the updates.

The sections in the jdbj.ini file are divided into the following categories:

- EnterpriseOne data-specific sections
- General sections

PeopleSoft EnterpriseOne Data-Specific Sections

The following jdbj.ini sections apply only when accessing EnterpriseOne data. These sections are ignored for standalone database access:

Setting	Description
[JDBj-BOOTSTRAP SESSION]	Contains sign-in information that provides access to system tables.
[JDBj-BOOTSTRAP DATA SOURCE]	Defines the data source where the OCM and some other system tables reside.
[JDBj-SPEC DATA SOURCE]	Defines the data source where the serialized specification tables reside

[JDBj-BOOTSTRAP SESSION]

This information is used to sign in for access to system tables. JDBj signs the user in by using the security server during the bootstrap process. If the sign-in information is not valid, then no access to the EnterpriseOne database is possible.

Note. This section is the same as the corresponding information specified in the [DB SYSTEM SETTINGS] section of PeopleSoft EnterpriseOne 8.9.

Parameter	Recommended Setting	Description
user=	Site-dependent variable	User name for logging in to the PeopleSoft EnterpriseOne security server.
password=	Site-dependent variable	Password for logging in to the PeopleSoft EnterpriseOne security server.
environment=	Site-dependent variable	The EnterpriseOne environment that contains the system tables.
role=	*ALL	Enter *ALL to access all roles.

[JDBj-BOOTSTRAP DATA SOURCE]

This section defines the data source where the OCM and some other system tables reside. JDBj uses this information at bootstrap time and at a later time to look up OCM entries on demand. If it is not valid, then no EnterpriseOne database access is possible.

Note. The information in this section should match the corresponding information specified in the [DB SYSTEM SETTINGS] section of the jde.ini file of the previous (before PeopleSoft EnterpriseOne 8.9) installation.

Parameter	Recommended Setting	Description
name=	Site-dependent variable	The name of the data source. This parameter is not critical for bootstrap connections, but it does show up in error messages and in the log file. (All servers)
databaseType=	I = AS/400 O = Oracle S = SQL Server W = UDB	The type of database used by the PeopleSoft EnterpriseOne system. (All servers)
server=	Site-dependent variable	Name of the server. (iSeries, SQL Server)
database=	Site-dependent variable	Name of the database. (Oracle, UDB)
serverPort=	Site-dependent variable	The port number of the server. (SQL Server)
physicalDatabase	Site-dependent variable	The physical database (used as the library qualifier for the iSeries). (iSeries, SQL Server)
Owner	Site-dependent variable	The database owner. (Oracle, SQL Server, UDB)
lob=	True False	Supports lob. (Oracle and iSeries)
Unicode=	True False	Performs Unicode conversion. (SQL Server)

[JDBj-SPEC DATA SOURCE]

This optional section defines the data source where the serialized specification tables reside. JDBj uses these parameters at bootstrap time and after to look up serialized specification objects on demand. If this section is not specified, then JDBj uses the OCM to find the serialized specification table. If it is not valid, no EnterpriseOne database access is possible.

Parameter	Recommended Setting	Description
name=	Site-dependent variable	The name of the data source. This parameter is not critical for bootstrap connections, but it shows up in error messages and in the log file. (All servers)
databaseType=	I = AS/400 O = Oracle S = SQL Server W = UDB	The type of database used by the PeopleSoft EnterpriseOne system. (All servers)
server=	Site dependent variable	Name of the server. (iSeries, SQL Server)
serverPort=	Site-dependent variable	The port number of the server. (SQL Server)
database=	Site-dependent variable	Name of the database. (Oracle, UDB)
physicalDatabase=	Site-dependent variable	The physical database (used as the library qualifier for the iSeries). (iSeries, SQL Server)
owner=	Site-dependent variable	The database owner. (Oracle, SQL Server, UDB)
lob=	True False	Supports lob. (Oracle and iSeries)
unicode=	True False	Performs Unicode conversion. (SQL Server)
user=	Site-dependent variable	User name for logging in to the PeopleSoft EnterpriseOne server.
password=	Site-dependent variable	Password for logging in to the PeopleSoft EnterpriseOne server.

General Sections

The rest of the web server jdbj.ini sections apply when accessing both PeopleSoft EnterpriseOne and standalone data:

Setting	Description
[JDBj-JDBC DRIVERS]	Defines JDBC drivers and JDBC specific settings.
[JDBj-ORACLE]	Defines the location of the tnsnames.ora file on the web server.
[JDBj-LOGS]	Enables JDBC tracing from the JDBC drivers.
[JDBj-CONNECTION POOL]	Currently, these settings are always used for pooling JDBC connections.
[JDBj-RUNTIME PROPERTIES]	These settings correspond to system runtime properties that are applicable to JDBj logical connections.

[ERPINTERACTIVITY]

Use the [ERPINTERACTIVITY] section to activate and configure the Interactive HTML settings.

Parameter	Recommended Setting	Description
InteractivityLevel=	LOW or HIGH	<p>Indicates the level of interactivity for the entire instance of JAS. Valid values are:</p> <ul style="list-style-type: none"> • LOW (default) • MEDIUM • HIGH <p>In low interactivity mode, whenever a critical or non-critical posting event happens, the entire page is sent to the web server and the user has to wait for the page to come back. When it does return, the page is repainted, which usually causes a flash on the browser. Critical events that force a post include Form, Row, View, Tools Exit, Toolbar button and Visual Assist clicks; switching Tab pages; expanding or collapsing tree nodes; parent and child tree drag-and-drops; and clicking static text controls. Other events can be marked in FDA to force a post.</p> <p>In medium interactivity mode, the data transfer and event execution occurs at the same points that low interactivity causes a full-page refresh. When these events happen, medium interactivity sends only the queued events and data to the server. Also, rather than doing an entire page refresh, it uses JavaScript and DHTML to repaint only the changed controls. The page flash does not occur in this mode.</p> <p>In high interactivity, events and data are transferred more frequently. It posts when critical events happen, and it posts whenever a change occurs on the form. For example, it posts whenever a control is exited and changed, or when grid columns are exited and changed. It sends only the queued events and data to the server. It does not do an entire page refresh; rather, it uses JavaScript and DHTML to repaint only the changed controls. The page flash does not occur in this mode.</p> <p>Note. A performance difference between high interactivity and medium interactivity is not perceptible because neither level causes a page refresh. The difference between these levels is in the amount and size of network traffic. High interactivity has more traffic, but it is small in size. Medium interactivity has less traffic but more data because it sends a batch of events at one time.</p>
MultipleBrowserEnabled=	FALSE	<p>This setting determines whether to launch multiple applications in separate browsers from Task Explorer and portal links. Valid values are:</p> <ul style="list-style-type: none"> • TRUE • FALSE (default)

Parameter	Recommended Setting	Description
MaxOpenBrowsers=	10	[1-n]. This parameter is the maximum number of open browsers that a user can have at any time. When this limit is reached, the system does <i>not</i> open the new browser. Instead, it displays the list of current open browsers and asks the user to close one before a new one can be opened.
DBFetchLimitBeforeWarning=	500	The default value is 500. The maximum number of records retrieved from a Query / Find before a warning is issued. This warning allows the user to modify the query so that it does not retrieve so many records. The web server displays a warning for every 500 records. For example, if you do a Find and the query retrieves 1000 records, you receive a warning. After you click OK, the web server displays a second warning for the second set of 500 records.

[JDBj-JDBC DRIVERS]

These values are used to specify the JDBC drivers that are used by the web server to access database types. In previous software releases, setting Oracle and iSeries drivers was not necessary because they were defaults for the web server. PeopleSoft EnterpriseOne does not assume any default drivers in order to avoid JAS classpath exceptions. The web server loads only the drivers you specify in this section:

Parameter	Recommended Setting	Description
Oracle=	oracle.jdbc.driver.OracleDriver	This driver is used for Oracle databases.
SQLSERVER=	com.microsoft.jdbc.sqlserver. SQLServerDriver	This driver is used for the Microsoft JDBC drivers that are used with SQL Server 2000.
AS400=	com.ibm.as400.access.AS400JDBCdriver	This driver is used for DB2 UDB for the iSeries.
UDB=	com.ibm.db2.jdbc.app.DB2Driver	This driver is used for DB2 UDB for Windows.

[JDBj-ORACLE]

This section defines the location of the tnsnames.ora file on the web server. This path is only required for data connections to an Oracle database.

Parameter	Recommended Setting	Description
tns=	Site-dependent variable	<p>Specifies the location of the Oracle tnsnames.ora file. This entry can be left blank if you are not using Oracle. You must un-comment this statement if you are using an Oracle database.</p> <p>The default value is:</p> <p>D:\Oracle\Ora9\ network\ADMIN\tnsnames.ora</p> <p>The value Ora9 identifies the version of Oracle that you are using. This value changes if you install a different version of Oracle.</p>

[JDBj-LOGS]

This section enables JDBC tracing from the JDBC drivers:

Parameter	Recommended Setting	Description
jdbcTrace=	false	This setting can enable JDBC tracing from the JDBC drivers. It is typically used only for debugging. Enabling JDBC tracing in a production environment negatively affects performance.

[JDBj-CONNECTION POOL]

The following settings are used for pooling JDBC connections:

Parameter	Recommended Setting	Description
jdbcPooling=	False	JDBC pooling is not currently supported, so even if this setting is enabled, pooling is still done by JDBj.
MaxConnection=	50	The maximum number of connections to a data source. Connection requests beyond this number are queued on the next available connection.
MinConnection=	0	The minimum number of connections to a data source. When closing old connections, this number remains in the pool, regardless of use.
PoolGrowth=	5	The number of connections that the system creates when a request for a connection cannot be satisfied with the current allocation.
InitialConnection=	5	The number of connections to create upon pool creation.
connectionTimeout	1800000	<p>The time (in milliseconds) before an inactive connection cache is removed from the pool.</p> <p>Before PeopleSoft EnterpriseOne 8.9, this setting was the <i>Connection</i> parameter in the [cache] section.</p>

Parameter	Recommended Setting	Description
CleanPoolInterval=	300000	<p>Specifies how often the pool cleaner is set to clean data sources that have a validation string.</p> <p>Note. The values specified for these keys are in milliseconds. For example, 60000 ms equals 1 minute.</p> <p>The validation string is in the form:</p> <p>ValidationString_x=<statement></p> <p>where x is I, 4, or R for DB2/400, S for SQL Server, O for Oracle</p> <p>and statement is a SQL statement that any user can execute.</p> <p>For example:</p> <p>ValidationString_I=Select * from QSYS2.SYSCOLUMNS WHERE I=2</p> <p>ValidationString_S=Select @@connections</p> <p>ValidationString_O=Select sysdate from dual</p>
maxSize	50	Maximum number of JDBC-prepared statements cached on each JDBC connection.
cachePurgeSize	5	Number of JDBC statements purged from a JDBC connection if the maxSize limit is reached.

[JDBj-RUNTIME PROPERTIES]

The settings in this section correspond to system runtime properties that are applicable to JDBj logical connections.

Note. In each case, the listed values are the default values. The template default entries are commented out. Remove the pound sign (#) when changing these values.

Parameter	Recommended Setting	Description
dataCacheEntrySizeThreshold=	500	<p>Sets the maximum row size for a single entry in the data cache. If a potential entry exceeds this threshold, then it is not cached. A value of -1 indicates that all of the eligible entries should be cached.</p> <p>Valid values are -1 or greater.</p>
dataCacheEntryThreshold=	100	<p>Sets the maximum entry size for the data cache. If the data cache exceeds this size, then the least recently used entries are removed to make room for the new entry. A value of -1 indicates no maximum.</p>

Parameter	Recommended Setting	Description
forceSingleDataSource=	False	<p>Indicates whether JDBC should force operations involving multiple database objects to run against a single data source. If this value is true, JDBC only resolves the physical data source for the first database object involved in an operation. If this value is false, JDBC resolves physical data sources for all of the database objects and throws an exception if a single operation spans multiple data sources. Valid values are:</p> <ul style="list-style-type: none"> • True • False
resultSetTimeout=	60000	<p>Time (in milliseconds) before a result set times out if it has not had any operations.</p> <p>PeopleSoft recommends the default setting.</p> <p>Valid values are -1 or greater.</p> <p>Before PeopleSoft EnterpriseOne 8.9, this setting was the ResultSet parameter in the [cache] section.</p>
retryInterval=	0	<p>Sets the interval (in milliseconds) to wait before retrying <i>idempotent</i> database operations. The value -1 means not to retry; 0 means to retry immediately.</p> <p>Valid values are -1 or greater.</p>
retryMaximum=	5	<p>Sets the number of times to retry <i>idempotent</i> database operations. The value -1 means to retry indefinitely.</p> <p>Valid values are -1 or greater.</p>
ocmCachePurge=	3600000	<p>Sets the number of milliseconds after which inactive OCM cache entries are purged.</p> <p>0 means to never purge OCM cache entries.</p>
personalSpecVersions=	False	<p>Indicates if a user's personal version can be read. This information is enforced during a read, and not enforced during a specification generation. If set to True, the personal version is returned; if no personal version exists, the public version is returned. If the property is set to False, then the personal version is not read and the public version is the default. Valid values are:</p> <ul style="list-style-type: none"> • True • False

Parameter	Recommended Setting	Description
securityCachePurge=	3600000	<p>Time (in milliseconds) before inactive service cache entries are purged. 0 means to never purge service cache entries.</p> <p>We recommend using the default values.</p> <p>Valid values are 0 or greater</p> <p>Before PeopleSoft EnterpriseOne 8.9, this setting was theSecurity parameter in the [cache] section.</p>
serviceCachePurge=	3600000	<p>Time (in milliseconds) before inactive service cache entries are purged. 0 means to never purge service cache entries.</p> <p>Valid values are 0 or greater</p> <p>Before PeopleSoft EnterpriseOne 8.9, this setting was theUDCInfo parameter in the [cache] section.</p>
specCachePurge=	3600000	<p>Time (in milliseconds) before inactive specification cache entries are purged. 0 means to never purge specification cache entries.</p> <p>Valid values are 0 or greater.</p> <p>Before PeopleSoft EnterpriseOne 8.9, this setting was theViewTable parameter in the [cache] section.</p>
specConsistencyCheck=	minimal	<p>The level of specification consistency checking. Set this property to a higher level to improve exception messages relating to specification inconsistency problems. Because it can degrade performance, set this property to a lower level when it is not needed. Valid values are:</p> <ul style="list-style-type: none"> • Full • Minimal • None
transactionIsolation=	default	<p>Sets the isolation level for transactions. Valid values are:</p> <ul style="list-style-type: none"> • Default • None • Read uncommitted • Read committed • Repeatable read • Serializable

Parameter	Recommended Setting	Description
transactionTimeout=	120000	<p>Time (in milliseconds) before a transaction timeout. A transaction times out if it has not had any operations for the specified period of time. If this timeout is set to -1, then the transaction timeout feature is disabled. (This action currently only happens when JDBj is run as part of a JAS transaction.)</p> <p>Valid values are -1 or greater.</p>
triggerAutoFetch=	none	<p>Indicates whether JDBj should automatically fetch rows to be changed to pass them to EnterpriseOne triggers. This action is needed for certain triggers to work properly. Valid values are:</p> <ul style="list-style-type: none"> • None • Single • All
updatableResultSetTimeout=	-1	<p>Time (in milliseconds) before an updatable result set times out if no operations have occurred. A value of -1 indicates that updatable result sets should have the same value as RESULT_SET_TIMEOUT.</p> <p>Valid values are -1 or greater.</p>
usageExecutionThreshold=	20000	<p>Maximum time (in milliseconds) for a single database operation to execute. If a single database operation takes longer than this threshold, then the statement and time are logged as part of usage tracking.</p> <p>Valid values are 0 or greater.</p>
usageFetchSizeThreshold=	500	<p>Expected maximum fetch size, in rows, for a single fetch to return. If a single fetch returns more than this threshold, then the actual fetch size is logged as part of usage tracking. A value of -1 indicates that any fetch size is valid.</p> <p>Valid values are -1 or greater.</p>
usageResultSetOpenThreshold=	60000	<p>Maximum time (in milliseconds) for a result set to remain open. If a result set is open longer than this threshold, then the result set and time are logged as part of usage tracking. When this setting is reached, the system does not automatically close the result set. An open threshold value of -1 for a usage result set indicates that no such usage tracking will occur.</p> <p>Valid values are -1 or greater.</p>

Parameter	Recommended Setting	Description
usageTracking=	false	Enables or disables usage tracking. This setting provides additional tracking and logging during testing. Usage tracking does incur a performance penalty, so it should be disabled for production code. Valid values: <ul style="list-style-type: none"> • True • False
usageTrackingOutput=	log	Specifies the destination of usage tracking output. Valid values are: <ul style="list-style-type: none"> • Log • Exception
usageTransactionActiveThreshold=	120000	Valid values are -1 or greater.

[LOGIN]

This section is used for setting login and Local Director options.

Parameter	Recommended Setting	Description
PassKey=	Site-dependent variable	Alphanumeric override for the key that is used to encrypt cookies.
externalhost=	machine:port	Used for building fully qualified URLs for a resource's browser request.
DisplayEnvironment=	Administrator preference	Environment display rule if a default environment is set with DefaultEnvironment. <ul style="list-style-type: none"> • Show: User can override the default environment at sign-in. • Hidden: User cannot see the environment box at sign-in. • ReadOnly: User cannot modify the environment setting at sign-in. UseDefault: The user can select different environments at sign-in, but the system overrides any other user choice and signs in to the default environment anyway.
DisablePasswordAboutToExpire	TRUE	Override that suppresses the <i>password about to expire</i> notification.

[TRANSACTIONS]

This section is used to set configuration settings to customize transaction processing within JAS:

Parameter	Recommended Setting	Description
ReapInterval=	5	Interval, in minutes, of how often the Transaction Reaper should check for abandoned transactions. Valid value is an integer from 1 to n. Default is 5 minutes.
MaxAge=	10	Maximum age, in minutes, of a transaction. Transactions older than this number are rolled back by the Transaction Reaper. Valid value is an integer from 1 to n. Default is 10 minutes.

[WEB GUI]

This section is used to configure the web GUI interface:

Parameter	Recommended Setting	Description
bandwidth=	narrow wide (default)	This setting is used to configure the GUI interface to account for networks with low bandwidth. By default, the web server uses tab decoration on all EnterpriseOne forms displayed in HTML. Tab decoration shows tabs with rounded corners, but it requires more bandwidth to display this format. Setting the bandwidth to narrow disables tab decoration and uses less bandwidth to display tabs. Using this setting, tabs displayed on HTML forms look like a rectangular box. Setting the bandwidth to wide enables tab decoration. This setting is optional. If it is not set, web decoration is wide by default.

Glossary of PeopleSoft Terms

absence entitlement	This element defines rules for granting paid time off for valid absences, such as sick time, vacation, and maternity leave. An absence entitlement element defines the entitlement amount, frequency, and entitlement period.
absence take	This element defines the conditions that must be met before a payee is entitled to take paid time off.
academic career	In PeopleSoft Enterprise Campus Solutions, all course work that a student undertakes at an academic institution and that is grouped in a single student record. For example, a university that has an undergraduate school, a graduate school, and various professional schools might define several academic careers—an undergraduate career, a graduate career, and separate careers for each professional school (law school, medical school, dental school, and so on).
academic institution	In PeopleSoft Enterprise Campus Solutions, an entity (such as a university or college) that is independent of other similar entities and that has its own set of rules and business processes.
academic organization	In PeopleSoft Enterprise Campus Solutions, an entity that is part of the administrative structure within an academic institution. At the lowest level, an academic organization might be an academic department. At the highest level, an academic organization can represent a division.
academic plan	In PeopleSoft Enterprise Campus Solutions, an area of study—such as a major, minor, or specialization—that exists within an academic program or academic career.
academic program	In PeopleSoft Enterprise Campus Solutions, the entity to which a student applies and is admitted and from which the student graduates.
accounting class	In PeopleSoft Enterprise Performance Management, the accounting class defines how a resource is treated for generally accepted accounting practices. The Inventory class indicates whether a resource becomes part of a balance sheet account, such as inventory or fixed assets, while the Non-inventory class indicates that the resource is treated as an expense of the period during which it occurs.
accounting date	The accounting date indicates when a transaction is recognized, as opposed to the date the transaction actually occurred. The accounting date and transaction date can be the same. The accounting date determines the period in the general ledger to which the transaction is to be posted. You can only select an accounting date that falls within an open period in the ledger to which you are posting. The accounting date for an item is normally the invoice date.
accounting split	The accounting split method indicates how expenses are allocated or divided among one or more sets of accounting ChartFields.
accumulator	You use an accumulator to store cumulative values of defined items as they are processed. You can accumulate a single value over time or multiple values over time. For example, an accumulator could consist of all voluntary deductions, or all company deductions, enabling you to accumulate amounts. It allows total flexibility for time periods and values accumulated.
action reason	The reason an employee's job or employment information is updated. The action reason is entered in two parts: a personnel action, such as a promotion, termination, or change from one pay group to another—and a reason for that action. Action reasons are used by PeopleSoft Human Resources, PeopleSoft Benefits Administration,

	PeopleSoft Stock Administration, and the COBRA Administration feature of the Base Benefits business process.
action template	In PeopleSoft Receivables, outlines a set of escalating actions that the system or user performs based on the period of time that a customer or item has been in an action plan for a specific condition.
activity	<p>In PeopleSoft Enterprise Learning Management, an instance of a catalog item (sometimes called a class) that is available for enrollment. The activity defines such things as the costs that are associated with the offering, enrollment limits and deadlines, and waitlisting capacities.</p> <p>In PeopleSoft Enterprise Performance Management, the work of an organization and the aggregation of actions that are used for activity-based costing.</p> <p>In PeopleSoft Project Costing, the unit of work that provides a further breakdown of projects—usually into specific tasks.</p> <p>In PeopleSoft Workflow, a specific transaction that you might need to perform in a business process. Because it consists of the steps that are used to perform a transaction, it is also known as a step map.</p>
address usage	In PeopleSoft Enterprise Campus Solutions, a grouping of address types defining the order in which the address types are used. For example, you might define an address usage code to process addresses in the following order: billing address, dormitory address, home address, and then work address.
adjustment calendar	In PeopleSoft Enterprise Campus Solutions, the adjustment calendar controls how a particular charge is adjusted on a student's account when the student drops classes or withdraws from a term. The charge adjustment is based on how much time has elapsed from a predetermined date, and it is determined as a percentage of the original charge amount.
administrative function	In PeopleSoft Enterprise Campus Solutions, a particular functional area that processes checklists, communication, and comments. The administrative function identifies which variable data is added to a person's checklist or communication record when a specific checklist code, communication category, or comment is assigned to the student. This key data enables you to trace that checklist, communication, or comment back to a specific processing event in a functional area.
admit type	In PeopleSoft Enterprise Campus Solutions, a designation used to distinguish first-year applications from transfer applications.
agreement	In PeopleSoft eSettlements, provides a way to group and specify processing options, such as payment terms, pay from a bank, and notifications by a buyer and supplier location combination.
allocation rule	In PeopleSoft Enterprise Incentive Management, an expression within compensation plans that enables the system to assign transactions to nodes and participants. During transaction allocation, the allocation engine traverses the compensation structure from the current node to the root node, checking each node for plans that contain allocation rules.
alternate account	A feature in PeopleSoft General Ledger that enables you to create a statutory chart of accounts and enter statutory account transactions at the detail transaction level, as required for recording and reporting by some national governments.
analysis database	In PeopleSoft Enterprise Campus Solutions, database tables that store large amounts of student information that may not appear in standard report formats. The analysis database tables contain keys for all objects in a report that an application program can use to reference other student-record objects that are not contained in the printed report. For instance, the analysis database contains data on courses that are considered for satisfying a requirement but that are rejected. It also contains information on

	courses captured by global limits. An analysis database is used in PeopleSoft Enterprise Academic Advisement.
AR specialist	Abbreviation for <i>receivables specialist</i> . In PeopleSoft Receivables, an individual in who tracks and resolves deductions and disputed items.
arbitration plan	In PeopleSoft Enterprise Pricer, defines how price rules are to be applied to the base price when the transaction is priced.
assessment rule	In PeopleSoft Receivables, a user-defined rule that the system uses to evaluate the condition of a customer's account or of individual items to determine whether to generate a follow-up action.
asset class	An asset group used for reporting purposes. It can be used in conjunction with the asset category to refine asset classification.
attribute/value pair	In PeopleSoft Directory Interface, relates the data that makes up an entry in the directory information tree.
audience	In PeopleSoft Enterprise Campus Solutions, a segment of the database that relates to an initiative, or a membership organization that is based on constituent attributes rather than a dues-paying structure. Examples of audiences include the Class of '65 and Undergraduate Arts & Sciences.
authentication server	A server that is set up to verify users of the system.
base time period	In PeopleSoft Business Planning, the lowest level time period in a calendar.
benchmark job	In PeopleSoft Workforce Analytics, a benchmark job is a job code for which there is corresponding salary survey data from published, third-party sources.
billing career	In PeopleSoft Enterprise Campus Solutions, the one career under which other careers are grouped for billing purposes if a student is active simultaneously in multiple careers.
bio bit or bio brief	In PeopleSoft Enterprise Campus Solutions, a report that summarizes information stored in the system about a particular constituent. You can generate standard or specialized reports.
book	In PeopleSoft Asset Management, used for storing financial and tax information, such as costs, depreciation attributes, and retirement information on assets.
branch	A tree node that rolls up to nodes above it in the hierarchy, as defined in PeopleSoft Tree Manager.
budgetary account only	An account used by the system only and not by users; this type of account does not accept transactions. You can only budget with this account. Formerly called "system-maintained account."
budget check	In commitment control, the processing of source transactions against control budget ledgers, to see if they pass, fail, or pass with a warning.
budget control	In commitment control, budget control ensures that commitments and expenditures don't exceed budgets. It enables you to track transactions against corresponding budgets and terminate a document's cycle if the defined budget conditions are not met. For example, you can prevent a purchase order from being dispatched to a vendor if there are insufficient funds in the related budget to support it.
budget period	The interval of time (such as 12 months or 4 quarters) into which a period is divided for budgetary and reporting purposes. The ChartField allows maximum flexibility to define operational accounting time periods without restriction to only one calendar.

business event	<p>In PeopleSoft Receivables, defines the processing characteristics for the Receivable Update process for a draft activity.</p> <p>In PeopleSoft Sales Incentive Management, an original business transaction or activity that may justify the creation of a PeopleSoft Enterprise Incentive Management event (a sale, for example).</p>
business unit	A corporation or a subset of a corporation that is independent with regard to one or more operational or accounting functions.
buyer	In PeopleSoft eSettlements, an organization (or business unit, as opposed to an individual) that transacts with suppliers (vendors) within the system. A buyer creates payments for purchases that are made in the system.
campus	In PeopleSoft Enterprise Campus Solutions, an entity that is usually associated with a distinct physical administrative unit, that belongs to a single academic institution, that uses a unique course catalog, and that produces a common transcript for students within the same academic career.
catalog item	In PeopleSoft Enterprise Learning Management, a specific topic that a learner can study and have tracked. For example, "Introduction to Microsoft Word." A catalog item contains general information about the topic and includes a course code, description, categorization, keywords, and delivery methods. A catalog item can have one or more learning activities.
catalog map	In PeopleSoft Catalog Management, translates values from the catalog source data to the format of the company's catalog.
catalog partner	In PeopleSoft Catalog Management, shares responsibility with the enterprise catalog manager for maintaining catalog content.
categorization	Associates partner offerings with catalog offerings and groups them into enterprise catalog categories.
category	In PeopleSoft Enterprise Campus Solutions, a broad grouping to which specific comments or communications (contexts) are assigned. Category codes are also linked to 3C access groups so that you can assign data-entry or view-only privileges across functions.
channel	In PeopleSoft MultiChannel Framework, email, chat, voice (computer telephone integration [CTI]), or a generic event.
ChartField	A field that stores a chart of accounts, resources, and so on, depending on the PeopleSoft application. ChartField values represent individual account numbers, department codes, and so forth.
ChartField balancing	You can require specific ChartFields to match up (balance) on the debit and the credit side of a transaction.
ChartField combination edit	The process of editing journal lines for valid ChartField combinations based on user-defined rules.
ChartKey	One or more fields that uniquely identify each row in a table. Some tables contain only one field as the key, while others require a combination.
checkbook	In PeopleSoft Promotions Management, enables you to view financial data (such as planned, incurred, and actual amounts) that is related to funds and trade promotions.
checklist code	In PeopleSoft Enterprise Campus Solutions, a code that represents a list of planned or completed action items that can be assigned to a staff member, volunteer, or unit. Checklists enable you to view all action assignments on one page.

class	<p>In PeopleSoft Enterprise Campus Solutions, a specific offering of a course component within an academic term.</p> <p>See also <i>course</i>.</p>
Class ChartField	<p>A ChartField value that identifies a unique appropriation budget key when you combine it with a fund, department ID, and program code, as well as a budget period. Formerly called <i>sub-classification</i>.</p>
clearance	<p>In PeopleSoft Enterprise Campus Solutions, the period of time during which a constituent in PeopleSoft Contributor Relations is approved for involvement in an initiative or an action. Clearances are used to prevent development officers from making multiple requests to a constituent during the same time period.</p>
clone	<p>In PeopleCode, to make a unique copy. In contrast, to <i>copy</i> may mean making a new reference to an object, so if the underlying object is changed, both the copy and the original change.</p>
cohort	<p>In PeopleSoft Enterprise Campus Solutions, the highest level of the three-level classification structure that you define for enrollment management. You can define a cohort level, link it to other levels, and set enrollment target numbers for it.</p> <p>See also <i>population</i> and <i>division</i>.</p>
collection	<p>To make a set of documents available for searching in Verity, you must first create at least one collection. A collection is set of directories and files that allow search application users to use the Verity search engine to quickly find and display source documents that match search criteria. A collection is a set of statistics and pointers to the source documents, stored in a proprietary format on a file server. Because a collection can only store information for a single location, PeopleSoft maintains a set of collections (one per language code) for each search index object.</p>
collection rule	<p>In PeopleSoft Receivables, a user-defined rule that defines actions to take for a customer based on both the amount and the number of days past due for outstanding balances.</p>
comm key	<p>See <i>communication key</i>.</p>
communication key	<p>In PeopleSoft Enterprise Campus Solutions, a single code for entering a combination of communication category, communication context, communication method, communication direction, and standard letter code. Communication keys (also called <i>comm keys</i> or <i>speed keys</i>) can be created for background processes as well as for specific users.</p>
compensation object	<p>In PeopleSoft Enterprise Incentive Management, a node within a compensation structure. Compensation objects are the building blocks that make up a compensation structure's hierarchical representation.</p>
compensation structure	<p>In PeopleSoft Enterprise Incentive Management, a hierarchical relationship of compensation objects that represents the compensation-related relationship between the objects.</p>
condition	<p>In PeopleSoft Receivables, occurs when there is a change of status for a customer's account, such as reaching a credit limit or exceeding a user-defined balance due.</p>
configuration parameter catalog	<p>Used to configure an external system with PeopleSoft. For example, a configuration parameter catalog might set up configuration and communication parameters for an external server.</p>
configuration plan	<p>In PeopleSoft Enterprise Incentive Management, configuration plans hold allocation information for common variables (not incentive rules) and are attached to a node without a participant. Configuration plans are not processed by transactions.</p>

constituents	In PeopleSoft Enterprise Campus Solutions, friends, alumni, organizations, foundations, or other entities affiliated with the institution, and about which the institution maintains information. The constituent types delivered with PeopleSoft Enterprise Contributor Relations Solutions are based on those defined by the Council for the Advancement and Support of Education (CASE).
content reference	Content references are pointers to content registered in the portal registry. These are typically either URLs or iScripts. Content references fall into three categories: target content, templates, and template pagelets.
context	<p>In PeopleCode, determines which buffer fields can be contextually referenced and which is the current row of data on each scroll level when a PeopleCode program is running.</p> <p>In PeopleSoft Enterprise Campus Solutions, a specific instance of a comment or communication. One or more contexts are assigned to a category, which you link to 3C access groups so that you can assign data-entry or view-only privileges across functions.</p> <p>In PeopleSoft Enterprise Incentive Management, a mechanism that is used to determine the scope of a processing run. PeopleSoft Enterprise Incentive Management uses three types of context: plan, period, and run-level.</p>
control table	Stores information that controls the processing of an application. This type of processing might be consistent throughout an organization, or it might be used only by portions of the organization for more limited sharing of data.
cost profile	A combination of a receipt cost method, a cost flow, and a deplete cost method. A profile is associated with a cost book and determines how items in that book are valued, as well as how the material movement of the item is valued for the book.
cost row	A cost transaction and amount for a set of ChartFields.
course	<p>In PeopleSoft Enterprise Campus Solutions, a course that is offered by a school and that is typically described in a course catalog. A course has a standard syllabus and credit level; however, these may be modified at the class level. Courses can contain multiple components such as lecture, discussion, and lab.</p> <p>See also <i>class</i>.</p>
course share set	In PeopleSoft Enterprise Campus Solutions, a tag that defines a set of requirement groups that can share courses. Course share sets are used in PeopleSoft Enterprise Academic Advisement.
current learning	In PeopleSoft Enterprise Learning Management, a self-service repository for all of a learner's in-progress learning activities and programs.
data acquisition	In PeopleSoft Enterprise Incentive Management, the process during which raw business transactions are acquired from external source systems and fed into the operational data store (ODS).
data elements	<p>Data elements, at their simplest level, define a subset of data and the rules by which to group them.</p> <p>For Workforce Analytics, data elements are rules that tell the system what measures to retrieve about your workforce groups.</p>
dataset	A data grouping that enables role-based filtering and distribution of data. You can limit the range and quantity of data that is displayed for a user by associating dataset rules with user roles. The result of dataset rules is a set of data that is appropriate for the user's roles.
delivery method	In PeopleSoft Enterprise Learning Management, identifies the primary type of delivery method in which a particular learning activity is offered. Also provides

default values for the learning activity, such as cost and language. This is primarily used to help learners search the catalog for the type of delivery from which they learn best. Because PeopleSoft Enterprise Learning Management is a blended learning system, it does not enforce the delivery method.

In PeopleSoft Supply Chain Management, identifies the method by which goods are shipped to their destinations (such as truck, air, rail, and so on). The delivery method is specified when creating shipment schedules.

delivery method type	In PeopleSoft Enterprise Learning Management, identifies how learning activities can be delivered—for example, through online learning, classroom instruction, seminars, books, and so forth—in an organization. The type determines whether the delivery method includes scheduled components.
directory information tree	In PeopleSoft Directory Interface, the representation of a directory's hierarchical structure.
division	In PeopleSoft Enterprise Campus Solutions, the lowest level of the three-level classification structure that you define in PeopleSoft Enterprise Recruiting and Admissions for enrollment management. You can define a division level, link it to other levels, and set enrollment target numbers for it. See also <i>population</i> and <i>cohort</i> .
document sequencing	A flexible method that sequentially numbers the financial transactions (for example, bills, purchase orders, invoices, and payments) in the system for statutory reporting and for tracking commercial transaction activity.
dynamic detail tree	A tree that takes its detail values—dynamic details—directly from a table in the database, rather than from a range of values that are entered by the user.
edit table	A table in the database that has its own record definition, such as the Department table. As fields are entered into a PeopleSoft application, they can be validated against an edit table to ensure data integrity throughout the system.
effective date	A method of dating information in PeopleSoft applications. You can predate information to add historical data to your system, or postdate information in order to enter it before it actually goes into effect. By using effective dates, you don't delete values; you enter a new value with a current effective date.
EIM ledger	Abbreviation for <i>Enterprise Incentive Management ledger</i> . In PeopleSoft Enterprise Incentive Management, an object to handle incremental result gathering within the scope of a participant. The ledger captures a result set with all of the appropriate traces to the data origin and to the processing steps of which it is a result.
elimination set	In PeopleSoft General Ledger, a related group of intercompany accounts that is processed during consolidations.
entry event	In PeopleSoft General Ledger, Receivables, Payables, Purchasing, and Billing, a business process that generates multiple debits and credits resulting from single transactions to produce standard, supplemental accounting entries.
equitization	In PeopleSoft General Ledger, a business process that enables parent companies to calculate the net income of subsidiaries on a monthly basis and adjust that amount to increase the investment amount and equity income amount before performing consolidations.
equity item limit	In PeopleSoft Enterprise Campus Solutions, the amounts of funds set by the institution to be awarded with discretionary or gift funds. The limit could be reduced by amounts equal to such things as expected family contribution (EFC) or parent contribution. Students are packaged by Equity Item Type Groups and Related Equity Item Types. This limit can be used to assure that similar student populations are packaged equally.

event	<p>A predefined point either in the Component Processor flow or in the program flow. As each point is encountered, the event activates each component, triggering any PeopleCode program that is associated with that component and that event. Examples of events are FieldChange, SavePreChange, and RowDelete.</p> <p>In PeopleSoft Human Resources, also refers to an incident that affects benefits eligibility.</p>
event propagation process	<p>In PeopleSoft Sales Incentive Management, a process that determines, through logic, the propagation of an original PeopleSoft Enterprise Incentive Management event and creates a derivative (duplicate) of the original event to be processed by other objects. Sales Incentive Management uses this mechanism to implement splits, roll-ups, and so on. Event propagation determines who receives the credit.</p>
exception	<p>In PeopleSoft Receivables, an item that either is a deduction or is in dispute.</p>
exclusive pricing	<p>In PeopleSoft Order Management, a type of arbitration plan that is associated with a price rule. Exclusive pricing is used to price sales order transactions.</p>
fact	<p>In PeopleSoft applications, facts are numeric data values from fields from a source database as well as an analytic application. A fact can be anything you want to measure your business by, for example, revenue, actual, budget data, or sales numbers. A fact is stored on a fact table.</p>
financial aid term	<p>In PeopleSoft Enterprise Campus Solutions, a combination of a period of time that the school determines as an instructional accounting period and an academic career. It is created and defined during the setup process. Only terms eligible for financial aid are set up for each financial aid career.</p>
forecast item	<p>A logical entity with a unique set of descriptive demand and forecast data that is used as the basis to forecast demand. You create forecast items for a wide range of uses, but they ultimately represent things that you buy, sell, or use in your organization and for which you require a predictable usage.</p>
fund	<p>In PeopleSoft Promotions Management, a budget that can be used to fund promotional activity. There are four funding methods: top down, fixed accrual, rolling accrual, and zero-based accrual.</p>
gap	<p>In PeopleSoft Enterprise Campus Solutions, an artificial figure that sets aside an amount of unmet financial aid need that is not funded with Title IV funds. A gap can be used to prevent fully funding any student to conserve funds, or it can be used to preserve unmet financial aid need so that institutional funds can be awarded.</p>
generic process type	<p>In PeopleSoft Process Scheduler, process types are identified by a generic process type. For example, the generic process type SQR includes all SQR process types, such as SQR process and SQR report.</p>
gift table	<p>In PeopleSoft Enterprise Campus Solutions, a table or so-called <i>donor pyramid</i> describing the number and size of gifts that you expect will be needed to successfully complete the campaign in PeopleSoft Contributor Relations. The gift table enables you to estimate the number of donors and prospects that you need at each gift level to reach the campaign goal.</p>
GL business unit	<p>Abbreviation for <i>general ledger business unit</i>. A unit in an organization that is an independent entity for accounting purposes. It maintains its own set of accounting books.</p> <p>See also <i>business unit</i>.</p>
GL entry template	<p>Abbreviation for <i>general ledger entry template</i>. In PeopleSoft Enterprise Campus Solutions, a template that defines how a particular item is sent to the general ledger. An item-type maps to the general ledger, and the GL entry template can involve multiple general ledger accounts. The entry to the general ledger is further controlled</p>

by high-level flags that control the summarization and the type of accounting—that is, accrual or cash.

GL Interface process

Abbreviation for *General Ledger Interface process*. In PeopleSoft Enterprise Campus Solutions, a process that is used to send transactions from PeopleSoft Enterprise Student Financials to the general ledger. Item types are mapped to specific general ledger accounts, enabling transactions to move to the general ledger when the GL Interface process is run.

group

In PeopleSoft Billing and Receivables, a posting entity that comprises one or more transactions (items, deposits, payments, transfers, matches, or write-offs).

In PeopleSoft Human Resources Management and Supply Chain Management, any set of records that are associated under a single name or variable to run calculations in PeopleSoft business processes. In PeopleSoft Time and Labor, for example, employees are placed in groups for time reporting purposes.

incentive object

In PeopleSoft Enterprise Incentive Management, the incentive-related objects that define and support the PeopleSoft Enterprise Incentive Management calculation process and results, such as plan templates, plans, results data, user interaction objects, and so on.

incentive rule

In PeopleSoft Sales Incentive Management, the commands that act on transactions and turn them into compensation. A rule is one part in the process of turning a transaction into compensation.

incur

In PeopleSoft Promotions Management, to become liable for a promotional payment. In other words, you owe that amount to a customer for promotional activities.

initiative

In PeopleSoft Enterprise Campus Solutions, the basis from which all advancement plans are executed. It is an organized effort targeting a specific constituency, and it can occur over a specified period of time with specific purposes and goals. An initiative can be a campaign, an event, an organized volunteer effort, a membership drive, or any other type of effort defined by the institution. Initiatives can be multipart, and they can be related to other initiatives. This enables you to track individual parts of an initiative, as well as entire initiatives.

inquiry access

In PeopleSoft Enterprise Campus Solutions, a type of security access that permits the user only to view data.

See also *update access*.

institution

In PeopleSoft Enterprise Campus Solutions, an entity (such as a university or college) that is independent of other similar entities and that has its own set of rules and business processes.

item

In PeopleSoft Inventory, a tangible commodity that is stored in a business unit (shipped from a warehouse).

In PeopleSoft Demand Planning, Inventory Policy Planning, and Supply Planning, a noninventory item that is designated as being used for planning purposes only. It can represent a family or group of inventory items. It can have a planning bill of material (BOM) or planning routing, and it can exist as a component on a planning BOM. A planning item cannot be specified on a production or engineering BOM or routing, and it cannot be used as a component in a production. The quantity on hand will never be maintained.

In PeopleSoft Receivables, an individual receivable. An item can be an invoice, a credit memo, a debit memo, a write-off, or an adjustment.

item shuffle

In PeopleSoft Enterprise Campus Solutions, a process that enables you to change a payment allocation without having to reverse the payment.

joint communication	In PeopleSoft Enterprise Campus Solutions, one letter that is addressed jointly to two people. For example, a letter might be addressed to both Mr. Sudhir Awat and Ms. Samantha Mortelli. A relationship must be established between the two individuals in the database, and at least one of the individuals must have an ID in the database.
keyword	In PeopleSoft Enterprise Campus Solutions, a term that you link to particular elements within PeopleSoft Student Financials, Financial Aid, and Contributor Relations. You can use keywords as search criteria that enable you to locate specific records in a search dialog box.
KPI	An abbreviation for <i>key performance indicator</i> . A high-level measurement of how well an organization is doing in achieving critical success factors. This defines the data value or calculation upon which an assessment is determined.
LDIF file	Abbreviation for <i>Lightweight Directory Access Protocol (LDAP) Data Interchange Format file</i> . Contains discrepancies between PeopleSoft data and directory data.
learner group	In PeopleSoft Enterprise Learning Management, a group of learners who are linked to the same learning environment. Members of the learner group can share the same attributes, such as the same department or job code. Learner groups are used to control access to and enrollment in learning activities and programs. They are also used to perform group enrollments and mass enrollments in the back office.
learning components	In PeopleSoft Enterprise Learning Management, the foundational building blocks of learning activities. PeopleSoft Enterprise Learning Management supports six basic types of learning components: web-based, session, webcast, test, survey, and assignment. One or more of these learning component types compose a single learning activity.
learning environment	In PeopleSoft Enterprise Learning Management, identifies a set of categories and catalog items that can be made available to learner groups. Also defines the default values that are assigned to the learning activities and programs that are created within a particular learning environment. Learning environments provide a way to partition the catalog so that learners see only those items that are relevant to them.
learning history	In PeopleSoft Enterprise Learning Management, a self-service repository for all of a learner's completed learning activities and programs.
ledger mapping	You use ledger mapping to relate expense data from general ledger accounts to resource objects. Multiple ledger line items can be mapped to one or more resource IDs. You can also use ledger mapping to map dollar amounts (referred to as <i>rates</i>) to business units. You can map the amounts in two different ways: an actual amount that represents actual costs of the accounting period, or a budgeted amount that can be used to calculate the capacity rates as well as budgeted model results. In PeopleSoft Enterprise Warehouse, you can map general ledger accounts to the EW Ledger table.
library section	In PeopleSoft Enterprise Incentive Management, a section that is defined in a plan (or template) and that is available for other plans to share. Changes to a library section are reflected in all plans that use it.
linked section	In PeopleSoft Enterprise Incentive Management, a section that is defined in a plan template but appears in a plan. Changes to linked sections propagate to plans using that section.
linked variable	In PeopleSoft Enterprise Incentive Management, a variable that is defined and maintained in a plan template and that also appears in a plan. Changes to linked variables propagate to plans using that variable.
LMS	Abbreviation for <i>learning management system</i> . In PeopleSoft Enterprise Campus Solutions, LMS is a PeopleSoft Student Records feature that provides a common set of interoperability standards that enable the sharing of instructional content and data between learning and administrative environments.

load	In PeopleSoft Inventory, identifies a group of goods that are shipped together. Load management is a feature of PeopleSoft Inventory that is used to track the weight, the volume, and the destination of a shipment.
local functionality	In PeopleSoft HRMS, the set of information that is available for a specific country. You can access this information when you click the appropriate country flag in the global window, or when you access it by a local country menu.
location	Locations enable you to indicate the different types of addresses—for a company, for example, one address to receive bills, another for shipping, a third for postal deliveries, and a separate street address. Each address has a different location number. The primary location—indicated by a <i>1</i> —is the address you use most often and may be different from the main address.
logistical task	In PeopleSoft Services Procurement, an administrative task that is related to hiring a service provider. Logistical tasks are linked to the service type on the work order so that different types of services can have different logistical tasks. Logistical tasks include both preapproval tasks (such as assigning a new badge or ordering a new laptop) and postapproval tasks (such as scheduling orientation or setting up the service provider email). The logistical tasks can be mandatory or optional. Mandatory preapproval tasks must be completed before the work order is approved. Mandatory postapproval tasks, on the other hand, must be completed before a work order is released to a service provider.
market template	In PeopleSoft Enterprise Incentive Management, additional functionality that is specific to a given market or industry and is built on top of a product category.
mass change	In PeopleSoft Enterprise Campus Solutions, mass change is a SQL generator that can be used to create specialized functionality. Using mass change, you can set up a series of Insert, Update, or Delete SQL statements to perform business functions that are specific to the institution. See also <i>3C engine</i> .
match group	In PeopleSoft Receivables, a group of receivables items and matching offset items. The system creates match groups by using user-defined matching criteria for selected field values.
MCF server	Abbreviation for <i>PeopleSoft MultiChannel Framework server</i> . Comprises the universal queue server and the MCF log server. Both processes are started when <i>MCF Servers</i> is selected in an application server domain configuration.
merchandising activity	In PeopleSoft Promotions Management, a specific discount type that is associated with a trade promotion (such as off-invoice, billback or rebate, or lump-sum payment) that defines the performance that is required to receive the discount. In the industry, you may know this as an offer, a discount, a merchandising event, an event, or a tactic.
meta-SQL	Meta-SQL constructs expand into platform-specific Structured Query Language (SQL) substrings. They are used in functions that pass SQL strings, such as in SQL objects, the SQLExec function, and PeopleSoft Application Engine programs.
metastring	Metastrings are special expressions included in SQL string literals. The metastrings, prefixed with a percent (%) symbol, are included directly in the string literals. They expand at run time into an appropriate substring for the current database platform.
multibook	In PeopleSoft General Ledger, multiple ledgers having multiple-base currencies that are defined for a business unit, with the option to post a single transaction to all base currencies (all ledgers) or to only one of those base currencies (ledgers).
multicurrency	The ability to process transactions in a currency other than the business unit's base currency.

national allowance	In PeopleSoft Promotions Management, a promotion at the corporate level that is funded by nondiscretionary dollars. In the industry, you may know this as a national promotion, a corporate promotion, or a corporate discount.
need	In PeopleSoft Enterprise Campus Solutions, the difference between the cost of attendance (COA) and the expected family contribution (EFC). It is the gap between the cost of attending the school and the student's resources. The financial aid package is based on the amount of financial need. The process of determining a student's need is called <i>need analysis</i> .
node-oriented tree	A tree that is based on a detail structure, but the detail values are not used.
pagelet	Each block of content on the home page is called a pagelet. These pagelets display summary information within a small rectangular area on the page. The pagelet provide users with a snapshot of their most relevant PeopleSoft and non-PeopleSoft content.
participant	In PeopleSoft Enterprise Incentive Management, participants are recipients of the incentive compensation calculation process.
participant object	Each participant object may be related to one or more compensation objects. See also <i>compensation object</i> .
partner	A company that supplies products or services that are resold or purchased by the enterprise.
pay cycle	In PeopleSoft Payables, a set of rules that define the criteria by which it should select scheduled payments for payment creation.
payment shuffle	In PeopleSoft Enterprise Campus Solutions, a process allowing payments that have been previously posted to a student's account to be automatically reapplied when a higher priority payment is posted or the payment allocation definition is changed.
pending item	In PeopleSoft Receivables, an individual receivable (such as an invoice, a credit memo, or a write-off) that has been entered in or created by the system, but hasn't been posted.
PeopleCode	PeopleCode is a proprietary language, executed by the PeopleSoft application processor. PeopleCode generates results based upon existing data or user actions. By using business interlink objects, external services are available to all PeopleSoft applications wherever PeopleCode can be executed.
PeopleCode event	An action that a user takes upon an object, usually a record field, that is referenced within a PeopleSoft page.
PeopleSoft Internet Architecture	The fundamental architecture on which PeopleSoft 8 applications are constructed, consisting of a relational database management system (RDBMS), an application server, a web server, and a browser.
performance measurement	In PeopleSoft Enterprise Incentive Management, a variable used to store data (similar to an aggregator, but without a predefined formula) within the scope of an incentive plan. Performance measures are associated with a plan calendar, territory, and participant. Performance measurements are used for quota calculation and reporting.
period context	In PeopleSoft Enterprise Incentive Management, because a participant typically uses the same compensation plan for multiple periods, the period context associates a plan context with a specific calendar period and fiscal year. The period context references the associated plan context, thus forming a chain. Each plan context has a corresponding set of period contexts.
person of interest	A person about whom the organization maintains information but who is not part of the workforce.

personal portfolio	In PeopleSoft Enterprise Campus Solutions, the user-accessible menu item that contains an individual's name, address, telephone number, and other personal information.
plan	In PeopleSoft Sales Incentive Management, a collection of allocation rules, variables, steps, sections, and incentive rules that instruct the PeopleSoft Enterprise Incentive Management engine in how to process transactions.
plan context	In PeopleSoft Enterprise Incentive Management, correlates a participant with the compensation plan and node to which the participant is assigned, enabling the PeopleSoft Enterprise Incentive Management system to find anything that is associated with the node and that is required to perform compensation processing. Each participant, node, and plan combination represents a unique plan context—if three participants are on a compensation structure, each has a different plan context. Configuration plans are identified by plan contexts and are associated with the participants that refer to them.
plan template	In PeopleSoft Enterprise Incentive Management, the base from which a plan is created. A plan template contains common sections and variables that are inherited by all plans that are created from the template. A template may contain steps and sections that are not visible in the plan definition.
planned learning	In PeopleSoft Enterprise Learning Management, a self-service repository for all of a learner's planned learning activities and programs.
planning instance	In PeopleSoft Supply Planning, a set of data (business units, items, supplies, and demands) constituting the inputs and outputs of a supply plan.
population	In PeopleSoft Enterprise Campus Solutions, the middle level of the three-level classification structure that you define in PeopleSoft Enterprise Recruiting and Admissions for enrollment management. You can define a population level, link it to other levels, and set enrollment target numbers for it. See also <i>division</i> and <i>cohort</i> .
portal registry	In PeopleSoft applications, the portal registry is a tree-like structure in which content references are organized, classified, and registered. It is a central repository that defines both the structure and content of a portal through a hierarchical, tree-like structure of folders useful for organizing and securing content references.
price list	In PeopleSoft Enterprise Pricer, enables you to select products and conditions for which the price list applies to a transaction. During a transaction, the system either determines the product price based on the predefined search hierarchy for the transaction or uses the product's lowest price on any associated, active price lists. This price is used as the basis for any further discounts and surcharges.
price rule	In PeopleSoft Enterprise Pricer, defines the conditions that must be met for adjustments to be applied to the base price. Multiple rules can apply when conditions of each rule are met.
price rule condition	In PeopleSoft Enterprise Pricer, selects the price-by fields, the values for the price-by fields, and the operator that determines how the price-by fields are related to the transaction.
price rule key	In PeopleSoft Enterprise Pricer, defines the fields that are available to define price rule conditions (which are used to match a transaction) on the price rule.
primacy number	In PeopleSoft Enterprise Campus Solutions, a number that the system uses to prioritize financial aid applications when students are enrolled in multiple academic careers and academic programs at the same time. The Consolidate Academic Statistics process uses the primacy number indicated for both the career and program at the institutional level to determine a student's primary career and program. The system also uses the

	number to determine the primary student attribute value that is used when you extract data to report on cohorts. The lowest number takes precedence.
primary name type	In PeopleSoft Enterprise Campus Solutions, the name type that is used to link the name stored at the highest level within the system to the lower-level set of names that an individual provides.
process category	In PeopleSoft Process Scheduler, processes that are grouped for server load balancing and prioritization.
process group	In PeopleSoft Financials, a group of application processes (performed in a defined order) that users can initiate in real time, directly from a transaction entry page.
process definition	Process definitions define each run request.
process instance	A unique number that identifies each process request. This value is automatically incremented and assigned to each requested process when the process is submitted to run.
process job	You can link process definitions into a job request and process each request serially or in parallel. You can also initiate subsequent processes based on the return code from each prior request.
process request	A single run request, such as a Structured Query Report (SQR), a COBOL or Application Engine program, or a Crystal report that you run through PeopleSoft Process Scheduler.
process run control	A PeopleTools variable used to retain PeopleSoft Process Scheduler values needed at runtime for all requests that reference a run control ID. Do not confuse these with application run controls, which may be defined with the same run control ID, but only contain information specific to a given application process request.
product category	In PeopleSoft Enterprise Incentive Management, indicates an application in the Enterprise Incentive Management suite of products. Each transaction in the PeopleSoft Enterprise Incentive Management system is associated with a product category.
programs	In PeopleSoft Enterprise Learning Management, a high-level grouping that guides the learner along a specific learning path through sections of catalog items. PeopleSoft Enterprise Learning Systems provides two types of programs—curricula and certifications.
progress log	In PeopleSoft Services Procurement, tracks deliverable-based projects. This is similar to the time sheet in function and process. The service provider contact uses the progress log to record and submit progress on deliverables. The progress can be logged by the activity that is performed, by the percentage of work that is completed, or by the completion of milestone activities that are defined for the project.
project transaction	In PeopleSoft Project Costing, an individual transaction line that represents a cost, time, budget, or other transaction row.
promotion	In PeopleSoft Promotions Management, a trade promotion, which is typically funded from trade dollars and used by consumer products manufacturers to increase sales volume.
prospects	In PeopleSoft Enterprise Campus Solutions, students who are interested in applying to the institution. In PeopleSoft Enterprise Contributor Relations, individuals and organizations that are most likely to make substantial financial commitments or other types of commitments to the institution.
publishing	In PeopleSoft Enterprise Incentive Management, a stage in processing that makes incentive-related results available to participants.

rating components	In PeopleSoft Enterprise Campus Solutions, variables used with the Equation Editor to retrieve specified populations.
record group	A set of logically and functionally related control tables and views. Record groups help enable TableSet sharing, which eliminates redundant data entry. Record groups ensure that TableSet sharing is applied consistently across all related tables and views.
record input VAT flag	Abbreviation for <i>record input value-added tax flag</i> . Within PeopleSoft Purchasing, Payables, and General Ledger, this flag indicates that you are recording input VAT on the transaction. This flag, in conjunction with the record output VAT flag, is used to determine the accounting entries created for a transaction and to determine how a transaction is reported on the VAT return. For all cases within Purchasing and Payables where VAT information is tracked on a transaction, this flag is set to Yes. This flag is not used in PeopleSoft Order Management, Billing, or Receivables, where it is assumed that you are always recording only output VAT, or in PeopleSoft Expenses, where it is assumed that you are always recording only input VAT.
record output VAT flag	Abbreviation for <i>record output value-added tax flag</i> . See <i>record input VAT flag</i> .
recname	The name of a record that is used to determine the associated field to match a value or set of values.
recognition	In PeopleSoft Enterprise Campus Solutions, the recognition type indicates whether the PeopleSoft Enterprise Contributor Relations donor is the primary donor of a commitment or shares the credit for a donation. Primary donors receive hard credit that must total 100 percent. Donors that share the credit are given soft credit. Institutions can also define other share recognition-type values such as memo credit or vehicle credit.
reference data	In PeopleSoft Sales Incentive Management, system objects that represent the sales organization, such as territories, participants, products, customers, channels, and so on.
reference object	In PeopleSoft Enterprise Incentive Management, this dimension-type object further defines the business. Reference objects can have their own hierarchy (for example, product tree, customer tree, industry tree, and geography tree).
reference transaction	In commitment control, a reference transaction is a source transaction that is referenced by a higher-level (and usually later) source transaction, in order to automatically reverse all or part of the referenced transaction's budget-checked amount. This avoids duplicate postings during the sequential entry of the transaction at different commitment levels. For example, the amount of an encumbrance transaction (such as a purchase order) will, when checked and recorded against a budget, cause the system to concurrently reference and relieve all or part of the amount of a corresponding pre-encumbrance transaction, such as a purchase requisition.
regional sourcing	In PeopleSoft Purchasing, provides the infrastructure to maintain, display, and select an appropriate vendor and vendor pricing structure that is based on a regional sourcing model where the multiple ship to locations are grouped. Sourcing may occur at a level higher than the ship to location.
relationship object	In PeopleSoft Enterprise Incentive Management, these objects further define a compensation structure to resolve transactions by establishing associations between compensation objects and business objects.
remote data source data	Data that is extracted from a separate database and migrated into the local database.
REN server	Abbreviation for <i>real-time event notification server</i> in PeopleSoft MultiChannel Framework.
requester	In PeopleSoft eSettlements, an individual who requests goods or services and whose ID appears on the various procurement pages that reference purchase orders.

reversal indicator	In PeopleSoft Enterprise Campus Solutions, an indicator that denotes when a particular payment has been reversed, usually because of insufficient funds.
role	Describes how people fit into PeopleSoft Workflow. A role is a class of users who perform the same type of work, such as clerks or managers. Your business rules typically specify what user role needs to do an activity.
role user	A PeopleSoft Workflow user. A person's role user ID serves much the same purpose as a user ID does in other parts of the system. PeopleSoft Workflow uses role user IDs to determine how to route worklist items to users (through an email address, for example) and to track the roles that users play in the workflow. Role users do not need PeopleSoft user IDs.
roll up	In a tree, to roll up is to total sums based on the information hierarchy.
run control	A run control is a type of online page that is used to begin a process, such as the batch processing of a payroll run. Run control pages generally start a program that manipulates data.
run control ID	A unique ID to associate each user with his or her own run control table entries.
run-level context	In PeopleSoft Enterprise Incentive Management, associates a particular run (and batch ID) with a period context and plan context. Every plan context that participates in a run has a separate run-level context. Because a run cannot span periods, only one run-level context is associated with each plan context.
search query	You use this set of objects to pass a query string and operators to the search engine. The search index returns a set of matching results with keys to the source documents.
search/match	In PeopleSoft Enterprise Campus Solutions and PeopleSoft Enterprise Human Resources Management Solutions, a feature that enables you to search for and identify duplicate records in the database.
seasonal address	In PeopleSoft Enterprise Campus Solutions, an address that recurs for the same length of time at the same time of year each year until adjusted or deleted.
section	In PeopleSoft Enterprise Incentive Management, a collection of incentive rules that operate on transactions of a specific type. Sections enable plans to be segmented to process logical events in different sections.
security event	In commitment control, security events trigger security authorization checking, such as budget entries, transfers, and adjustments; exception overrides and notifications; and inquiries.
serial genealogy	In PeopleSoft Manufacturing, the ability to track the composition of a specific, serial-controlled item.
serial in production	In PeopleSoft Manufacturing, enables the tracing of serial information for manufactured items. This is maintained in the Item Master record.
service impact	In PeopleSoft Enterprise Campus Solutions, the resulting action triggered by a service indicator. For example, a service indicator that reflects nonpayment of account balances by a student might result in a service impact that prohibits registration for classes.
service indicator	In PeopleSoft Enterprise Campus Solutions, indicates services that may be either withheld or provided to an individual. Negative service indicators indicate holds that prevent the individual from receiving specified services, such as check-cashing privileges or registration for classes. Positive service indicators designate special services that are provided to the individual, such as front-of-line service or special services for disabled students.

session	<p>In PeopleSoft Enterprise Campus Solutions, time elements that subdivide a term into multiple time periods during which classes are offered. In PeopleSoft Contributor Relations, a session is the means of validating gift, pledge, membership, or adjustment data entry. It controls access to the data entered by a specific user ID. Sessions are balanced, queued, and then posted to the institution's financial system. Sessions must be posted to enter a matching gift or pledge payment, to make an adjustment, or to process giving clubs or acknowledgements.</p> <p>In PeopleSoft Enterprise Learning Management, a single meeting day of an activity (that is, the period of time between start and finish times within a day). The session stores the specific date, location, meeting time, and instructor. Sessions are used for scheduled training.</p>
session template	In PeopleSoft Enterprise Learning Management, enables you to set up common activity characteristics that may be reused while scheduling a PeopleSoft Enterprise Learning Management activity—characteristics such as days of the week, start and end times, facility and room assignments, instructors, and equipment. A session pattern template can be attached to an activity that is being scheduled. Attaching a template to an activity causes all of the default template information to populate the activity session pattern.
setup relationship	In PeopleSoft Enterprise Incentive Management, a relationship object type that associates a configuration plan with any structure node.
share driver expression	In PeopleSoft Business Planning, a named planning method similar to a driver expression, but which you can set up globally for shared use within a single planning application or to be shared between multiple planning applications through PeopleSoft Enterprise Warehouse.
single signon	With single signon, users can, after being authenticated by a PeopleSoft application server, access a second PeopleSoft application server without entering a user ID or password.
source key process	In PeopleSoft Enterprise Campus Solutions, a process that relates a particular transaction to the source of the charge or financial aid. On selected pages, you can drill down into particular charges.
source transaction	In commitment control, any transaction generated in a PeopleSoft or third-party application that is integrated with commitment control and which can be checked against commitment control budgets. For example, a pre-encumbrance, encumbrance, expenditure, recognized revenue, or collected revenue transaction.
speed key	See <i>communication key</i> .
SpeedChart	A user-defined shorthand key that designates several ChartKeys to be used for voucher entry. Percentages can optionally be related to each ChartKey in a SpeedChart definition.
SpeedType	A code representing a combination of ChartField values. SpeedTypes simplify the entry of ChartFields commonly used together.
staging	A method of consolidating selected partner offerings with the offerings from the enterprise's other partners.
standard letter code	In PeopleSoft Enterprise Campus Solutions, a standard letter code used to identify each letter template available for use in mail merge functions. Every letter generated in the system must have a standard letter code identification.
statutory account	Account required by a regulatory authority for recording and reporting financial results. In PeopleSoft, this is equivalent to the Alternate Account (ALTACCT) ChartField.

step	In PeopleSoft Sales Incentive Management, a collection of sections in a plan. Each step corresponds to a step in the job run.
storage level	In PeopleSoft Inventory, identifies the level of a material storage location. Material storage locations are made up of a business unit, a storage area, and a storage level. You can set up to four storage levels.
subcustomer qualifier	A value that groups customers into a division for which you can generate detailed history, aging, events, and profiles.
Summary ChartField	You use summary ChartFields to create summary ledgers that roll up detail amounts based on specific detail values or on selected tree nodes. When detail values are summarized using tree nodes, summary ChartFields must be used in the summary ledger data record to accommodate the maximum length of a node name (20 characters).
summary ledger	An accounting feature used primarily in allocations, inquiries, and PS/nVision reporting to store combined account balances from detail ledgers. Summary ledgers increase speed and efficiency of reporting by eliminating the need to summarize detail ledger balances each time a report is requested. Instead, detail balances are summarized in a background process according to user-specified criteria and stored on summary ledgers. The summary ledgers are then accessed directly for reporting.
summary time period	In PeopleSoft Business Planning, any time period (other than a base time period) that is an aggregate of other time periods, including other summary time periods and base time periods, such as quarter and year total.
summary tree	A tree used to roll up accounts for each type of report in summary ledgers. Summary trees enable you to define trees on trees. In a summary tree, the detail values are really nodes on a detail tree or another summary tree (known as the <i>basis</i> tree). A summary tree structure specifies the details on which the summary trees are to be built.
syndicate	To distribute a production version of the enterprise catalog to partners.
system function	In PeopleSoft Receivables, an activity that defines how the system generates accounting entries for the general ledger.
TableSet	A means of sharing similar sets of values in control tables, where the actual data values are different but the structure of the tables is the same.
TableSet sharing	Shared data that is stored in many tables that are based on the same TableSets. Tables that use TableSet sharing contain the SETID field as an additional key or unique identifier.
target currency	The value of the entry currency or currencies converted to a single currency for budget viewing and inquiry purposes.
tax authority	In PeopleSoft Enterprise Campus Solutions, a user-defined element that combines a description and percentage of a tax with an account type, an item type, and a service impact.
template	A template is HTML code associated with a web page. It defines the layout of the page and also where to get HTML for each part of the page. In PeopleSoft, you use templates to build a page by combining HTML from a number of sources. For a PeopleSoft portal, all templates must be registered in the portal registry, and each content reference must be assigned a template.
territory	In PeopleSoft Sales Incentive Management, hierarchical relationships of business objects, including regions, products, customers, industries, and participants.
3C engine	Abbreviation for <i>Communications, Checklists, and Comments engine</i> . In PeopleSoft Enterprise Campus Solutions, the 3C engine enables you to automate business processes that involve additions, deletions, and updates to communications, checklists,

and comments. You define events and triggers to engage the engine, which runs the mass change and processes the 3C records (for individuals or organizations) immediately and automatically from within business processes.

3C group	Abbreviation for <i>Communications, Checklists, and Comments group</i> . In PeopleSoft Enterprise Campus Solutions, a method of assigning or restricting access privileges. A 3C group enables you to group specific communication categories, checklist codes, and comment categories. You can then assign the group inquiry-only access or update access, as appropriate.
TimeSpan	A relative period, such as year-to-date or current period, that can be used in various PeopleSoft General Ledger functions and reports when a rolling time frame, rather than a specific date, is required. TimeSpans can also be used with flexible formulas in PeopleSoft Projects.
trace usage	In PeopleSoft Manufacturing, enables the control of which components will be traced during the manufacturing process. Serial- and lot-controlled components can be traced. This is maintained in the Item Master record.
transaction allocation	In PeopleSoft Enterprise Incentive Management, the process of identifying the owner of a transaction. When a raw transaction from a batch is allocated to a plan context, the transaction is duplicated in the PeopleSoft Enterprise Incentive Management transaction tables.
transaction state	In PeopleSoft Enterprise Incentive Management, a value assigned by an incentive rule to a transaction. Transaction states enable sections to process only transactions that are at a specific stage in system processing. After being successfully processed, transactions may be promoted to the next transaction state and “picked up” by a different section for further processing.
Translate table	A system edit table that stores codes and translate values for the miscellaneous fields in the database that do not warrant individual edit tables of their own.
tree	The graphical hierarchy in PeopleSoft systems that displays the relationship between all accounting units (for example, corporate divisions, projects, reporting groups, account numbers) and determines roll-up hierarchies.
tuition lock	In PeopleSoft Enterprise Campus Solutions, a feature in the Tuition Calculation process that enables you to specify a point in a term after which students are charged a minimum (or <i>locked</i>) fee amount. Students are charged the locked fee amount even if they later drop classes and take less than the normal load level for that tuition charge.
unclaimed transaction	In PeopleSoft Enterprise Incentive Management, a transaction that is not claimed by a node or participant after the allocation process has completed, usually due to missing or incomplete data. Unclaimed transactions may be manually assigned to the appropriate node or participant by a compensation administrator.
universal navigation header	Every PeopleSoft portal includes the universal navigation header, intended to appear at the top of every page as long as the user is signed on to the portal. In addition to providing access to the standard navigation buttons (like Home, Favorites, and signoff) the universal navigation header can also display a welcome message for each user.
update access	In PeopleSoft Enterprise Campus Solutions, a type of security access that permits the user to edit and update data. See also <i>inquiry access</i> .
user interaction object	In PeopleSoft Sales Incentive Management, used to define the reporting components and reports that a participant can access in his or her context. All Sales Incentive Management user interface objects and reports are registered as user interaction objects. User interaction objects can be linked to a compensation structure node through a compensation relationship object (individually or as groups).

variable	In PeopleSoft Sales Incentive Management, the intermediate results of calculations. Variables hold the calculation results and are then inputs to other calculations. Variables can be plan variables that persist beyond the run of an engine or local variables that exist only during the processing of a section.
VAT exception	Abbreviation for <i>value-added tax exception</i> . A temporary or permanent exemption from paying VAT that is granted to an organization. This terms refers to both VAT exoneration and VAT suspension.
VAT exempt	Abbreviation for <i>value-added tax exempt</i> . Describes goods and services that are not subject to VAT. Organizations that supply exempt goods or services are unable to recover the related input VAT. This is also referred to as exempt without recovery.
VAT exoneration	Abbreviation for <i>value-added tax exoneration</i> . An organization that has been granted a permanent exemption from paying VAT due to the nature of that organization.
VAT suspension	Abbreviation for <i>value-added tax suspension</i> . An organization that has been granted a temporary exemption from paying VAT.
warehouse	A PeopleSoft data warehouse that consists of predefined ETL maps, data warehouse tools, and DataMart definitions.
work order	In PeopleSoft Services Procurement, enables an enterprise to create resource-based and deliverable-based transactions that specify the basic terms and conditions for hiring a specific service provider. When a service provider is hired, the service provider logs time or progress against the work order.
worker	A person who is part of the workforce; an employee or a contingent worker.
workset	A group of people and organizations that are linked together as a set. You can use worksets to simultaneously retrieve the data for a group of people and organizations and work with the information on a single page.
worksheet	A way of presenting data through a PeopleSoft Business Analysis Modeler interface that enables users to do in-depth analysis using pivoting tables, charts, notes, and history information.
worklist	The automated to-do list that PeopleSoft Workflow creates. From the worklist, you can directly access the pages you need to perform the next action, and then return to the worklist for another item.
XML schema	An XML definition that standardizes the representation of application messages, component interfaces, or business interlinks.
yield by operation	In PeopleSoft Manufacturing, the ability to plan the loss of a manufactured item on an operation-by-operation basis.
zero-rated VAT	Abbreviation for <i>zero-rated value-added tax</i> . A VAT transaction with a VAT code that has a tax percent of zero. Used to track taxable VAT activity where no actual VAT amount is charged. Organizations that supply zero-rated goods and services can still recover the related input VAT. This is also referred to as exempt with recovery.

Index

A

- action security
 - changing 118
 - See Also* security types
 - removing 118
 - reviewing 116
 - setting up 116
- activity rules
 - object transfer 27
 - overview 9
 - project status 26
- additional documentation xxiv
- Address Book data security
 - creating permission list definitions 145
 - creating permission list relationships 146
 - setting up permission list definitions 144
 - setting up permission list relationships 146
 - understanding 143
- Address Book Master table (F0101) 82
- allowed (user) actions
 - configuring 13
 - setting up 13
- Anonymous User Access Table (F00926) 78
- application fundamentals xxiii
- application security
 - adding 111
 - changing 112
 - managing 109
 - removing 113
 - setting up exclusive application security 133
 - understanding 110
- assigning environments to user and role profiles 85
- attachments, adding 277
- authenticate tokens
 - properties 209
 - understanding 209
- authentication mode, enabling for LDAP 194
- auxiliary security servers 179

B

- barcode font, setting up for EnterpriseOne 54
- batch applications, overriding specifications with Scheduler 259
- batch jobs, scheduling a recurring job 253
- batch processes
 - creating profiles 80
 - creating user profiles with 86
 - for vocabulary overrides 245
- business unit security
 - overview 149
 - setting up 149
 - setting up UDC sharing 150, 151
- business views, configuring for text search indices 284

C

- cached security information 105
- Collaborative Portal EnterpriseOne Menu, configuring for single signon 223
 - See Also* single signon
- column security
 - deleting 123
 - setting up 121, 123
- comments, submitting xxviii
- common elements xxviii
- contact information xxviii
- control records, using with the Scheduler server 264
- CRM portlets, configuring for single signon 224
- cross-references xxvii
- CSS portlet, configuring for single signon 223
- Customer Connection website xxiv

D

- data dictionary
 - administration 3
 - updating display decimals 4
- data sources
 - managing for user security 174
 - naming conventions 297
 - revising for user security 175

- data, viewing in Universal Table Browser 289
- daylight savings rules 268
- default printer, defining 48
- default projects
 - managing non-Object Librarian objects 8
 - See Also* OMW
 - overview 8
- default security settings for PeopleSoft Solution Explorer 186
- dispatch functions, using with the Scheduler server 264
- display decimals, updating 4
- displaying roles at sign-in 97
- Distributed Next Number Update UBE (R0002D1) 240
- distributed next numbers
 - configuring for mobile clients 235
 - enabling distributed next numbers for mobile clients 236
 - mapping the EnterpriseOne user ID to the Distributed Next Numbers application 238
 - scheduling updates to distributed next numbers applications 240
 - setting up by application 238
 - setting up by system for mobile clients 237
- documentation
 - printed xxiv
 - related xxiv
 - updates xxiv

E

- encryption, of passwords 156
- enterprise server mappings, mapping from LDAP to EnterpriseOne 197
 - See Also* LDAP-enabled EnterpriseOne
- enterprise servers
 - changing the jde.ini file for security 178
 - iSeries server jde.ini settings, *See* iseries server jde.ini settings
 - server jde.ini settings for WebSphere 377
 - UNIX jde.ini file settings 342
 - UNIX/Linux server Jde.ini settings 342
 - See Also* UNIX/Linux server jde.ini settings
 - Windows server jde.ini settings 359

- See Also* Windows server jde.ini file settings

- ENTERPRISE TIMEZONE
 - ADJUSTMENT setting, configuring for single signon 225
- EnterpriseOne Links portlet, configuring for single signon 224
- EnterpriseOne security, *See* security types environments
 - assigning to role and user profiles 80, 85
 - overriding the environment 257
- ESS portlet, configuring for single signon 223
- exclusive application security
 - adding 133
 - removing 134
 - setting up 133
- exit security
 - adding 131
 - changing 132
 - removing 132
 - setting up 130
- external calls security
 - adding 135
 - removing 136
 - revising 136
 - setting up 134

F

- F00092 table 78
- F00165 table 272, 275
- F00921 table 78
- F00922 table 78
- F00925 table 78
- F00926 table 78
- F0093 table 78
- F0094 table 78
- F00950 table 105
- F0101 table 82
- F98101 table 273, 280
- F986180 table 216
- F986181 table 216
- F986182 table 216
- F98MOQUE table 273
- F98OWSEC table 103
- flat file encoding
 - activating a flat file encoding record 295
 - adding 294

- flat file encoding record example 292
- understanding 291
- form security, securing users to a
 - form 115
- functions
 - configuring in OMW 20
 - configuring notification
 - subscriptions 31

G

- glossary 409

H

- holding jobs 61
- Hosted EnterpriseOne Portlet, configuring
 - for single signon 223

I

- image media objects 273
- imaging
 - files 271
 - setting up 275, 279
 - typical process flow for 280
 - understanding 272
- Imaging Constants (F98101) 273, 280
- individual users, adding 79
- INI file, locating on the iSeries, *See* jde.ini file
- integration, disabling SAR system
 - integration 20
- Intellisync Server, importing files for PIM
 - synchronization 233
- interactive vocabulary overrides, *See*
 - vocabulary overrides
- iSeries server jde.ini settings
 - [AS400] 319
 - [BSFN BUILD] 320
 - [DB SYSTEM SETTINGS] 322
 - [DEBUG] 325
 - ENTERPRISE TIMEZONE
 - ADJUSTMENT 326
 - [INSTALL] 326
 - [INTEROPERABILITY] 327
 - [JDEIPC] 327
 - [JDEITDRV] 328
 - [JDEMAIL] 328
 - [JDENET] 329
 - [JDENET_KERNEL_DEFx] 331
 - [LOCK MANAGER] 336

- [NETWORK QUEUE
 - SETTINGS] 337
- [SECURITY] 337
- [SVR] 339
- [TCENGINE] 339
- [UBE] 340
- [WORKFLOW] 341
- [WORLD ENVIRONMENT
 - MAP] 341
- [XML Dispatch] 342
- [XTS] 342

J

- jde.ini file
 - changing for user security 177
 - changing the timeout value 178
 - changing the workstation file for
 - security 177
 - enabling and disabling unified
 - logon 183
 - enabling LDAP authentication
 - mode 194
 - enterprise server 178
 - locating the file 302
 - parameters for roles 89
 - print settings for the workstation
 - jde.ini 43
 - See Also* printing considerations
 - server jde.ini settings for
 - WebSphere 377
 - See Also* server jde.ini settings for WebSphere
 - setting auxiliary security servers in the
 - server jde.ini 179
 - settings for single signon
 - configuring the ENTERPRISEONE
 - TIMEZONE ADJUSTMENT 225
 - modifying settings for a
 - pre-EnterpriseOne 8.11 release 220
 - sample node settings 220
 - understanding 301
- job expiration specifications,
 - overriding 257
- job launcher, activate or deactivate 266
- job monitor loops, using with the Scheduler
 - server 265
- job monitor, activate or deactivate 266
- job queues
 - adding 67
 - changing the status of 69

- copying 68
- managing 64
- overriding 66, 69
- revising 68
- jobs
 - changing launch status 262
 - changing printer 62
 - changing priority 62
 - defining resubmission time 258
 - holding and releasing jobs 61
 - overriding expiration specifications 257
 - overriding printer location 60
 - printing jobs 63
 - resetting the job schedule 263
 - reviewing all or local jobs 256
 - reviewing online 60
 - reviewing schedules 261
 - revising a scheduled job 255
 - scheduling a recurring job 253
 - scheduling jobs 250
 - setting the status manually 262
 - status and priority 60
 - terminating 61, 64
 - viewing job details 262
 - viewing job logs 60
 - working with job properties 256
 - working with server jobs 60
- JSR168 portlet, configuring for single signon 223

L

- language role descriptions 94, 101
- language specific media object attachments, adding 277
- launch loops, using with the Scheduler server 265
- LDAP
 - changing the configuration status 198
 - configuring mappings between LDAP and EnterpriseOne enterprise server 197
 - See Also* LDAP-enabled EnterpriseOne
 - configuring server settings 195
 - creating an LDAP configuration 194
 - default user profile settings 199
 - enabling authentication mode 194
 - implementing LDAP support in EnterpriseOne 191

- modifying LDAP default user profile settings 200
- modifying LDAP default user security settings 201
- modifying the default role relationship 200
- understanding 187, 188
- using LDAP Bulk Synchronization (R9200040)
 - example 206
- using LDAP over SSL 207
 - See Also* SSL
- using with single signon 226
- LDAP Bulk Synchronization report (R9200040) 206
- LDAP-enabled EnterpriseOne
 - Administration Password Revisions program changes 203
 - Scheduler program changes 203
 - Security Revisions program changes 202
 - User Default Revisions program changes 202
 - User Profile Revisions program changes 202
 - User Profile Self-Service program changes 203
 - User-Role Relationship Preferences program changes 203
- Library List Control (F0093) 78
- Library List Master File (F0094) 78
- Library User (F00092) 78
- line printers
 - designing reports to run on line printers 55
 - setting up 56
- Linux server jde.ini settings, *See* UNIX/Linux server jde.ini settings
- log files
 - location on server 52
 - setting default directory on server 52
- logging
 - controlling detail 21
 - logging failure
 - controlling development in event of 22
 - understanding the logging system 8
- logs
 - creating for your report 53
 - generating for reports 52

viewing logs for a job 63

M

media object queues
 adding 277
 defining queue location 278
 deleting 279
 setting up 277
 understanding 272
 Media Object Queues program
 (F98MOQUE) 273
 media objects
 enabling 276
 enabling media objects 282
 enabling PeopleSoft EnterpriseOne to
 use media objects 275
 for text search indices 284
 See Also text search indices
 image media objects 273
 language considerations for 273
 media object tables 273
 OLE media objects 273
 setting up imaging 279
 See Also imaging
 text items 272
 typical process flow for imaging 280
 URL media objects 273
 using standard processing 276
 working with media object queues 272
 Media Objects Storage (F00165) 272,
 275
 MMA Partners xxiv
 mobile clients
 distributed next numbers for 235
 enabling functionality 235
 setting up distributed next numbers by
 system 237
 multiple users, adding 79

N

naming conventions
 data sources 297
 package names 298
 path codes 297
 servers 299
 workstations 299
 Node Configuration Table (F986180) 216
 Node Lifetime Configuration Table
 (F986182) 216

nodes

default settings for single signon 215
 for single signon
 See Also single signon
 adding a node configuration 217
 adding a trusted node
 configuration 219
 changing the status of a node 217
 deleting a node configuration 218
 deleting trusted node
 configurations 219
 how nodes work in single signon 210
 revising a node configuration 217
 properties 210
 non-Object Librarian objects, *See* OMW
 notes xxvii
 notification subscriptions 9
 notifications, object action 9

O

object action notifications
 disabling 31
 See Also OMW
 enabling 31
 understanding 9
 Object Management Log Purge report
 (R98210B) 11
 Object Management Workbench (OMW)
 administration, *See* OMW
 object save locations, *See* OMW
 deleting 30
 modifying 30
 overview 9
 objects
 deleting save location 30
 enabling action notification 31
 modifying save location 30
 object transfer activity rules 27
 saving locations 9
 OLE media objects 273
 OLE objects 271
 OMW
 activity rules 9
 allowed (user) actions 13
 configuring 7
 configuring notification
 subscriptions 31
 configuring object save locations 29
 configuring OMW functions 20
 default projects 8

- development 22
- locating object logs 35
- locating project logs 38
- logging detail 21
- logging system 8
- managing non-Object Librarian
 - objects 8
- non-Object Librarian objects 8
- notification subscriptions 9
- object action notifications 9, 31
- object save location 30
- object save locations 9, 30
- object transfer activity rules 27
- printing logs 40
- project constants 8, 22
- project promotion life cycle 23
- project status 9
 - See Also* allowed actions
- project status activity rules 26
- projects 8
- SAR integration 20
- securing OMW applications 11
- user roles 11, 13
- viewing detail logs 39
- viewing project or object logs 35
- working with logs 34
- OMW Configuration System program (P98230) 11
- OMW Transfer Activity Rules Director program (P98231) 11

P

- P0092 program 202
- P0092SS program 203
- P00950 program 109
- P91300 program 203, 249
- P950411 application, *See* distributed next numbers
- P95921 program 203
- P98230 program 11
- P98231 program 11
- P986116 program 60
- P98OWSEC program 202
- packages, naming conventions 298
- paper type, deleting 50
- password encryption 156
- passwords
 - changing sign-in (administrators only) 173
 - encryption of 156

- path codes, naming conventions 297
- PDF files
 - location on server 52
 - setting default directory on server 52
- PeopleBooks
 - ordering xxiv
- PeopleCode, typographical
 - conventions xxvi
- PeopleSoft application fundamentals xxiii
- PeopleSoft Solution Explorer security
 - configuring 186
 - default settings 186
 - settings 185
 - understanding 185
- permission list
 - definitions 144
 - relationships 146
- PIM synchronization
 - exporting PIM user records 232
 - importing PIM synchronization files into Intellisync Server 233
 - setting the processing option 230
 - setting up users for 231
 - understanding 229
 - user defined codes 230
- Populate User Profiles report (R0092) 87
- portlets, configuring for single signon 222
- prerequisites xxiii
- printed documentation xxiv
- printers, setting up for iSeries 57
- printing
 - changing a printer 62
 - copying an existing printer 49
 - defining a default printer 48
 - deleting a paper type 50
 - deleting a printer 50
 - designing reports to run on line printers 55
 - determining logical printers attached to batch processes 51
 - jobs 63
 - modifying an existing printer 49
 - print-time characteristics 42
 - searching for incomplete records 51
 - searching for incorrect printer records 51
 - setting up a line printer 56
 - setting up EnterpriseOne to use a barcode font 54

- settings for the workstation jde.ini
 - file 43
 - understanding 41
 - viewing logs for a job 63
 - viewing reports online 63
 - working with the printers
 - application 43
- PrintQueue directory, location on
 - server 52
- processing option security
 - adding 125
 - removing 127
 - reviewing current settings 125
 - revising 126
- processing options, entering for
 - Scheduler 252
- project status activity rules, setting up 26
- projects
 - default projects 8
 - promotion life cycle for OMW 23
 - setting up constants 8, 22
- properties, viewing column
 - properties 290
- Purge Scheduled Jobs report, printing 269

Q

- queue management, job queues 64
- queues
 - job 64
 - media object 272

R

- read/write reports security
 - setting up 138
 - understanding 137
- related documentation xxiv
- remote printers, printing multiple copies on
 - the iSeries 57
- reports
 - adding values to report
 - interconnect 260
 - checking status 62
 - creating logs for your reports 53
 - designing for line printers 55
 - generating logs 52
 - printing 41
 - retrieving logs 52
 - running on the server 42
 - running on the workstation 42

- running Scheduler reports 268
- running the Security Analyzer by Data
 - Source (R98OWSECA) 180
- viewing online 63
- role profiles
 - assigning business preferences 86
 - assigning environments to 80, 85
 - copying 80
 - copying role profiles 85
 - creating using a batch process 80, 86
 - how role profiles make profiling
 - easier 77
- role relationships
 - creating 98
 - modifying the LDAP default role
 - relationships 200
 - revising 98
- role security
 - copying 139
 - copying a single security record 140
 - deleting security on the Work with
 - User/Role form 140
- roles
 - adding roles to a user 99
 - adding users to a role 100
 - administering roles 89
 - copying security 139
 - copying user roles 101
 - creating role-to-role relationships 98
 - defining 94
 - displaying roles at sign-in 97
 - migrating 91
 - removing data sources 176
 - revising language role descriptions 94, 101
 - revising role relationships 98
 - setting up user roles 88
 - workstation initialization file parameters
 - for roles 89
- row security
 - removing 121
 - setting up 119
- Row Security Revisions form 121

S

- SAR system
 - disabling SAR integration 20
- save locations, *See* OMW
 - deleting 30
 - modifying 30

- understanding 9
- Scheduled Jobs report, printing 269
- Scheduler
 - adding values to a report
 - interconnect 260
 - changing job launch status 262
 - control records 264
 - daylight savings rules 267
 - defining resubmission time 258
 - dispatch functions 264
 - entering processing options 252
 - job monitor loops 265
 - overriding batch application
 - specifications 259
 - overriding job expiration
 - specifications 257
 - overriding the environment 257
 - reports 269
 - resetting the job schedule 263
 - reviewing all jobs or local jobs 256
 - reviewing job schedules 261
 - reviewing the job schedule 260
 - revising a scheduled job 255
 - running Scheduler reports 268
 - scheduling a recurring job 253
 - scheduling jobs 250
 - setting job status manually 262
 - understanding 249
 - understanding the Scheduler server 263
 - using advanced scheduling options 256
 - viewing job details 262
 - working with job properties 256
- Scheduler program (P91300), changes to P91300 when LDAP is enabled 203
- Scheduler server
 - launch loops 265
 - modifying the sleep time 267
 - refreshing the settings 266
 - resetting 266
 - stopping or restarting 265
 - using 264
- scheduling jobs 250
- Secure Socket Layer (SSL), *See* SSL
- security 169
 - See Also* security types; user security
 - adding action security 117
 - adding exit security 131
 - adding to a tab 128
 - adding to an application 111
 - changing action security 118
 - changing exit security 132
 - changing for an application 112
 - changing tab security 129
 - configuring PeopleSoft Solution Explorer security 186
 - copying a single record for a user or role 140
 - copying for a user or role 139
 - deleting on the Row Security Revisions form 121
 - deleting user security 140
 - how PeopleSoft EnterpriseOne checks security 104
 - managing miscellaneous security 137
 - modifying enterprise server jde.ini security settings 178
 - See Also* jde.ini file
 - object-level security 106
 - process flow for sign-in security 157
 - removing action security 118
 - removing exit security 132
 - removing from a tab 129
 - removing from an application 113
 - removing from processing options 127
 - revising processing option security 126
 - securing a user or role all EnterpriseOne objects 112
 - securing OMW applications 11
 - securing users to a form 115
 - setting up action security 116
 - setting up column security 121
 - setting up exclusive application security 133
 - setting up exit security 130
 - setting up external call security 134
 - setting up processing option security 124
 - setting up row security 119
 - setting up sign-in security 156
 - sign-in security for web users 162
 - types, *See* security types
 - understanding cached information 105
 - understanding sign-in security 155
 - understanding Solution Explorer security 185
 - user roles 11
 - user security 174
 - See Also* managing data sources
- Security (F98OWSEC) 156

- Security Analyzer by Data Source Report (R98OWSECA)
 - running the report 181
 - understanding 180
- security history, reviewing 174
- Security Revisions program (P98OWSEC),
 - changes to P98OWSEC when LDAP is enabled 202
- security server communication error 178
- Security table (F98OWSEC) 103
- security tables
 - accessing 156
- security types
 - action 116
 - Address Book data 143
 - application 109
 - business unit 149
 - column 121
 - exclusive application 133
 - exit 130
 - external calls 134
 - processing option 124
 - read/write reports 137
 - row 119
 - tab 128
 - understanding 105
- Security Workbench (P00950) 109
- Security Workbench table (F00950) 105
- server jde.ini settings for WebSphere
 - [JDENET_KERNEL_DEF13] 377
 - [MQSI] 378
- server jde.ini, setting auxiliary security servers 179
- servers
 - naming conventions 299
 - running reports 42
 - understanding the Scheduler server 263
- services
 - for unified logon 184
 - removing for unified logon 184
- shortcuts, for media objects 272
- ShowUnifiedLogon setting 162
- sign-in passwords, changing 173
- sign-in security
 - for web users 162
 - process flow 157
 - requiring 174
 - revising 172
 - setting up 156
 - ShowUnifiedLogon setting 162
 - understanding 155
- single signon
 - adding a trusted node configuration 219
 - adding token lifetime configuration records 218
 - between Enterprise Portal and an EnterpriseOne application 212
 - between EnterpriseOne Collaborative Portal and an EnterpriseOne application 214
 - configuring between Enterprise Portal and EnterpriseOne 224
 - configuring for a pre-EnterpriseOne 8.11 release 219
 - configuring for Collaborative Portal 222
 - configuring nodes, *See* nodes
 - configuring tokenengen.ini settings for portlets 223
 - configuring without a security server 221
 - deleting token lifetime configuration records 218
 - for portlets 222
 - synchronizing user mappings between LDAP and EnterpriseOne while using LDAP authentication 226
 - understanding 209
 - See Also* authenticate tokens; nodes
 - understanding configurations 216
 - using authenticate token 209
 - using with LDAP 226
 - validating authenticate tokens 211
 - viewing user ID mapping when using LDAP 227
- SSL
 - using LDAP over SSL 207
 - using LDAP over SSL for iSeries 208
 - using LDAP over SSL for Windows and UNIX 207
- SSS portlet, configuring for single signon 223
- stop words, defining for text search indices 288
- subscriptions, notification 9
- subsystems
 - enabling 72
 - locating subsystems running on a server 73
 - logical sequence of events diagram 70

- stopping 74
- terminating 73, 74
- understanding EnterpriseOne
 - subsystems 70
- suggestions, submitting xxviii
- synonyms, defining for text search
 - indices 288

T

- tab security
 - adding 128
 - removing 129
 - revising 129
 - setting up 128
- tables
 - viewing column properties 290
 - viewing data in 289
- terms 409
- text items 272
- text search business view-data source pair,
 - adding 287
- text search indices
 - adding a text search business view-data
 - source pair 287
 - building 285
 - defining 283
 - defining languages for 285
 - defining media objects for 284
 - defining stop words for 288
 - defining topics for 288
 - designating data sources for business
 - views 284
 - properties for 285
 - understanding 283
- token lifetime configuration records
 - adding 218
 - deleting 218
- tokengen.ini, configuring settings for single
 - signon for portlets 223
- topics, defining for text search indices 288
- transaction security
 - revising 153
 - setting up 153
 - understanding 152
- Trusted Node Configuration Table
 - (F986181) 216
- trusted nodes
 - adding 219
 - deleting 219
- typographical conventions xxvi

U

- UDC groups, revising for UDC
 - sharing 152
- UDC sharing 149
 - revising UDC groups 152
 - setting up 150
- unified logon 155
 - enabling and disabling in the jde.ini
 - file 183
 - removing a service 184
 - setting up a service 184
 - understanding 183
- Universal Table Browser
 - overview 289
 - viewing column properties in a
 - table 290
 - viewing data in tables 289
- UNIX/Linux server jde.ini settings
 - [BSFN BUILD] 342
 - [CLUSTER] 344
 - [DB SYSTEM SETTINGS] 345
 - [DEBUG] 346
 - [INSTALL] 347
 - [INTEROPERABILITY] 348
 - [JDEIPC] 348
 - [JDEITDRV] 348
 - [JDEMAIL] 349
 - [JDENET] 349
 - [JDENET_KERNEL_DEFX] 351
 - [LOCK MANAGER] 355
 - [LREngine] 355
 - [NETWORK QUEUE
 - SETTINGS] 356
 - [SAMPLE_EVENT] 356
 - [SECURITY] 356
 - [SERVER ENVIRONMENT
 - MAP] 357
 - [SVR] 357
 - [WORKFLOW] 358
- URL media objects 273
- User Access Definition (F00925) 78
- User Default Revisions, changes to
 - User Default Revisions when LDAP is
 - enabled 202
- User Display Preferences (F00921) 78
- User Display Preferences Tag
 - (F00922) 78
- user ID and user-role search hierarchy in
 - the LDAP server 193

- User Profile Revision program (P0092) 78
- User Profile Revisions (P0092), changes to P0092 when LDAP is enabled 202
- User Profile Revisions program (P0092), processing options 82
- User Profile Self-Service (P0092SS), changes to P0092SS when LDAP is enabled 203
- user profiles
 - assigning business preferences 86
 - assigning environments to 80, 85
 - copying 80
 - copying user profiles 85
 - creating using a batch process 80, 86
 - default user profile settings for LDAP 199
 - reviewing LDAP default user profile settings 199
 - running the Populate User Profiles report (R0092) 87
 - tables used by the User Profiles Revision program 78
 - understanding 77
- user roles
 - configuring 13
 - securing 11
 - setting up 88
- user security
 - changing the jde.ini file 177
 - copying 139, 171
 - copying a single security record 140
 - creating 169
 - creating security 168
 - deleting 140
 - deleting security on the Work with User/Role form 140
 - managing data sources 174
 - removing data sources 176
 - revising 168
 - revising data sources 175
 - revising for all users 172
 - working with user security 167
- User Security program, processing options 165
- User-Role Relationship Preferences program (P95921), changes to P95921 when LDAP is enabled 203
- users
 - adding 78

- adding individual users 79
- adding multiple 79

V

- Verity, EnterpriseOne's text search engine 283
- visual cues xxvii
- vocabulary overrides
 - accessing from Object Management Workbench 243
 - accessing the Interactive Vocabulary Overrides form 243
 - accessing vocabulary overrides 242
 - creating a batch vocabulary override 245
 - creating an interactive vocabulary override 244
 - creating vocabulary overrides 241
 - overview 241
 - resetting 246
 - resetting all overrides in an application (interactive and batch) 247
 - reviewing vocabulary overrides 246

W

- warnings xxvii
- web server jas.ini settings
 - [CACHE] 381
 - [JAS PREFERENCE] 383
 - [JDENET] 383
 - [LOGS] 383
 - overview 379
 - [OWWEB] 384
 - [PORTALCONFIGURATION] 387
 - [SECURITY] 393
 - [SERVER COMPONENTS] 395
 - [SERVER] 394
- web server jdbj.ini settings
 - [ERPINTERACTIVITY] 399
 - general sections 399
 - [JDBj-BOOTSTRAP DATA SOURCE] 397
 - [JDBj-BOOTSTRAP SESSION] 396
 - [JDBj-CONNECTION POOL] 402
 - [JDBj-JDBC DRIVERS] 401
 - [JDBj-LOGS] 402
 - [JDBj-ORACLE] 401
 - [JDBj-RUNTIME PROPERTIES] 403
 - [JDBj-SPEC DATA SOURCE] 398

- [LOGIN] 407
- overview 395
- [TRANSACTIONS] 407
- [WEB GUI] 408
- Windows server jde.ini file settings
 - [BSFN BUILD] 360
 - [BSFN Builder] 361
 - [DB SYSTEM SETTINGS] 362
 - [DEBUG] - Intel Processor 363
 - [ENTERPRISE TIMEZONE ADJUSTMENT] 365
 - [INSTALL] 365
 - [INTEROPERABILITY] 366
 - [JDE_CG] 367
 - [JDEIPC] 367
 - [JDEITDRV] 368
 - [JDEMAIL] 369
 - [JDENET] 369
 - [LOCK MANAGER] 371
 - [LREngine] 372
 - [MQSI] 372
 - [NETWORK QUEUE SETTINGS] 373
 - [SAMLE_EVENT] 375
 - [SECURITY] 375
 - [SERVER ENVIRONMENT MAP] 376
 - [SVR] 376
 - [UBE] 359
- Work with Server Jobs form, checking report status 62
- Work with Servers program (P986116)
 - processing options 62
 - usage 59
- Work with User/Role form 140
- Work With User/Role Profiles form 83
- workflow status monitoring security
 - setting up 138
 - understanding 137
- workstation jde.ini settings
 - [ACTIVE DIRECTORY] 302
 - [DB SYSTEM SETTINGS - SECONDARY] 305
 - [DB SYSTEM SETTINGS] 302
 - [DEBUG] 306
 - [EVEREST] 307
 - [INSTALL] 307
 - [JDE_CG] 309
 - [JDEMAIL] 309
 - [JDENET] 310
 - [LOCK MANAGER] 311
 - [NETWORK QUEUE SETTINGS] 43, 312
 - [OBJECT LIBRARIAN] 312
 - [OFFLINE DB SYSTEM SETTINGS] 313
 - [SECURITY] 177, 315
 - [SVR] 315
 - [UBE] 317
 - [WORKFLOW] 319
- workstations
 - changing the jde.ini file for security 177
 - naming conventions 299
 - running reports on the workstation 42