PeopleSoft

EnterpriseOne System Administration 8.9 PeopleBook

September 2003

EnterpriseOne
System Administration 8.9 PeopleBook
SKU REL9ESy0309

Copyright© 2003 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

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.

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.

Table of Contents

Data Dictionary Administration

Just as a dictionary contains word definitions, the J.D. Edwards 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 ERP 9.0 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 your data dictionary administrator for each application area in your ERP 9.0 enterprise. Data dictionary administrators should be experienced with ERP 9.0 and have a comprehensive knowledge of their product area, such as financial 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 your enterprise server.

Data dictionary administrators should consider the following:

- If your setup is similar to the suggested setup in the *Typical Customer Configuration* section of the *Configurable Network Computing Implementation Guide*, 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 (P98DREP) to prevent unauthorized users from making data dictionary changes.
- If you are running a coexistence enterprise, you must create all of your data items in both WorldSoftware and ERP 9.0 because the two products cannot share the same data dictionary.

Before You Begin

- ❑ Ensure that you are familiar with the concepts in the *Data Dictionary* section of the *Development Tools Guide*. This section describes using the data dictionary and defining a data term.

Updating Display Decimals

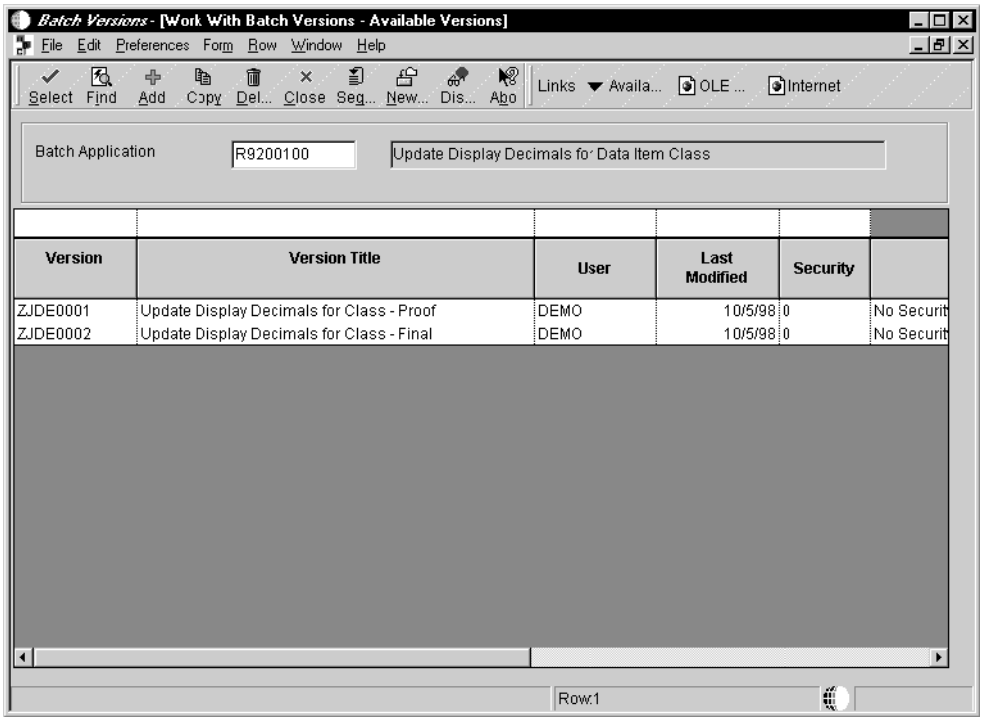
You can change the position of the display decimal for the quantity field class. Data items that belong to the QTYINV data item class come with the display decimal set at 0 (zero), but you can change the display decimal to any number up to 8. For example, if you change the display decimal to 4, instead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

Caution

You should change the display decimal value in a CRP environment before any live production data is entered. The reason is because ERP 9.0 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.

► To update display decimals

On the System Administration Tools menu (GH9011), choose Batch Versions (P98305).



1. On Work With Batch Versions – Available Versions, type 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

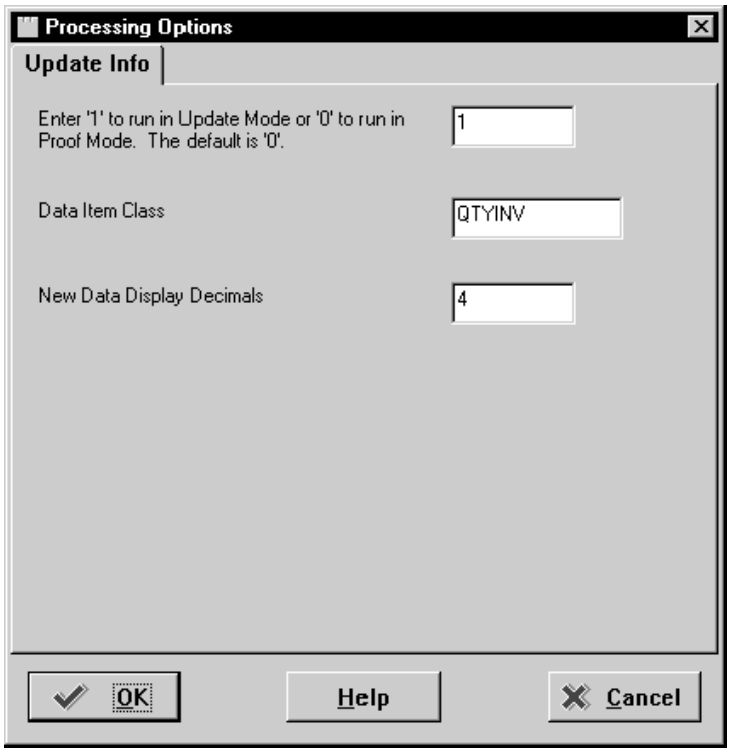
     The final version actually makes the changes.
3. On the Version Prompting form, click Data Selection and then click Submit.
4. On the Data Selection form, create the following statement:

   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 ERP 9.0. Also, if you modify which data items reside in the QTYINV data item class, you must research and test how the modifications affect ERP 9.0.

5. Click OK.

   If you changed the Data Selection statement, first click Update, and then click OK.



6. On Processing Options, complete the following 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 the following spec files:

   ```
   qlbltbl.ddb, qlbltbl.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.

Understanding Object Management Workbench Configuration

The Object Management Workbench (OMW) automates many of the object management tasks users performed manually in previous releases of 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 following optional features:

Option	Description
Constants	Enables you to set general constants pertaining to OMW projects.
SAR System Integration	Enables you to disable SAR system integration with OMW and, thus, ERP 9.0 development tools.
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, which sends a notification message when an action such as checkin or checkout is performed on an object.
Notification Setup	Enables developers to be notified, via subscription, when actions are performed on an object.
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 OMWfor the first time, the system creates a default project and tags it with your user ID. The default project is your personal project that you can use for development and research.

You can use default projects to do the following:

- 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.

Configuration Process Flow

The recommended process flow for using all of the Object Management Workbench Configuration tools follows. The first three steps 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.

Activity Rules

The following 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 APPL objects be transferred from the DV9 location to the PY9 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.

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, a detail log is created and attached to the major log record.

Project Constants

The Object Management Constants form enables an administrator to set the following 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.

Object Save Locations

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

Object Action Notifications

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

Notification Subscriptions

The notification system sends e-mail messages to users regarding changes to objects in the system, such as object checkin and checkout. The Notification Subscriptions form allows you to add, delete, and modify notification subscriptions, as well as to sort notification subscription records by criteria that you choose.

Application and User Role Security

You should secure the following applications using application security:

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

Securing User Roles

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

However, all users must be able to add the following 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 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

All configuration options are set up through the OMW Configuration System application (P98230). You choose the option that you want to configure by clicking the button that corresponds to the desired option.

► To choose a configuration option

From the Cross Application Development Tools menu (GH902), choose Object Management Configuration (P98230).

1. If necessary, click the General tab to display function options.
2. Click one of the following 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

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.

Configuring 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.

The following table shows the allowed user actions that J.D. Edwards 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 - Cancelled 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
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
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 following 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
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

The following 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)

► To modify a user role

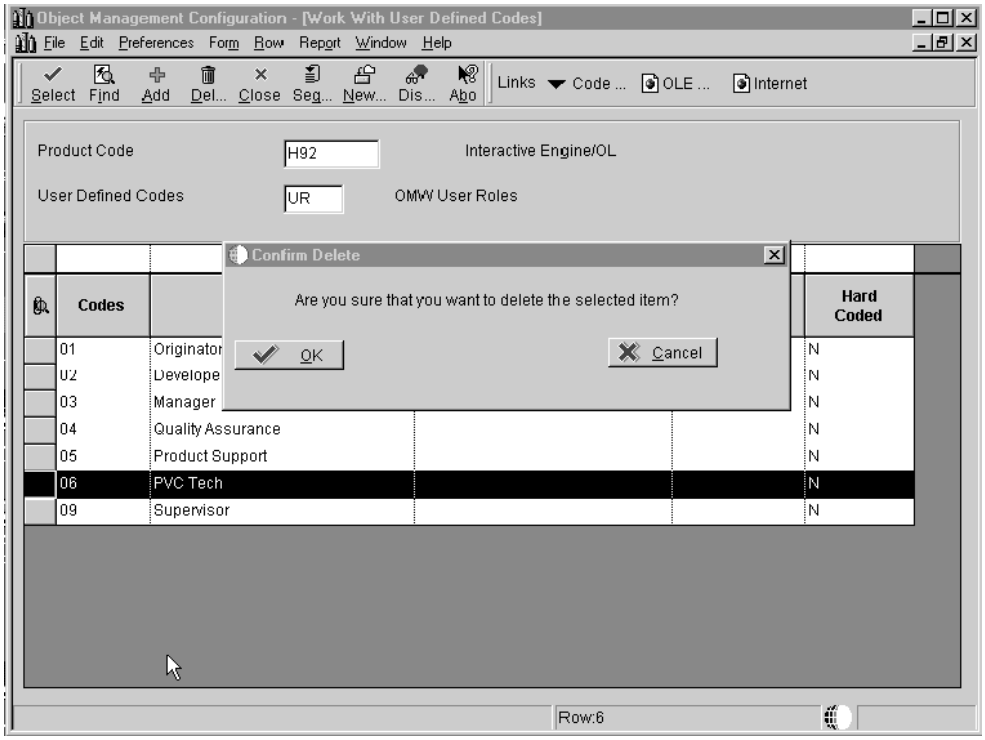
From the Object Management menu (GH9081), choose Object Management Setup (P98230).

1. From the Object Management Setup form, click User Roles.
2. 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 modifications required.
5. Click Find and verify that the modifications you made appear in the list.
6. Click OK.

► To delete a user role

From the Object Management menu (GH9081), choose Object Management Setup (P98230).

1. From the Object Management Setup form, click the User Roles button.
2. Click the cell to the left of the User Role 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 have been deleted.
7. Click OK.

Setting Up Allowed User Actions

The Allowed Actions Form lets you assign allowed actions to user roles for each object type during a specific project status. The following user defined codes (UDCs) define allowed Object Management Workbench actions involving objects:

- 02 – Check in
- 03 – Check out
- 04 - Delete
- 05 - Add
- 06 - Copy
- 07 - Install
- 08 - Save
- 09 - Restore
- 10 - Design
- 11 - Get
- 12 - Remove object from project

- 13 - Update the project
- 16 - Add an object to the project
- 21 - Switch tokens
- 23 - Release from token queue
- 30 - Erase check out
- 38 - Status change

For example, if you want the developer to be allowed to check in all object types when the project is at project status 21, you would enter 02 - Developer in the User Role field, *ALL in the Object Type field, select 02 – Check in in the Allowed Action field, and 20 - Programming in the Project Status field.

Note

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

► To set up allowed user actions

From the Object Management Setup form, click the Allowed Actions button.

1. Click Find to display previously defined user actions.
2. To create a blank row in which to add a definition, sort on the allowed user action to be worked on.
3. Complete one or more of the query by example (QBE) columns and click Find.
4. Scroll to a blank row at the bottom of the sorted list.
5. Complete the following fields in the blank row:
    - OMW User Role
    - Object Type
    - Project Status
    - Action

    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 row appears.
6. Repeat this procedure until all allowed user actions are set up.
7. Click OK.

Configuring Object Management Workbench Functions

To configure Object Management Workbench (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.

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.

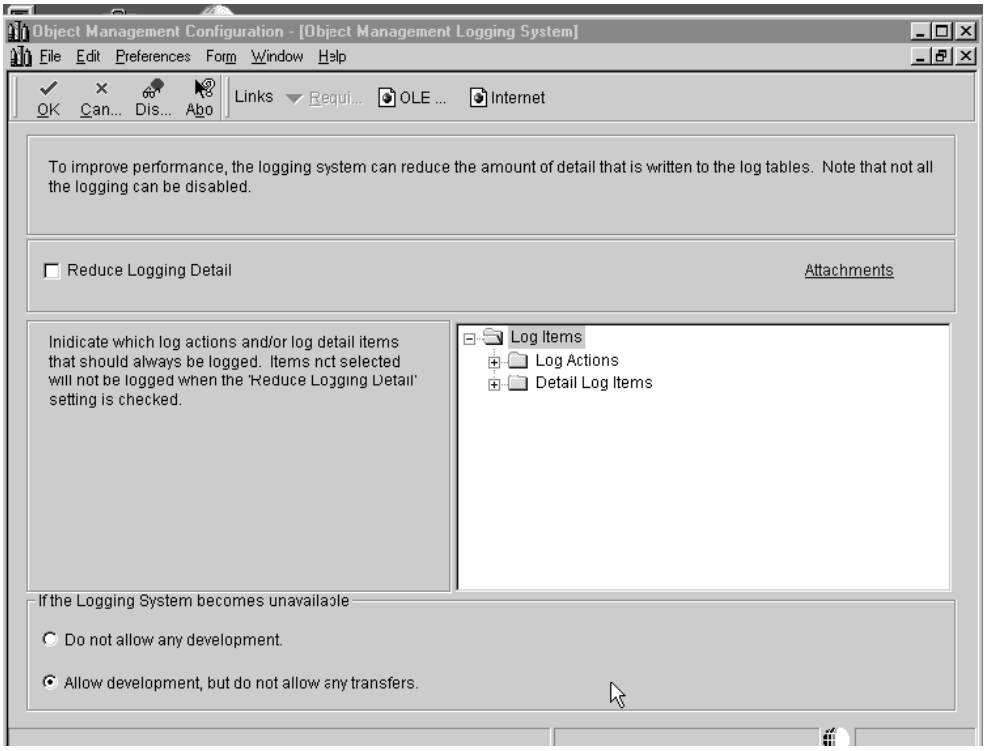
► To disable SAR system integration

1. Click the SAR System Integration button on the Object Management Setup form.
2. Make sure the Integrate SAR System option is blank.
3. Verify that all other fields are grayed out and deselected.
4. Click OK.

► To control logging detail

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

1. From the Object Management Setup form, click the Logging System button.

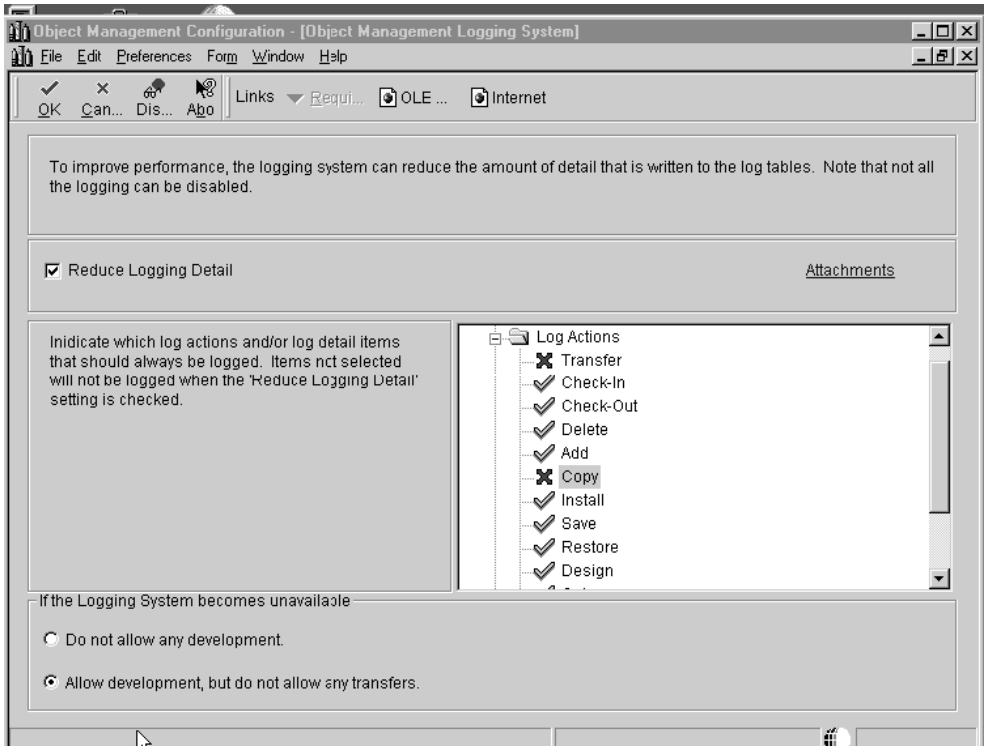


2. Click the Reduce Logging Detail option.

   A check mark appears next to the option chosen.

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

   A red X appears next to the deselected items.



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

► To control development in the event of logging failure

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

1. On the Object Management Setup form, click the Logging System button.
2. To disable development if logging fails, choose the Do not allow any development option.
3. 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.

Note
The Allow development but do not allow any transfers option is chosen by default.

4. 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

► To set up project constants

1. Click the Constants button on the Object Management Setup form.
2. To enter a project status for a user's personal default project, click the visual assist for the following field:
   - Enter the Project Status for user's personal default project
3. Double-click a project status.
4. To enter the initial project status for all new projects, click the visual assist of the following field:
   - Enter the initial Project Status for all new projects
5. Double-click a project status.
6. To enter the User Role to use when assigning the originator to a project, click the visual assist for the following field:
   - Enter the User Role to use when assigning the originator to a project
7. Double-click a project status.

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

Configuring 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 activities that occur during a project development cycle. Object transfer activity rules work in conjunction with project status activity rules, and define the From and To locations for moved objects.

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 the following:

- 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 turned on.

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 - Cancelled Entered in Error

► To set up project status activity rules

1. From the Object Management Setup form, click the Activity Rules button.
2. Click Find.

   All available From project statuses appear.

3. Click the From Project Status for which you want to set up one or more To project statuses.
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 the following 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
   - To Project Status

- From SAR Status

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

- To SAR Status

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

  A blank row appears below the row 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. Click Close.

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 the following information:

- Determine project statuses when users can check in, check out, and get objects. Getting an object means copying its specifications to your work area without checking it out.
- Determine at which status change you would like objects to be transferred.
- Determine project statuses when object tokens are released.

The following 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 DV9 to PY9.
- 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 DV9 to PY9 and then to PD9, you will want to set up rules to transfer the object from DV9 to PY9 and from DV9 to PD9 because the object could be retrieved in any order.

► To set up object transfer activity rules

1. From the Object Management Setup form, click the Activity Rules button.
2. 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.

5. Click Select.
6. Scroll to the blank row at the bottom of the list. Complete the following fields for the object type desired:

   - Active
   - User

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

   - 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.

   - From Release

   This field contains the release level of ERP 9.0 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 F98811 (Activity Specifications table) 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 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 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

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.

Creating a Save Location

During the installation process, an additional path code might not have been created to use as your 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.

► To add an object's save location

The Object Save Locations form indicates the save-off location for Object Librarian (OL) objects. Defining the save location will transfer objects that are saved into the path code specified. Currently, only the save locations for Object Librarian objects may be defined.

1. Click the Save Locations button on the Object Management Setup form.

   The Location column contains the names of path code where your version of ERP 9.0 is installed.

2. To add a new save location, click a blank field in the Location column.
3. Click the visual assist button.
4. Locate and double-click the current location of the object.

The Object Save Locations form reappears with your object's current location in the Location column.

5. In the same row, scroll to and double-click the Save Location field located to the right of the Location field clicked previously.
6. Click the visual assist button.
7. Scroll to and double-click the new save location of the object.

   The Object Path Save Locations form reappears with your object's new save location in the Save Location column.

8. Click OK.

► To modify an object's save location

The Object Save Locations form enables you to modify the save location for Object Librarian objects, which might be necessary during a project.

1. Click the Save Locations button on the Object Management Setup form.
2. Click the Save Location field.
3. Click the visual assist button.
4. Scroll and double-click the object's new save location.

   The Object Save Locations form reappears with the modified object save location in the Save Location column.

5. Click OK.

► To delete an object’s save location

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 the Object Management Setup form, 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

Notification subscriptions allow you to alert users via e-mail regarding 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.

► To enable or disable object action notifications

1. On the Object Management Setup form, click the Object Action Notification button.
2. To enable object action notification, choose the Activate Object Action Notification option.
3. To disable object action notification, clear the Activate Object Action Notification option.
4. 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 e-mail message is sent to the user.

► To add a notification subscription

1. From the Object Management Setup form, click the Notification Setup button.
2. Click Find to display the current notification subscriptions.
3. Scroll to a blank row and complete the following mandatory fields:
    - OMW User Role
    - Action
4. Complete the following optional fields:
    - Object Type
    - Object Name
    - Reporting System Code
    - Path Code

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

Note

Notification Subscriptions can be created for an action performed on the following 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.

► To modify a notification subscription

1. From the Object Management Setup form, 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 your changes.
4. Click OK.

► To delete a notification subscription

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

► To sort notification subscriptions

1. From the Object Management Setup form, click the Notification Setup button.
2. Above the rule headers, click the Query by Example column to be filtered.

   If a visual assist appears, click it and double-click your filter criteria. In other Query by Example columns, enter your filter criteria.

3. Click Find.

   The filtered notification subscriptions appear.

4. Click OK.

Working with 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 your 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 allows 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. The following two tasks must be performed together to produce customized project and object development reports.

- Reorder log record fields
- Print logs

► To view project or object logs

1. On Solution Explorer, type GH902 in the Fast Path field and press Enter.
2. From Cross Application Development Tools, choose Object Management Logging.

3. On Work With Object Management Log, perform one of the following 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.
    - Turn on the Show Only Last Action option to show only the last logging action for a given project or object.
4. Click Close.

► To locate object logs

1. In Solution Explorer, type GH902 in the Fast Path field and press Enter.
2. From Cross Application Development Tools, choose Object Management Logging.
3. On Work With Object Management Log, click Form and then click Object Logs.
4. On Work With Object Logs, you can do the following:
    - Click Find to show all OMW object logs.
    - Enter data in the Query by Example cells to narrow your search and click Find.
    - Turn on the Show Only Last Action option to show only the last logging action.
    - Click the Check for Attachments button to check for object attachments.
5. Click Close.

► To locate project logs

1. On Solution Explorer, type GH902 in the Fast Path field and press Enter.
2. From Cross Application Development Tools, choose Object Management Logging.
3. On Work With Object Management Log, click Form and then click Project Logs.
4. On Work With Project Logs, you can perform the following functions:
    - Click Find to show all OMW project logs.
    - Enter data in the Query by Example cells to narrow your search, and then click Find.
    - Turn on 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.
5. Click Close.

► To view detail logs

1. Double-click any log record you wish to research. Or, click the desired log record row to highlight it, 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.

► To reorder log record fields

1. In Solution Explorer, type GH902 in the Fast Path field and press Enter.
2. From the Cross Application Development Tools, choose Object Management Logging.
3. On Work With Object Management Log, click Sequence.
4. Click the first column you want to sort in the Columns Available window.
5. Click the right-pointing arrow to move it to the Columns Sorted window on the right.
6. Repeat steps 3 and 4 as required until all the columns you wish 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.

7. Click OK in the Select Grid Row Sort Order form to reorder the log columns.

► To print logs

From the Cross Application Development Tools menu (GH902), choose Object Management Logging (P98210).

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.

Printing ERP 9.0 Reports

The Printers application (P98616) provides a single point of entry for configuring your printers within ERP 9.0. The application allows you to define printers for workstations and enterprise servers. These definitions reside in ERP 9.0 tables that are maintained by the Printers application (P98616).

In addition to creating your own reports, ERP 9.0 includes a number of predefined reports and report versions, which you can use and modify for your business needs. ERP 9.0 uses the batch engine to create reports, and generates these reports in Portable Document format (PDF). You can view the PDF files 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.

Understanding ERP 9.0 Printing

When you submit an ERP 9.0 report, the batch engine generates a portable document format (PDF) file. The batch engine uses a device context to create the PDF file. This device context consists of information such as page size and the printable area of a page. ERP 9.0 generates this information from the printer tables for all platforms.

ERP 9.0 gives you the option of viewing the report (the PDF file) on your workstation, using Adobe Acrobat Reader, or sending the report to a printer. You can also print the report from the Adobe Acrobat Reader. When you send the report to a printer, ERP 9.0 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 ERP 9.0 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:

1. 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.
2. 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.
3. The RDA specifications pass a printer name to the batch process. If this process retrieves a valid printer name, the following process is ignored.
4. ERP 9.0 determines from the Printer Definition table (F98616) a valid default printer based on the current user, the environment that 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 your 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, ERP 9.0 copies the PDF file from the server to the local \b9\PrintQueue directory on your 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 your report. When you view a log, your workstation stores the log file in the \b9\PrintQueue directory.

See Also

- *Generating and Retrieving Logs for Your Report* in the *System Administration Guide* for more information about the location of the PrintQueue directory on a server

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 Acrobat Reader. The PDF file is stored in your local \b9\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 ERP 9.0 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 ERP 9.0 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 ERP 9.0 saves the output after processing the report.

```
[NETWORK QUEUE SETTINGS]

PrintImmediate=TRUE/FALSE

SaveOutput=TRUE/FALSE
```

Setting	Description
PrintImmediate	Specifies whether or not the system automatically prints the report after processing is complete. Valid values are: 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. 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.
SaveOutput	Specifies whether the system saves or deletes the output after you view or print the job. Valid values are: TRUE. The system saves the output after you have viewed or printed the job. FALSE. The system deletes the output after you have viewed or printed the job.

Working with the Printers Application

ERP 9.0 provides a single application that uses a director interface to help you set up your 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 your printers use at the time that you add and modify printer settings.

Note

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

See Also

- *Understanding ERP 9.0 Printing* in the *System Administration Guide* for information about how ERP 9.0 determines which printer to print to when a user submits a report

Before You Begin

When you add a printer, ERP 9.0 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.

- Follow the procedures for adding a new printer as described by the Printer Setup director.

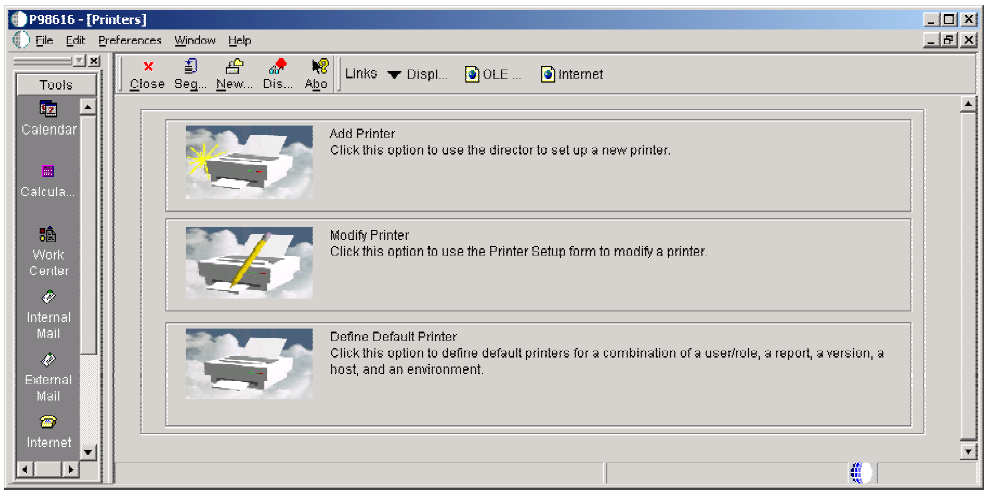
- First-time users who are installing their first printer must complete the “To add a new printer” task and then the “To define a default printer” task.
- You must complete all of the fields that appear on the director forms.

► To add a new printer

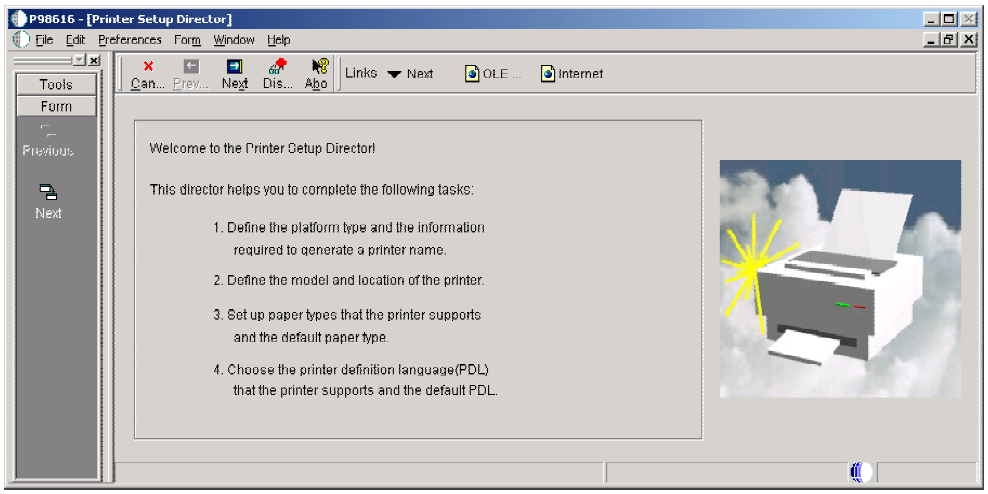
Note

You must complete all of the fields that appear on the director forms.

On the Batch Processing Setup menu (GH9013), choose Printers (P98616).

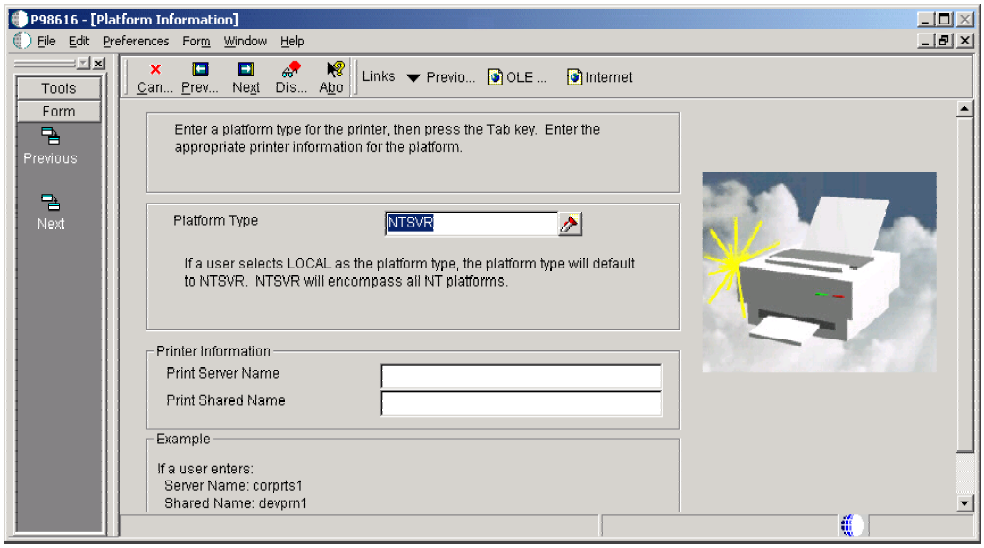


1. On the Printers form, click the Add Printer button.



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 your ERP 9.0 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 your platform. ERP 9.0 uses this name, along with the print shared name, to create the printer name, which appears grayed-out on the subsequent form.

     AS/400: library name/outqueue name

     For the AS/400, the physical printer name must be the same as the outqueue name. If you use the default QGPL library to store your outqueues, you need only enter the outqueue name in this field. This information must be entered in upper case.

     Example: DEVDES3A

     If your 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.

     Example: QUSERSYS/DEVDES3A

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

Windows NT: \\server name\printer name

Example: \\corprts1\docprf2

UNIX: printer name (no slashes)

Example: devprn16

This information must be entered in lower case.

For printing reports to a non-network printer, leave this field blank.

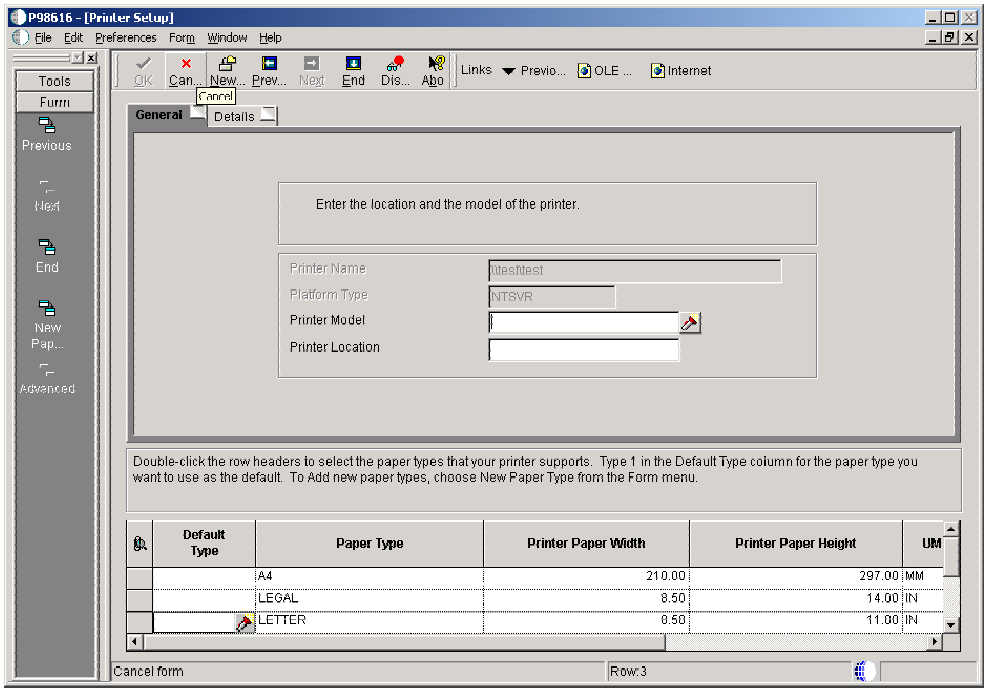
- Print Shared Name

  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 your platform. ERP 9.0 uses this name, along with the print server name, to create the printer name, which appears grayed -out 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 (AS/400 only).

Note
When you change an existing printer, you make your modifications on this page. See *To modify an existing printer* in the *System Administration Guide.*



5. On the General tab, complete the following fields:

- Printer Model
- Printer Location

6. Click the Details tab:

   717297]

7. On the Details tab, under Printer Definition Language, choose any the following options:

   - PostScript
   - PCL
   - Line Printer

   Note
   If you choose PostScript or PCL, ERP 9.0 disables the Line Printer option. If you choose the Line Printer option, ERP 9.0 disables the PostScript and PCL options. You can choose 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 your default. You can override this PDL when a batch process is submitted.

8. When you choose 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 ERP 9.0 to draw paper.

9. When you choose the Line Printer option, complete the following fields under Line Printers to set the paper dimensions and line parameters:

   717300]

   - 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 AS/400 server, fields appear within a box labeled AS400 Only. You use these fields to set the AS/400 encoding that your printer supports. Choose one of the following:

    - ASCII Encoding
    - EBCDIC Encoding

    717301]

    Note
    If you choose a PostScript or PCL printer along with an AS/400 server, the ASCII Encoding option is automatically checked and the AS400 Only box is disabled.

11. When you choose 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.

    - Turn on 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.

      717304]

    - On Work with Conversion Programs, choose one of the filters or click Add, and then click Select or Copy.

      717308]

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 (AS/400, HP9000, and so on) and the type of printer (postscript, PCL, or line). For example:

-s *string_name* -l *library_name* -f convertPDFToPS

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 your 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.

386791]

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.

386792]

15. To add a new paper type, do the following:

    a. From the Form menu, choose New Paper Type.

717312]

    b. On Work With Paper Types, click Add.

717313]

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

    - Paper Type
    - Paper Height
    - Paper Width
    - UM

ERP 9.0 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.

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

    ERP 9.0 saves the new printer and displays the Printer form.

► To define a default printer

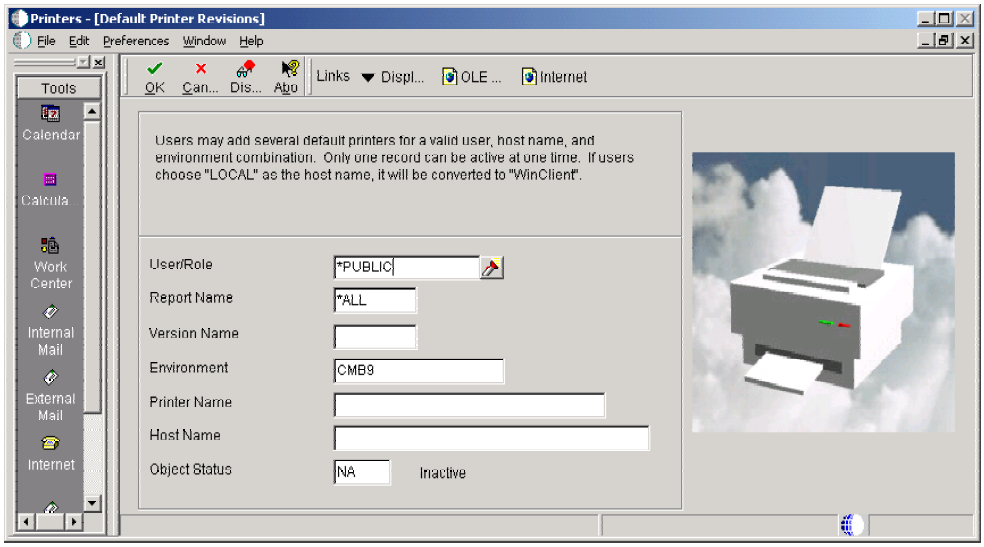
On the Batch Processing Setup menu (GH9013), choose Printers (P98616).

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

   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 to choose 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

  ERP 9.0 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 to 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 as 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, choose a default record and then, from the Row menu, choose Change Status.

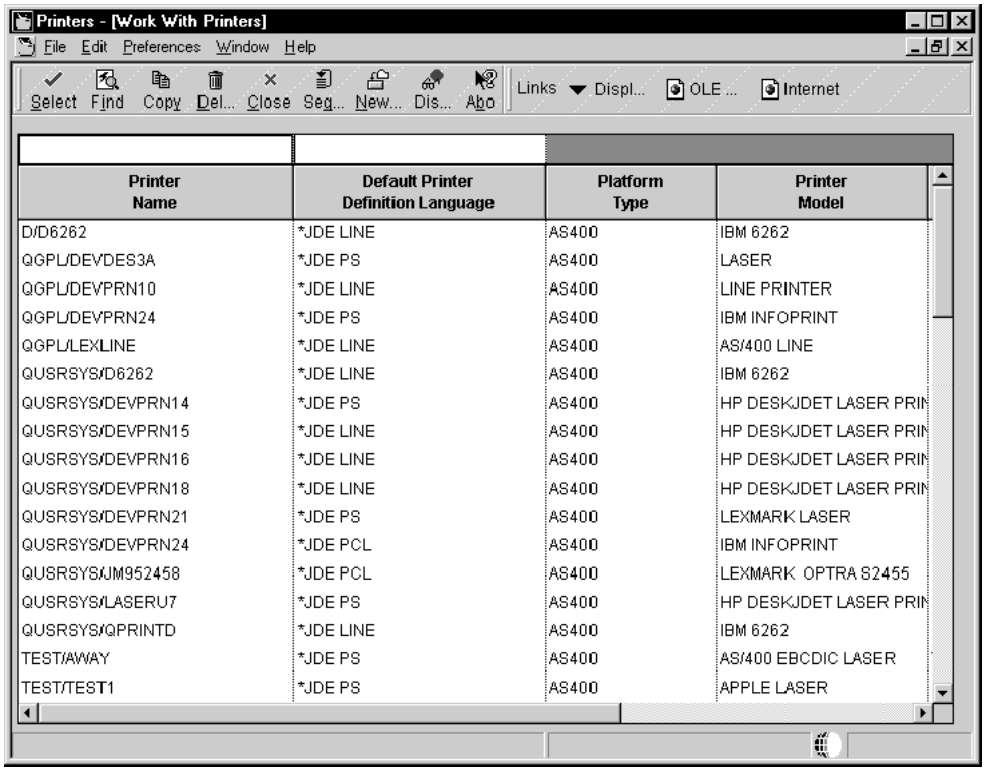
   If another printer is already apecified as the active default printer, an error occurs. To change the original default printer to inactive, choose it, from the Row menu choose Change Status, and then make the new printer the default.

► To modify an existing printer

On the Batch Processing Setup menu (GH9013), choose Printers (P98616).

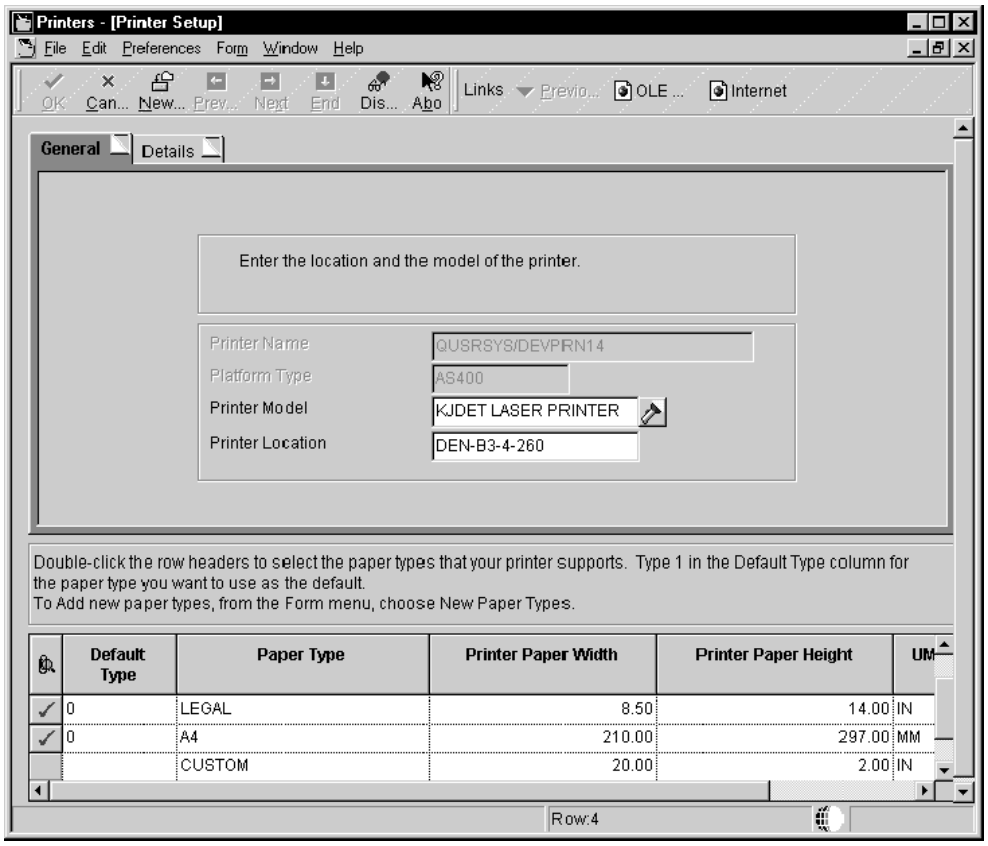
1. On the Printers form, choose the Modify Printer option.

   The Work With Printers form appears. This form lists all available printers.



2. 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 types.



3. Modify the information for your printer as necessary and then 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.

   ERP 9.0 saves the new printer information and returns you to the Work With Printers form.

► To copy an existing printer

On the Batch Processing Setup menu (GH9013), choose Printers (P98616).

1. On the Printers form, choose the Modify Printer option.

   The Work With Printers form appears. This form lists all available printers.

2. Choose the printer that you want to copy, and then click Copy.

   The Printer Setup form appears.

3. Complete the following 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 NT printer would be: `\\corprts1\docprf2`. If you use multiple platforms, you must define a printer for each platform, using the following naming conventions:

   - AS/400: *library name/outqueue name*

For the AS/400, the printer name must be the same as the outqueue name. If you use the default QGPL library to store your outqueues, you need only enter the outqueue name in this field. The information that you enter must be in upper case.

Example: DEVDES3A

If your 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.

Example: QUSERSYS/DEVDES3A

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

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

  Example: \\corprts1\docprf2

  The information that you enter must be in lower case.

- UNIX: *printer name* (no slashes)

  Example: devprn16

  The information that you enter must be in lower case.

- Platform Type

Enter the platform that you are printing from, such as an AS/400 server.

4. On the Details tab, change any information as needed.
5. Click OK.

► To delete a printer

On the Printers menu (GH9013), choose Printers (P98616).

1. On the Printers form, choose the Modify Printer option.

   The Work With Printers form appears. This form lists all available printers.

2. Choose a printer or choose multiple printers by holding down the Ctrl key, and then clicking Delete.

   This action removes the printer definition from ERP 9.0.

► To delete a paper type

On the Printers menu (GH9013), choose Printers (P98616).

1. On the Printers form, choose the Modify Printer option.

   The Work With Printers form appears. This form lists all available printers.

2. Choose a printer, and then click Select.

   The Printer Setup form appears.

3. On the Printer Setup form, from the Form menu, choose New Paper Type.

   The Work With Paper Types form appears.

4. Choose a paper type and click Delete.
5. On Confirm Delete, click OK.

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

► To search for incorrect printer records

Use the following batch process to search the Printer Capability table (F986163) and to list printer records that are incomplete or contain incorrect printer information. This report lists information that can help you correct your printing records.

From the System Administration Tools (GH9011) menu, choose Batch Versions.

1. On Work With Batch Versions - Available Versions, type `R9861602` in the Batch Application field and click Find.

   The `XJDE0001` version appears.

2. Run the version.

Note
See *Submitting a Report* in the *Enterprise Report Writing Guide*. 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 ERP 9.0.

See *To modify an existing printer in the System Administration Guide. U*sing the report, find the printer record and correct it.

To determine logical printers attached to batch processes

Use the following batch process to determine which of your batch processes, if any, are attached to printers.

From the System Administration Tools (GH9011) menu, choose Batch Versions.

3. On the Work With Batch Versions - Available Versions form, in the Batch Application field, type `R9861601`, and click Find.

   The `XJDE0001` version appears.

4. Run the version.

Note
See *Submitting a Report in* the *Enterprise Report Writing Guide*. 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 ERP 9.0.

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

   Only someone familiar with RDA should attempt to attach a printer.

Generating and Retrieving Logs for Your Report

When you run an ERP 9.0 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 `jdedebug.log`. These logs allow you to review how your reports process on the server. These logs reside in a specific directory on the server. Your `jde.ini` settings determine the location of this directory. Also, the `jde.ini` settings differ slightly, depending on the platform that you use. The following list provides sample `jde.ini` settings for the directory where your report logs reside:

AS/400

```
 [INSTALL]
DefaultSystem=B9SYS
```

Example path: B9SYS\PRINTQUEUE

UNIX

```
 [INSTALL]
B9=/usr/PeopleSoft/output
```

Example path: /usr/PeopleSoft/output/PrintQueue

Windows NT Server

```
 [INSTALL]
B9=d:\PeopleSoft\output
```

Example path: d:\PeopleSoft\output\PrintQueue

The default directory for your 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 your report output resides after processing. If you set your `jde.ini` to save the output for your reports, ERP 9.0 saves a PDF file for the report in the report output directory.

► To create logs for your report

On the System Administration Tools menu (GH9011), choose Batch Versions (P98305).

The Work with Batch Versions form appears. On this form you can locate and run reports. Also, you can modify version detail information, data selection, and data sequencing.

1. Type an application ID in the Batch Application field and click Find.

   For example, type R014021 to locate a version for the One Line Per Address report.

2. Choose a version to submit, and then click Select.

   The Version Prompting form appears. On this form, you can choose to change the data selection, change the data sequencing, and access the Advanced Operations form.

3. Choose Advanced from the Form menu.

   The Advanced Operations form appears. On this form, you can override the location where your report processes, activate the jde.log, activate the jdedebug.log, and modify the level of information that your logs include.

4. Modify the following information, then click OK:

   - Logging (JDE.log)

   Turn on this option to activate a basic log that helps you determine when a fault occurs during a batch process.

   - Tracing (JDEDEBUG.log)

   Turn on this option to turn on advanced UBE logging that includes details about the batch process.

   - UBE Logging Level

   The value that you enter here, from 0 to 6, determines the level to which your batch process log shows errors, ranging from error messages to object level messages and UBE function messages.

   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.

Setting Up an ERP 9.0 Printer to Use a Barcode Font

ERP 9.0 supports the use of the BC C39 3 to 1 Medium barcode font. J.D. Edwards includes this barcode font with ERP 9.0. After you set up your ERP 9.0 printers, you can assign a printer to use a barcode font for your reports.

Note

ERP 9.0 printers that support barcodes must use either the PostScript or PCL printer definition languages.

► To set up an ERP 9.0 printer to use a barcode font

On the Printers menu (GH9013), choose Bar Code Support (P986166).

1. On the Work With Bar Code Font form, click Add.

   The Bar Code Font Revisions form appears. Use this form to determine which printer uses the barcode font.

2. Complete the following fields and options:

   - Printer Name

   Click the visual assist for this field to access a list of ERP 9.0 printers.

   - Printer Definition Language

   Choose the appropriate option, depending on the printer definition language of the printer in the Printer Name field.

   - True Type Font Name

   Click this button to select the true type barcode font BC C39 3 to 1 Medium on the Font form.

   - Printer Font Name
   - Symbol Set ID

   (PCL only). This value defines the character and the character mapping for a particular symbol set. Contact your PCL printer font vendor to obtain this information.

3. After you finish entering information for a barcode-capable printer, click OK.

   ERP 9.0 saves the information and clears the revision form. You can continue to enter information for other ERP 9.0 printers that support barcodes, or click Cancel to exit the form.

► To modify ERP 9.0 barcode printer information

On the Printers menu (GH9013), choose Bar Code Support (P986166).

1. On the Work With Bar Code Font form, click Find.

   ERP 9.0 printers previously set to support the barcode font appear in the detail area.

2. Choose the printer that has the information you want to modify, and click Select.

   The Bar Code Font Revisions form appears.

3. Change the information on this form as necessary and click OK.

► To copy ERP 9.0 barcode printer information for a new printer

On the Printers menu (GH9013), choose Bar Code Support (P986166).

1. On the Work With Bar Code Font form, click Find.

   ERP 9.0 printers previously set to support the barcode font appear in the detail area.

2. Choose the printer that has the information you want to copy, and click Copy.

   The Bar Code Font Revisions form appears.

3. Change the name of the printer. You can also change any other information on this form as necessary.
4. Click OK to save your information.

► To delete barcode support information from an ERP 9.0 printer

On the Printers menu (GH9013), choose Bar Code Support (P986166).

1. On the Work With Bar Code Font form, click Find.

   ERP 9.0 printers previously set to support the barcode font appear in the detail area.

2. Choose the printer that you want to delete, and click Delete.
3. On the Confirm Delete form, click OK.

Designing Reports to Run on ERP 9.0 Line Printers

When you run a report on a line printer in ERP 9.0, you must follow specific guidelines to ensure that the information that is 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.

This section provides the information that is necessary to create ERP 9.0 line printer reports.

Important Note

The information in this section is intended for users with previous experience in creating ERP 9.0 reports and setting up ERP 9.0 printers.

See Also

- *Report Design Director* in the *Enterprise Report Writing Guide* for specific information about working with the Report Design tool
- *Printing ERP 9.0 Reports* in the *System Administration Guide* for specific information about ERP reports

See the following topics in the *Server and Workstation Administration Guide*:

- *Setting Up a Printer for AS/400* for information about setting up printers on AS/400 servers
- *Setting Up a Printer for UNIX* for information about setting up printers on UNIX servers

- *Setting Up a Printer for Windows NT* for information about setting up printers on Windows NT servers

► To design an ERP 9.0 report to run on a line printer

Important

In the Batch Versions application, create a version of the report to use only on line 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 properly on other printer platforms.

On the Cross Application Development Tools menu (GH902), choose Report Design Aid.

1. Open the report with the version that you want to modify to support line printers.
2. From the Layout menu, choose Grid Alignment.

   The Alignment Grid form appears. On this form, you need to modify the vertical grid spacing for the report.

3. Set the value in the Vertical field to 16 and click OK.
4. From the File menu, choose Report Properties.

   The Properties form appears. On this form, you need to change the font properties for the report.

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. Turn on the Apply settings to all objects option to make sure these settings apply to objects that might have individual font settings applied.
7. 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.

   Note
   See *Basic Report Enhancements* in the *Enterprise Report Writing Guide* for specific information about formatting your report.

(Steps 7 through 10 apply to Group sections only.)

8. If some data fields still do not properly align, press and hold the Ctrl key, and then click each field that you want to align.

   The last field that you choose is the field, the top edge of which you will use 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.

► To set up an ERP 9.0 line printer

Important

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 an ERP 9.0 printer in the *Working with the Printers Application* topic in the *System Administration Guide*.

On the Printers menu (GH9013), choose Printers (P98616).

1. On the Printers form, choose Add Printer.
2. On Printer Setup Director, click Next.
3. On Platform Information, complete the following 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 the lines per page (LPP) values.

   These values determine the paper dimensions that your line printer will use when printing ERP 9.0 reports. For example, set the following values to print on an 8.5 inch x 11 inch piece of paper:

   - Characters Per Inch: 10
   - Columns Per Page: 85
   - Lines Per Inch: 6
   - Lines Per Page: 66

   Note
   Use the following formula to calculate your paper dimensions:

   CPP / CPI = width in inches (85 / 10 = 8.5)

LPP / LPI = height in inches (66 / 6 = 11)

8. Click End to save these settings.

► To print multiple copies to a remote AS/400 line printer

This task is necessary only if the output queue for an AS/400 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.
4. Your output queue should now be able to send multiple copies of your documents to the remote printer.

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 into 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

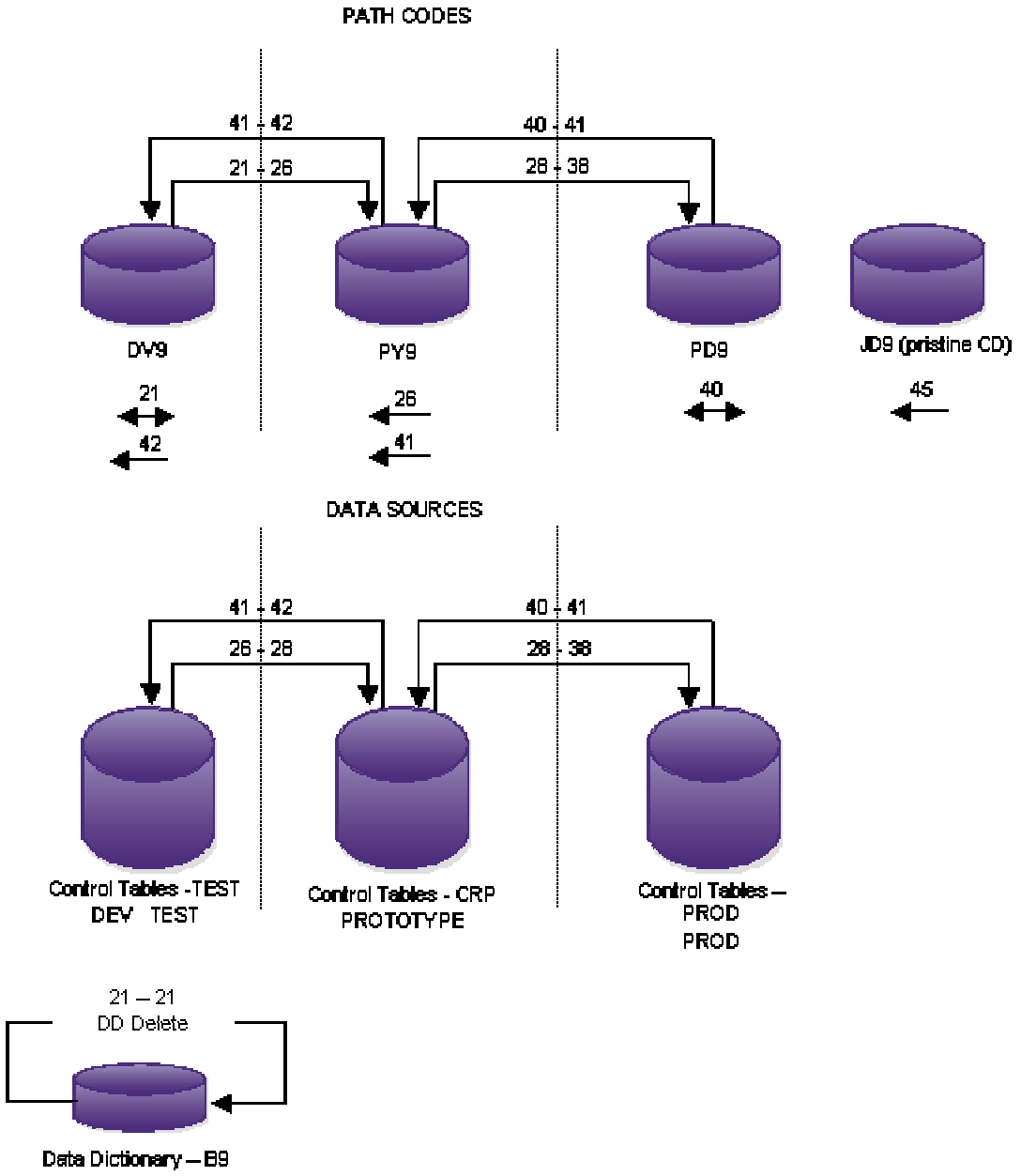
42 = Transfer from Prototype to Development

01 = Complete

During this promotion cycle, administrators check objects out of and into 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; J.D. Edwards recommends that you apply status activity rules that limits this promotion cycle to a specific group -- those with the User ID for administrators.

The following illustration shows the project promotion life cycle:

Project Promotion Life Cycle



Working with Servers

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

- Server jobs
- ERP 9.0 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 ERP 9.0 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.

You also can use the Work With Servers program to end and to stop ERP 9.0 subsystems, and to view the status of ERP 9.0 subsystems that are running or are waiting to process jobs.

Working with 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 ERP 9.0 server. Similarly, using the Submitted Reports applications, workstation users can, in general, control only those jobs submitted by them.

You should use ERP 9.0 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 (P986116) allows 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 Reports application (P986116). 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).

From within Work With Servers, select Server Jobs from the Row exit menu to access the Submitted Job Search form, and access the following options from the Row menu:

- Print

  This option allows you to print jobs with a status of E or D. Using a standard print form, you can print to your default printer or print to another available printer.

- View PDF

  This option allows you to launch the Adobe Acrobat Reader program and display your report online. You can review your report online, and then print to your default printer or to another available printer.

- View CSV

  This option enables you to output reports to a file with “Comma Separated Values.” The output can be opened in an Excel database.

- View OSA

  This option allows you to output reports to a file with a user-defined output type. To use this option, you must first set up the output conversion.

- View Logs

  This option allows you to view the jde.log and the jdedebug.log.

- Terminate

  This option ends the job if it is processing. This option does not remove the job but moves it to an E (error) status, thereby allowing a user to view the logs.

- Release

  This option removes the H (hold) status from a job and sends it into the queue.

- Hold

  This option stops a job until you release it again.

Checking the Status of Reports

After you submit your report, you can check the status of your job in the queue. Depending on the status of your job, you can perform tasks such as printing your report, viewing your report output online, deleting your report, and holding your report in the queue.

► To check the status of reports

On System Administration Tools (GH9011), choose Work With Servers (P986116).

1. On the Work With Servers form, choose a server or use the query by example row to locate a specific server.
2. Choose a server with which to work and click Select.
3. On the Submitted Job Search form, complete the following fields and then click Find:

   - User ID

   The default user ID is the user logged on to the current ERP 9.0 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 the user you want.

   - Job Queue

   Enter the name of the logical queue on the server for which you want to view jobs.

   From the Submitted Job Search form, you can print, view, delete, and hold your job. You can also view logs with detailed information about how your report processed.

   The detail area of the form displays the jobs and their statuses. You can use the visual assist in the Status field to read the UDCs for status codes in your installation.

Changing the Priority and the Printer for Jobs

To move your job up or down in the queue, you can change the priority of the job while the job is at the status of W (Waiting). You might choose to move jobs with priority up in the queue and those with less priority down in the queue. You can also override the location where your job prints.

► To change the priority and the printer for jobs

On System Administration Tools (GH9011), choose Work With Servers (P986116).

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 your 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. Choose a job with which to work and click Select.

   The Job Maintenance form appears. On this form, you can review information about your batch job, modify the priority of the job, and change the printer on which the job will print.

3. Modify the following information and click OK:

   - Job Priority

Printing Jobs

For jobs with a status of D (Done) and E (Error), you can send your job directly to your default printer without viewing the PDF file online. A status of D means that the processing for your 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 your report.

► To print jobs

On System Administration Tools (GH9011), choose Work With Servers (P986116).

1. On the Work With Servers form, choose a server or use the query by example row to choose a specific server.
2. From the Row menu, choose Server Jobs.

   The Submitted Job Search form appears. Jobs specific to your user ID appear in the grid of this form by default. Depending on your security level, you can change the User ID field and the Job Queue field to search for other jobs.

3. Choose 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 your report.

4. To print your job, click OK.

Viewing Reports Online

After your 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 your report output online, the system also creates a PDF file for the report in the following directory on your workstation:

\b9\PrintQueue

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

Before You Begin

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

► To view reports online

On System Administration Tools (GH9011), choose Work With Servers (P986116).

The Work With Servers form appears. On this form, you can access a list of servers used to process batch applications.

1. Choose a server from the list, or use the query by example row to choose a specific server.
2. Click Select or choose Server Jobs from the Row menu.

   The Submitted Job Search form appears. Jobs specific to your user ID appear on this form by default. Depending on your security level, you can change the User ID field and the Job Queue field to search for other jobs.

3. Choose the job that you want to view and then, from the Row menu, choose View Job.

   Adobe Acrobat Reader displays an online version of your report output. Refer to Adobe Acrobat Reader online help for more information about using Acrobat Reader.

Viewing the Logs for a Job

You can view logs that detail the steps taken while your job processed. From the Submitted Job Search form, you can access the `jde.log` and the `jdedebug.log` for your 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, which might not be the same machine as your workstation.

The `jde.log` is a general-purpose log used to track error messages generated by ERP 9.0 processing. The `jde.log` tracks any fault that might occur within ERP 9.0, including whether the sign on is successful. When you are looking for startup errors, you should read the `jde.log` from the top down. For other errors, you should read from the bottom up.

The `jdedebug.log` contains API calls 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 `jdedebug.log` to track errors; iInstead, it uses this log to track the timing of ERP 9.0 processes.

See Also

- *Working with the Workstation Log Files* and *Working with the Enterprise Server Log Files* in the *Server and Workstation Administration Guide* for more information about troubleshooting errors with submitted jobs

► To view the logs for a job

On System Administration Tools (GH9011), choose Work With Servers (P986116).

The Work With Servers form appears. On this form, you can access a list of servers used to process batch applications.

1. Click Find to locate all servers or use the query by example row to locate a specific server.
2. Choose the server that processed the job that you want to troubleshoot, and click Select.
3. Click Select, or from the Row Exit, choose Server Jobs.

   The Submitted Job Search form appears. Jobs specific to your user ID appear on this form by default. Depending on your security level, you can change the User ID field and the Job Queue field to search for other jobs.

4. Choose the job for which you want to view a log, and then choose View Logs from the Row menu.

   The View Logs form appears. On this form, you can choose to view the `jde.log` and the `jdedebug.log`.

5. Click OK to view the logs.

Note
If you choose both the `jde.log` and the `jdedebug.log`, the logs open in the same window. To view the logs separately, you must choose the logs separately.

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.

► To terminate jobs

On the System Administration Tools menu (GH9011), choose Work With Servers (P986116).

The Work With Servers form appears. On this form, you can access a list of servers used to process batch applications.

1. Choose a server from the list or use the query by example row to choose a specific server.
2. Click Select or choose Server Jobs from the Row menu.

   The Submitted Job Search form appears. Jobs specific to your user ID appear on this form by default. Depending on your security level, you can change the User ID field and the Job Queue field to search for other jobs.

3. Choose the job to terminate, and then choose 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

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.

► To hold a job

On System Administration Tools (GH9011), choose Work With Servers (P986116).

The Work With Servers form appears. On this form, you can access a list of servers used to process batch applications.

1. Choose a server from the list or use the query by example row to choose a specific server.
2. Click Select or choose Server Jobs from the Row menu.

   The Submitted Job Search form appears. Jobs specific to your user ID appear on this form by default. Depending on your security level, you can change the User ID field and the Job Queue field to search for other jobs.

3. Choose the job to hold and then, from the Row menu, choose Hold.
4. Click Find to update the detail area.

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

► To release a job

On System Administration Tools (GH9011), choose Work With Servers (P986116).

The Work With Servers form appears. On this form, you can access a list of servers used to process batch applications.

1. Choose a server from the list or use the query by example row to choose a specific server.
2. Click Select or choose Server Jobs from the Row menu.

   The Submitted Job Search form appears. Jobs specific to your user ID appear on this form by default. Depending on your security level, you can change the User ID field and the Job Queue field to search for other jobs.

3. Choose the job to release and then, from the Row menu, choose Release.

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

4. 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).

Processing Options: Work with Servers (P986116)

Security

This processing option specifies the level of security used when working with servers.

For information about a processing option, right-click the processing option field and choose What's This from the menu. Or, click the processing option field and press F1.

1. Security Flag

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

Blank No Security

1 Allow users to view jobs by group.

2 Allow users to view only their own jobs.

Managing ERP 9.0 Queues

Each ERP 9.0 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.

ERP 9.0 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

F986130 is a system table that is new with the ERP 9.0 release. Be sure to account for it when you map objects using Object Configuration Manager (OCM).

The following list summarizes how ERP 9.0, 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-ERP 9.0 queue, verifies that the native queue (for example, AS/400) exists.
- Inserts job record into the F986110 table.
- Sends a message to the queue kernel that is 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.

An ERP 9.0 application, Work With Job Queues (P986130), allows you to dynamically administer queues. You can use this application to create, modify, copy, delete, or change the status of job queues, regardless of platform.

You can also administer queue information contained in job versions using the Work With Batch Versions – Available Versions application (P98305). For example, you can change the queue to which a job is submitted on a server.

See Also

- *Working with Server Jobs* in the *System Administration Guide* for information about using the Work With Servers application (P986116) to administer UBEs

Administering Queues

You use the Work With Job Queues application (P986130) to define and manage queues. 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. You can copy a queue to another server. Finally, you can dynamically administer a queue by changing its status.

Before You Begin

- 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.dll
dispatchDLLFunction=_DispatchQueueMessage@28
maxNumberofProcesses=1
numberofAutoStartProcesses=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=1
QKOnIdle=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
```

► To add a queue

On the Batch Processing Setup menu (GH9013), choose Job Queues (P986130).

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 ERP 9.0 queue or a non-ERP 9.0 queue. Non-ERP 9.0 queues work only on the AS/400 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 blank for a non-default queue.

► To revise a queue

On the Batch Processing Setup menu (GH9013), choose Work With Job Queues (P986130).

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

► To copy a queue

On the Batch Processing Setup menu (GH9013), choose Work With Job Queues (P986130).

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

► **To change the status of a queue**

On the Batch Processing Setup menu (GH9013), choose Work With Job Queues (P986130).

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

   ERP 9.0 changes the status of the queue from Active to Inactive or from Inactive to Active, depending on its prior status.

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.

ERP 9.0 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

► **To override a job queue**

On the System Administration Tools menu (GH9011), choose Batch Versions (P98305).

The Work With Batch Versions – Available Versions form appears.

1. Find a version of a job that you want to submit and click Select.

   The Version Prompting form appears.

2. From the Form menu, choose Advanced.

   The Advanced Version Prompting form appears.

3. 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, choose 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. Choose 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.

Working with ERP 9.0 Subsystems

ERP 9.0 uses subsystems to offload processing from the enterprise server.

Understanding ERP 9.0 Subsystems

Subsystems are continuously running batch jobs that run independently of ERP 9.0 applications. Some ERP 9.0 applications use subsystems to complete needed work. You must manually start ERP 9.0 subsystems to minimize the consumption of system resources.

ERP 9.0 Subsystems

The term *subsystem* is an industry-wide generic term that usually indicates a system that is a subprocess to an operating system. On AS/400 server platforms, a subsystem is a logical process that is used to run system jobs, whether they are ERP 9.0 or other application jobs. For UNIX, an ERP 9.0 subsystem is functionally equivalent to a daemon. On UNIX and Windows NT server platforms, system jobs are processed in queues; these queues are functionally equivalent to subsystems on the AS/400.

Within ERP 9.0, subsystems are defined as continuously running batch jobs that run independently of, and asynchronously with, ERP 9.0 applications. ERP 9.0 subsystem jobs function within the logical process of the operating system or the queue defined for the server platform. You can configure ERP 9.0 to use one or more subsystems.

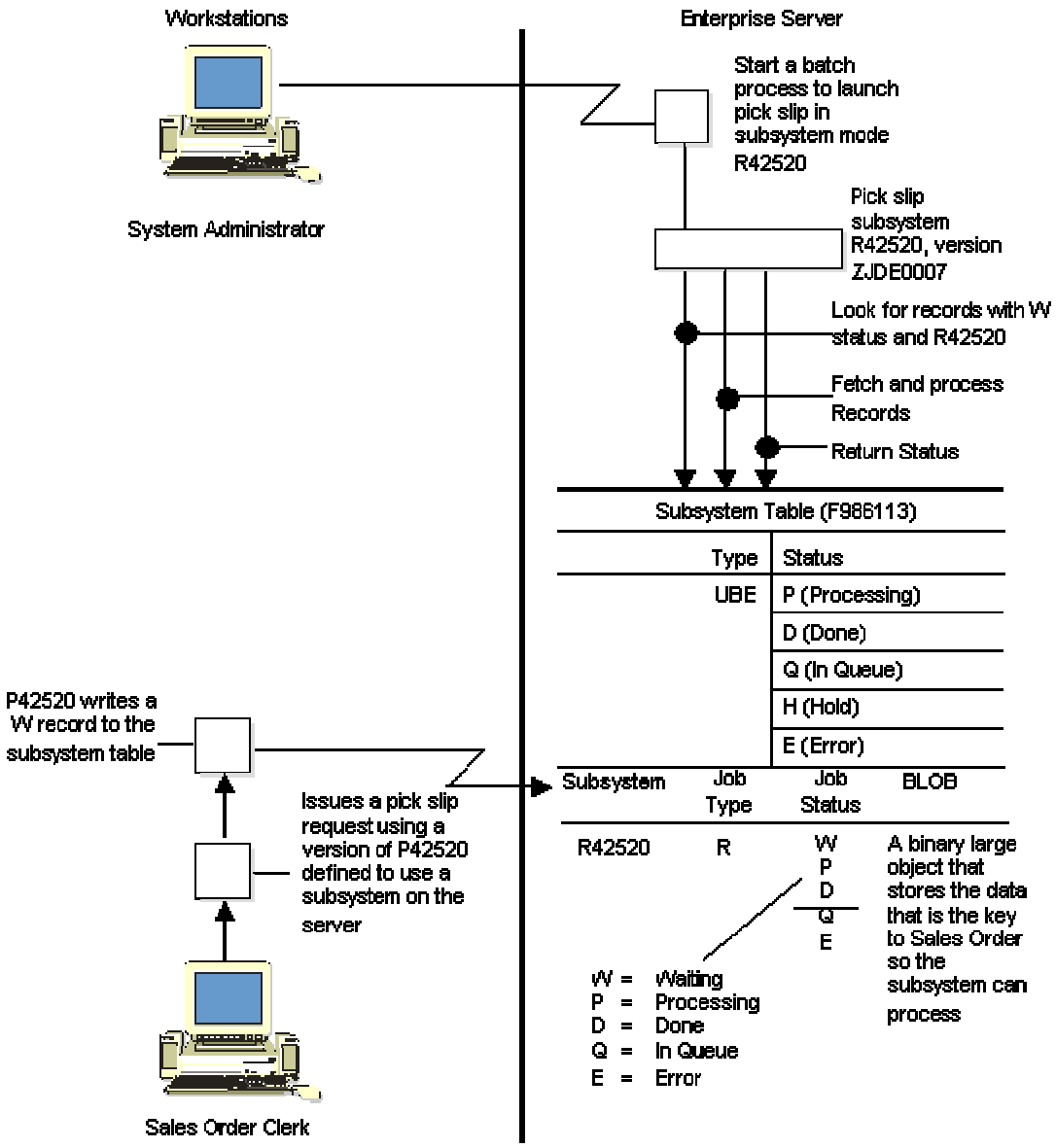
How ERP 9.0 Uses Subsystems

Some ERP 9.0 applications are designed to use subsystems. For example, you can instruct Sales Order Processing to print pick slips through an ERP 9.0 subsystem. You activate a subsystem through the processing options of an interactive application. Then you create a specific version of the interactive application, using that processing option to run the application in subsystem mode. When started, ERP 9.0 subsystems run continuously, looking for and processing requests from ERP 9.0 applications. Subsystems run until you terminate them.

Typically, you use subsystem jobs running on the enterprise server to offload 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 real time. 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 an ERP 9.0 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 ERP 9.0 subsystem to process the record without additional interaction with the requesting application. The continuously running ERP 9.0 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.

The following illustration shows the logical sequence of events associated with subsystems:



Enabling ERP 9.0 Subsystems

To prevent excessive processing overhead during server startup and to prevent unnecessary uses of processor resources for ERP 9.0 subsystem jobs that might be in use, you must manually start ERP 9.0 subsystems. Generally, the system administrator or manager-level user is responsible for this task. To manually start ERP 9.0 subsystems, a version of an ERP 9.0 batch process with a processing option set to enable the use of subsystems is run.

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

Platform (Subsystem or Queue)	Description
AS/400 (JDENET)	One AS/400 subsystem is used for ERP 9.0. This subsystem is started automatically when you issue the ERP 9.0 startup command STRNET. The subsystem name is version-specific. For example, for release B73.1, the subsystem name is JDEB731. To process requests that are destined for ERP 9.0 subsystems, you must define a specific job queue running under the JDENET subsystem. For example, a job queue might be named QBATCH. User requests for ERP 9.0 subsystem-defined batch jobs are executed by the job queue that is based on definition in the AS/400 user profile.
UNIX (jdequeue)	One or more queues can exist for ERP 9.0. These queues can be named the same or differently. You define queues by parameters in the startup shell script `RunOneWorld.sh`. To process requests that are destined for ERP 9.0 subsystems, you must define one or more queues. For example, a jdequeue might be named QBATCH. User requests for ERP 9.0 subsystem-defined batch jobs are executed by the job queue, based on the process ID.
NT (`jde.ini` settings)	One or more queues can exist for ERP 9.0. These queues must have the same name. You define queues using settings in the `jde.ini` file. To process requests that are destined for ERP 9.0 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. User requests for ERP 9.0 subsystem-defined batch jobs are executed by the job queue, based on the process ID.

System administrators can display all of the ERP 9.0 subsystems that are running on a server by using the Subsystems Jobs application (P986113). Use this application to:

- Locate a list of ERP 9.0 subsystems that are running on a server.
- Locate a list of ERP 9.0 subsystem records that are unprocessed (not available for AS/400 servers).
- Locate the current record that a ERP 9.0 subsystem is processing (not available for AS/400 servers).
- Stop or delete any ERP 9.0 subsystem.

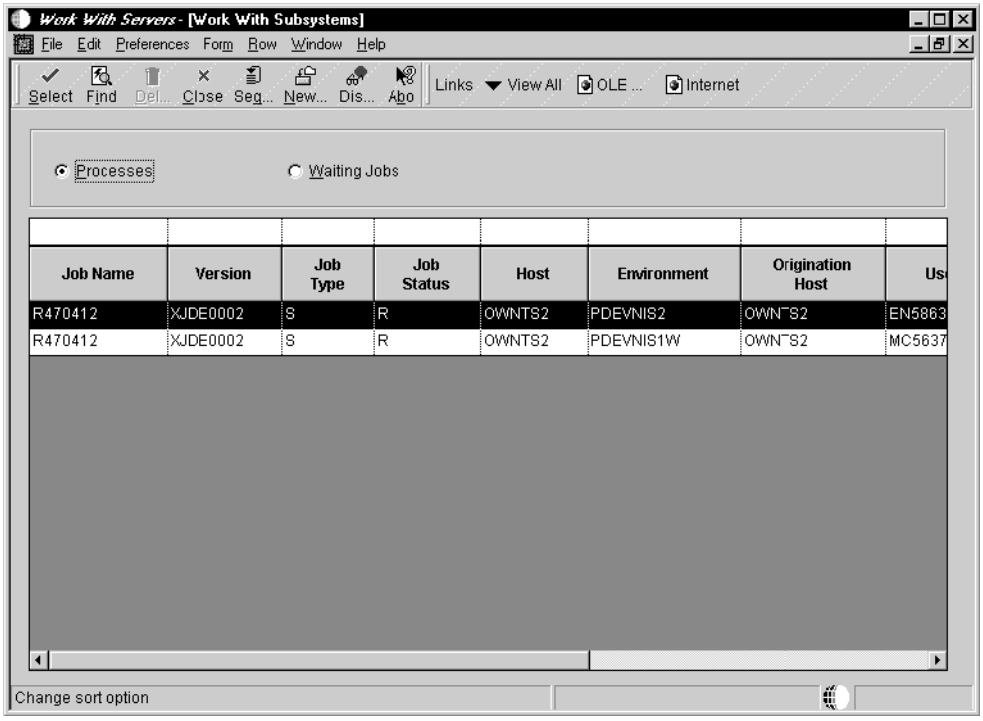
Locating ERP 9.0 Subsystems Running on a Server

You can use Work With Subsystems to determine which ERP 9.0 subsystems are currently running or waiting on a particular server. The running subsystems are identified by report number and version.

► To locate ERP 9.0 subsystems running or waiting on a server

On System Administration Tools (GH9011), choose Work with Servers (P986116).

1. On Work With Servers, choose a server from the list or use the query by example row to choose a specific server.
2. From the Row menu, choose Subsystem Jobs.



3. On Work With Server Jobs, turn on one of the 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. Thye are identified by an R (subsystem record) value in the Job Type field.

   All currently running ERP 9.0 subsystems are displayed. The status of each subsystem is shown by codes in the following fields:

   - Job Type

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

   - R, subsystem record
   - S, subsystem job

- Job Status

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

- W: subsystem record waiting
- P: subsystem record processing
- E: subsystem record to end the job
- R: subsystem job running

Reviewing Job Records for ERP 9.0 Subsystems

Multiple ERP 9.0 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.

Before You Begin

- Locate an ERP 9.0 subsystem job. See *Locating ERP 9.0 Subsystems Running on a Server* in the *System Administration Guide*.

► To view job records for ERP 9.0 subsystems

1. On Work With Subsystems, click Find.
2. Choose a record in the detail area, and then choose 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 ERP 9.0 Subsystems

You can use Work With Server Jobs to terminate ERP 9.0 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).

► To stop ERP 9.0 subsystems

On Work With Subsystems, locate a running subsystem.

1. Choose the running subsystem that you want to stop.
2. From the Row menu, choose 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. On End Subsystem Job, click OK.

► To end ERP 9.0 subsystems

On Work With Subsystems, locate a running subsystem.

1. Choose the running subsystem that you want to end.
2. From the Row menu, choose 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.

3. On End Subsystem Job, click OK.

User Profiles

A user profile defines a specific user to an ERP 9.0 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 ERP 9.0, 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 Solution Explorer.

Understanding User Profiles

You can use the User Profile Revisions application (P0092) to define specific users or ERP 9.0 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 ERP 9.0. 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 starting ERP 9.0.
- The language preference and country code for the text that displays on ERP 9.0's menus, forms, and country-specific applications.

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 that 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, ERP 9.0 takes the information from the role profile.

ERP 9.0 uses roles for the following purposes:

- Environments
- User overrides
- Application security
- Creation of sign-on security records

Tables Used by the User Profile Revisions Application

The User Profile Revisions application (P0092) uses the following 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

You can create user profiles one at a time by using the User Profile Revisions application (P0092), or you can simultaneously create multiple profiles by using batch processes. When you are ready to create user profiles for the first time, you might need to create hundreds of profiles. In this case, use the batch processes to create the profiles. If you only need to add a few users, use the User Profile Revisions application.

This section is a checklist for all the steps that are needed to add a new user. These steps do not include installing ERP 9.0 on a workstation or third-party setup issues such as assigning network user IDs.

Adding an Individual User

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

See Also

- *Address Book Maintenance* in the *Address Book Guide* for information on adding an address book record
- *Defining Machines* in the *Package Management Guide* for information on populating the machine table

See the following topics in the *System Administration Guide*:

- *Creating and Modifying User and Role Profiles* for information on adding a role profile
- *Understanding Signon Security* for information on adding up signon security
- *Understanding the Security Workbench* for information on security workbench overrides

► To add an individual user

1. If you plan to create a new role for the user that you are adding, 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 this new user, add a role profile.
3. Add an Address Book record for the new user.
4. Add a user profile.
5. Add signon security records for the user.
6. Add any security workbench 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 he or she belongs.

Adding Multiple Users

The following procedure shows the steps that you need to perform when you use the batch process to add multiple user profiles simultaneously. This batch process automates the process of user profile creation.

If you have the processing option for user profiles set to validate address book numbers, you should begin at step 1. If you do not have the processing option enabled, begin at step 2.

Note

See *Understanding Processing Options for User Profiles* in the *System Administration Guide* for additional information on validating address book numbers.

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

Signon security is not based on roles because individuals must have their own ERP 9.0 passwords. A program exists with signon security to quickly create individual security records by role; however, after the records are created, security is assigned by an individual. See *Working with Signon Security* in the *System Administration Guide* for information.

See Also

See the following topics in the *System Administration Guide*:

- *Creating and Modifying User and Role Profiles*
- *Creating Profiles By Using a Batch Process*
- *Setting Up User Profiles*
- *To run the User Profiles Summarization (R900921) report* for information on role profile summaries
- *Working with Security Workbench* for information on creating security workbench records
- *Understanding Signon Security* for information on creating signon security records

► To add multiple users

1. Using the Address Book Revisions application (P01012), create address book records for Roles that you will use in user profiles.
2. Using the User Profiles application (P0092), add the Role profiles.
3. Populate the various Address Book tables.

If you are migrating data from a non-ERP 9.0 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 User Profile Creation (R0092) batch process to create user profile records from existing Address Book records.

   Normally this report is based upon Address Book records with a search type for employees (E). You have the option of picking one default Role to put everyone in or running the report more than once to put people in different Roles.

5. Adjust each user's Role assignments.

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

   The following settings are dictated by Role:

   - Environments
   - User Overrides
   - Application Security

6. Run the User Profiles Summarization (R00921) batch process to view your new user profiles.
7. Create security workbench records for all Roles and any individual overrides to those Roles.
8. Create signon security records.

   You can create signon security records for all individuals within a Role by entering one record for the Role.

9. Manually populate the Machine/Group Identification table (F009650).

   This table is automatically populated each time a machine signs on to ERP 9.0. 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

You use the User Profile Revisions application (P0092) to set up user profiles. When you set up profiles as a system administrator, you create group profiles and user profiles for each user in the system. You also determine the environments that are available to each group and user, and set up display preferences, such as language.

► To set 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 the following preferences:

- Environments, to determine the environments that you want to be available to each Role or user.
- Display preferences, to determine ERP 9.0 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 your 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.

Creating and Modifying User and Role Profiles

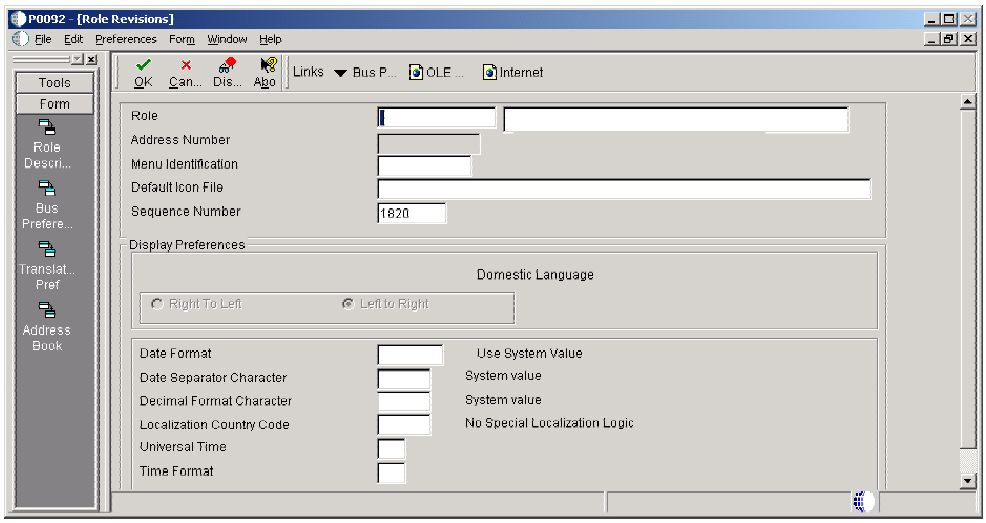
The system administrator needs to create a user profile for every user. The user profile defines certain setup and display features, such as access to fast path, language, date format, or country code. The administrator should first create all of the Role profiles that are needed for the enterprise. This action makes creating profiles easier; instead of defining specific environments, packages, and machine configurations to 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, ERP 9.0's menu filtering process displays for that user any special menu selections that are unique to that country code. For example, if you entered CA (Canada), that user sees the Canadian Tax Information application on the appropriate menu, which users without that country code would not see.

► To create and modify role profiles

On the System Administration Tools menu (GH9011), choose User Profiles (P0092).

1. On the Work With User / Role Profiles form, do one of the following operations:
   - If you want to create a new Role, click Add Role in the Form menu.
   - If you want to modify an existing profile, choose Roles Only, click Find, choose a role in the detail area, and then click Select.



2. On the Role Revisions form, complete or modify the following fields, as necessary.
   - Role

     Enter the name of the Role, such as ACCOUNTING.

     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.

   - Enter a Description for the Role.
   - Address Number

     Enter an Address Book number if the role will be used with a workflow

   - Sequence Number
   - You can enter a sequence number, or the system will automatically add one for you

     The sequence number determines where in the Role hierarchy this role will be.

     - Menu Identification
     - Default Icon File
3. Click OK.

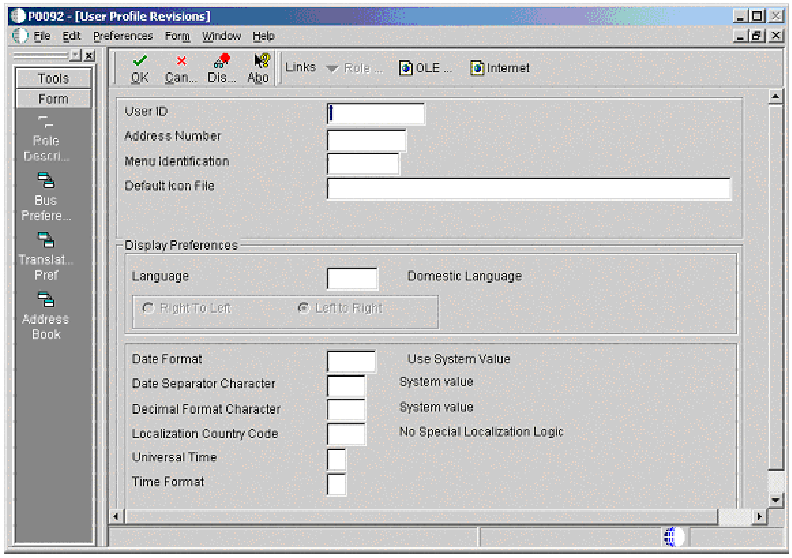
Copying User and Role Profiles

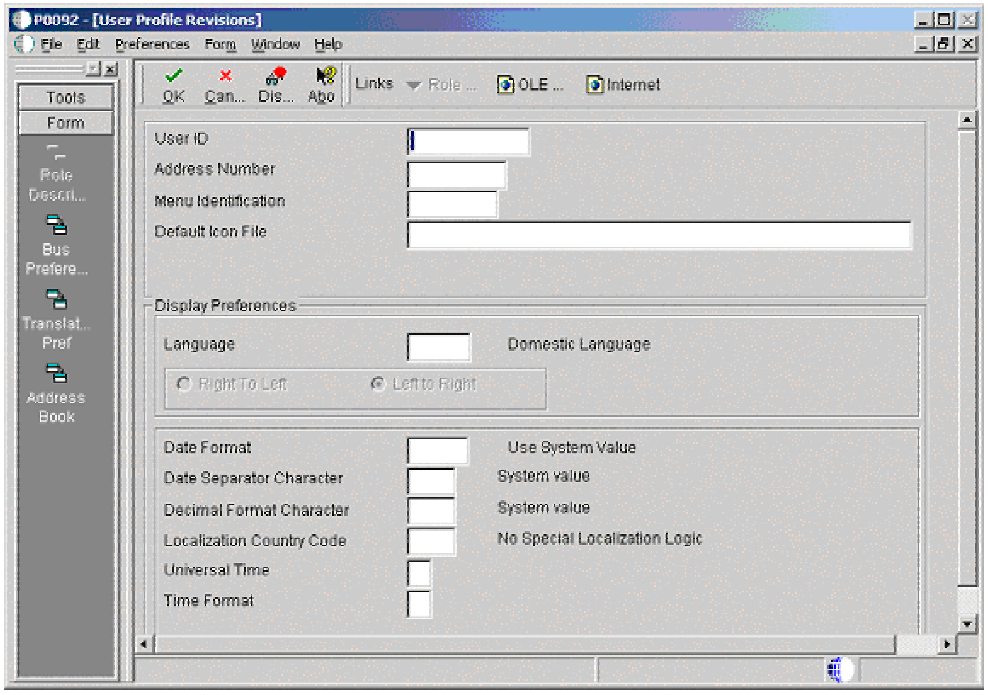
You can copy all or part of a user profile. When you copy an entire user or role profile (display and environment preferences), you are creating a new user profile with the information from another profile. When you copy part of a user profile, you are copying the environment preferences from another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

► To create and modify user profiles

On the System Administration Tools (GH9011) menu, choose User Profiles (P0092).

1. On the Work With User/Role Profiles form, do one of the following operations:
   - If you want to create a new user profile, click Add.
   - If you want to modify an existing profile, click Find, choose a User profile in the detail area, and then click Select.





2. On the User Profile Revisions form, in the header area, do one of the following to create an individual profile:
    - To create an individual profile, do the following:
        - In the User ID field, enter the user ID for the individual.

          When you modify a user profile, this field displays the user ID.

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

3. In the header area of the form, complete the remaining fields.
    - Address Number
    - Menu Identification
    - Default Icon File
4. If you are creating a User Profile, in the Display Preferences box complete the following fields, and then click OK:
    - Language
    - Date Format
    - Date Separator Character
    - Decimal Format Character**To copy user or role profiles**

On the System Administration Tools menu (GH9011), choose User Profiles (P0092).

1. On the Work With User / Role Profiles form, locate a user profile, and do one of the following:
    - To copy an entire profile (the display, environment, and deployment preferences), click Copy.

      The User Profile Revisions form appears. Because this creates a new profile, the user profile that you create cannot already exist in ERP 9.0.

    - To copy environment preferences, from the Row menu, choose 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 ID field, enter a user ID or Role name to copy the profile into, and change any other information.
3. Click OK when you are finished.

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 ERP 9.0. 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

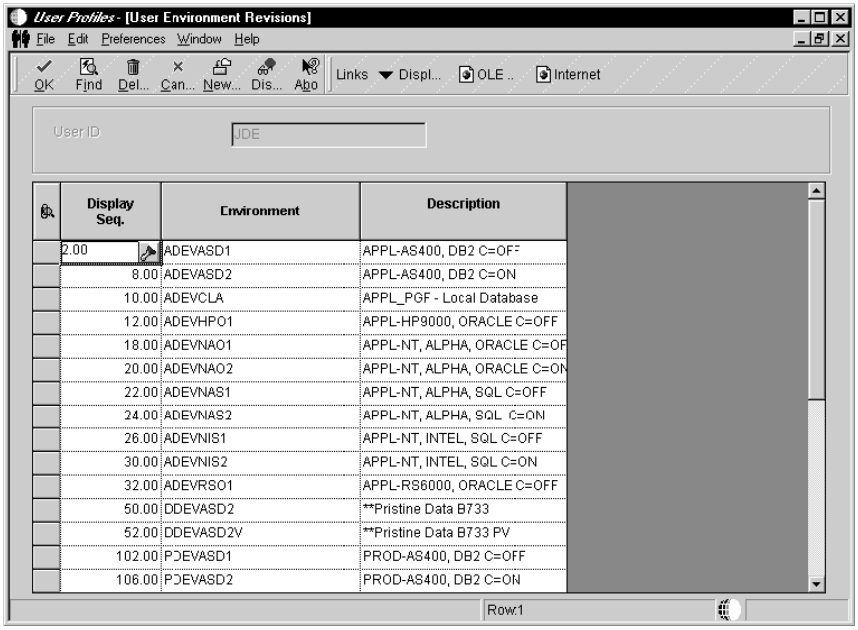
user starts ERP 9.0. You can assign more than one environment from which a user can choose, or delete environments if they are no longer relevant to the user.

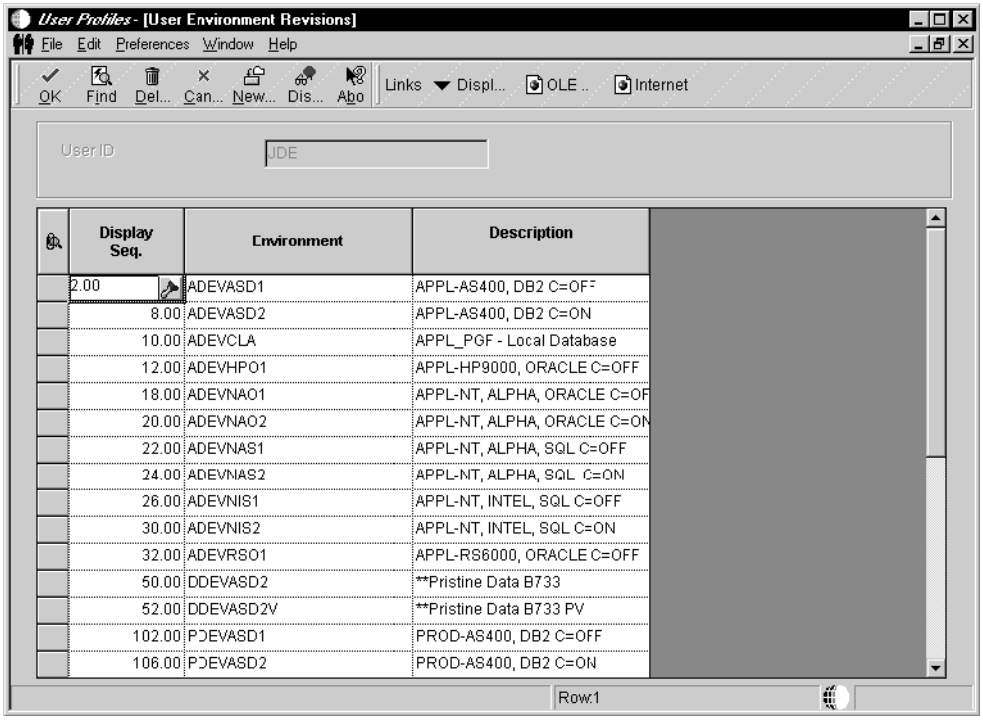
► To assign or delete environments

On the System Administration Tools menu (GH9011), choose User Profiles (P0092).

1. On Work with User / Role Profiles, click Find, and then choose a user profile.
2. From the Row menu, choose Environments.

   The User Environment Revisions form appears. This form displays the list of environments available for a particular Role.





3. To add a new environment, complete the following fields on the last row:
    - Display Seq.
    - Environment
4. To delete an environment from the list, choose the environment and click Delete.
5. On the Confirm Delete form, click OK.

Assigning Business Preferences to User and Role Profiles

You can assign business preferences to user profiles to create customized processes with the ERP 9.0 Workflow application. You define the codes for the preferences based on industry, business partner, or customer. You need 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. The Workflow process might send a message, update a database, or start another application.

See Also

- *Creating Workflow Processes* in the *Enterprise Workflow Management Guide* for more information about setting up a workflow process

► To assign a business preference to user and role profiles

On the System Administration Tools menu (GH9011), choose User Profiles (P0092).

1. On Work with User / Role Profiles, click Find.
2. Choose a user profile, and then click Select.

   The User Profile Revisions form appears.

3. From the Row menu, choose Business Preferences.

   The Business Preferences form appears.

4. Complete any of the following 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.

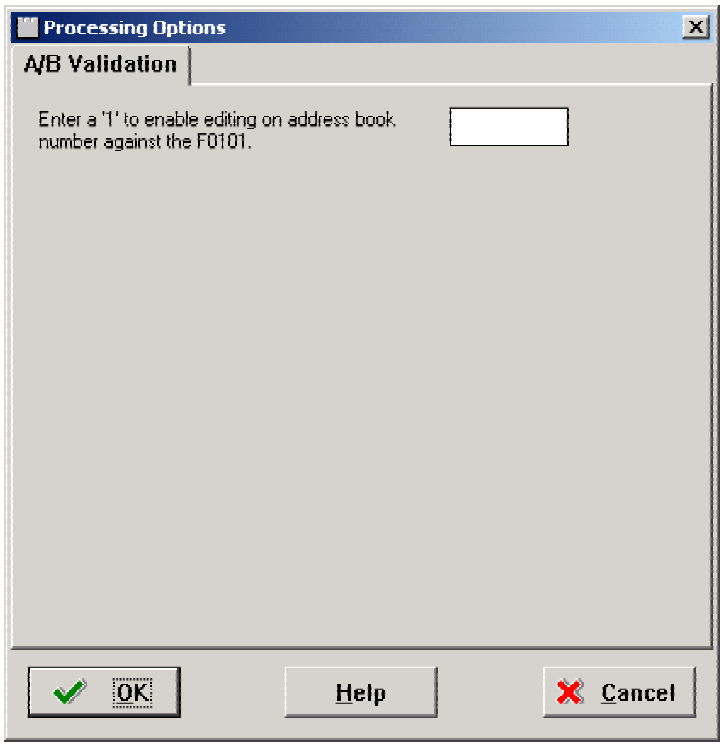
   - Customer Code

   This field associates the user profile with a specific customer.

Note
You can click Cancel on the Business Preferences form to cancel the addition of the current business preference.

Processing Options for User Profiles

The User Profile Revisions application (P0092) has the following processing option:



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 causes User Profiles to validate, upon creation of a user profile, each new user ID against the Address Book Master table (F0101). As a result, you cannot create a user profile for a user who is not already defined in the Address Book Master table. J.D. Edwards recommends 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 Address Book Master table.

See Also

- *Setting Up User Roles* in the *System Administration Guide* for a discussion of roles

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 your Address Book and user profile records, and ease the transition of taking ERP 9.0 to production.

You can create user profiles through the Populate User Profiles batch process (R0092). With this process, you can assign display and environment preferences to users. This process allows 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 (P0092).

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

Before You Begin

- Create all of the role profile information by using the User Profile Revisions application.
- Defined the following:
  - Role profiles
  - Environments that the roles can access

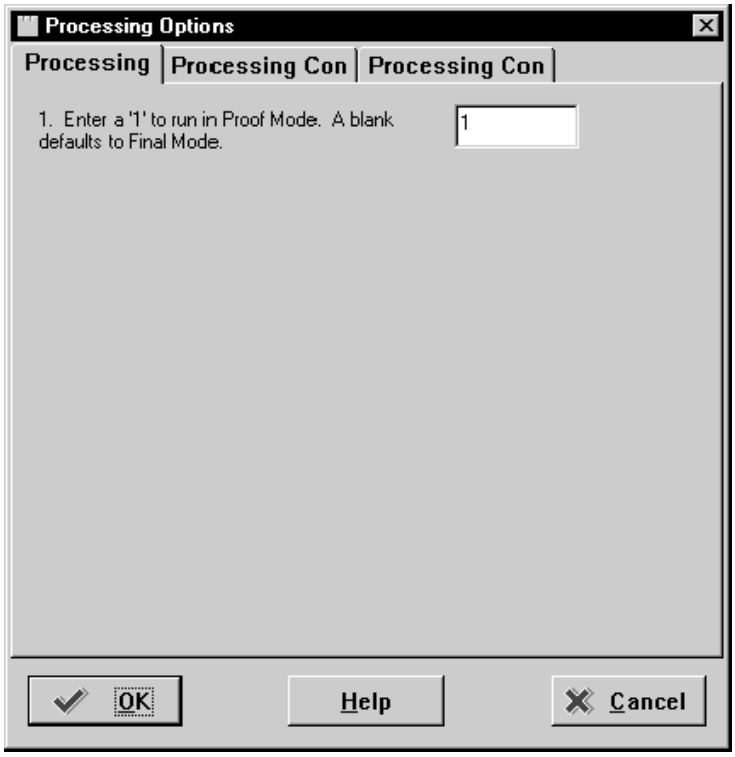
► To run the Create User Profiles from A/B Records (R0092) batch application

On the Advanced Operations menu (GH9012), choose Create User Profiles from A/B Records (R0092).

1. On the Work With Batch Versions form, choose the J.D. Edwards default version (XJDE0001) or the equivalent for your installation, and then click Select.
2. On the Versions Prompting form, click Data Selection, and then click Submit.
3. 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 above form, the Processing Options form appears.



4. On the Processing Options form, enter the following information:
   - Option 1; enter one of the following values:
     - 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 you specified and creates a report showing the profiles created.
   - Option 2; enter one of the following values 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.

     Note
     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 the following user profile fields for Option 2:

     - Fast Path
     - Language
     - Date Format
     - Data Separator Character

- Data Format Character
- Country

- 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.

► To run the User Profiles Summarization (R900921) report

On the Advanced Operations menu (GH9012), choose Summarize Role Profile Information (R900921).

1. On the Work With Batch Versions form, choose a version and click Select.

   The J.D. Edwards default version XJDE0001 creates a report for all role profiles in the enterprise. The J.D. Edwards 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

After you have set up user profiles, you can assign roles to the users in your organization. A role defines the tasks that a user sees when he or she works in a task view of the Solution Explorer. You also use roles to define a user's permissions within ERP 9.0. You can customize each role to provide the appropriate level of access to ERP functions.

Assigning roles accomplishes the following purposes:

- Users see only those tasks and perform only those activities that relate to their jobs. For example, a user playing the role of A/P clerk might not need to see all the tasks that an A/P manager would need to see. You can create both of these roles and define a different set of tasks for each one.
- Users can play multiple roles. Within an organization, a user might have many responsibilities, no one of which can be defined by a single role. A user who has been assigned multiple roles can switch roles, according to the work required.
- Administrators can set up ERP 9.0 security that is 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 he or she has been assigned.

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

Administrative Step	Application Used	Form used	Tables Used
Populate User Profile table with roles that are stored in UDC H95/RL during Roles Phase I	R89959211, R89959212	N/A	F00926, F0092
Run UBE to populate Role Relationships table	R8995921	N/A	F0092, F95921
Define roles	P0092 (User Profile Revisions)	W0092A (User Profile Revisions); Form exit from the Work With User Profiles form (W0092D)	F0092
Sequence roles	P0092	W0092L (Work With Role Sequences); Form exit from the Work With User Profiles form	F00926
Create role relationships tying users to 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, Solution Explorer, and ERP 9.0 client workstations use the role relationships data in the Role Relationships Table (F95921) and various APIs to retrieve data and allow users to play assigned roles.

Migrating Roles for ERP 9.0

On a client machine, open the Batch Versions application in ERP 9.0, and run the following Universal Batch Engines (UBEs) to migrate generic roles into your ERP 9.0 environments.

Set Up Roles

Run the UBE R89959212

Universal Batch Engine (UBE) R8959212 populates the Library Lists - User table (F0092) and the Anonymous User Access Table (F00926) from the roles and descriptions that have been previously set up in the user defined code (UDC) H95/RL. This UDC was used for Phase I and is now being removed.

Processing Option

None

Performance

The performance of this UBE is directly dependant upon how many records are in the User Defined Codes table (F0005) and the User Defined Codes – Alternate Language Descriptions table (F0005D) under the UDC H95/RL. It should finish quickly.

Once complete, the UBE produces a report (in our system, roughly two pages long). The UDC H95/RL must be manually removed.

Note

See portable document format (PDF) in `G:\OneWorld_Documentation\SMT\OET\Project Management\Project Folders\Roles\Phase II\Other` for details.

Run the TC R89959211

TC R89959211 takes all of the current groups in the UGRP field in the Library Lists – User table (F0092) table 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 Anonymous User Access Table (F00926) record as well. This sequence number begins at 1500 and increments by 5 with each record that is written.

Processing Option

None

Performance

The performance of this UBE is directly dependent upon the number of *GROUP records in the Library Lists – User table (F0092). It should finish quickly.

Once Complete

This table conversion (TC) produces no PDF. To verify that the table conversion completed, open the Universal Table Browser (UTB) and check the Anonymous User Access Table (F00926) for some of the groups that are defined in the Library Lists – User table (F0092). 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 Profiles records in the Library Lists – User table (F0092) and inserts a User/Role Relationship Record that is based on the User ID (F0092.USER) and Group (F0092.UGRP). The record that is added to the Role Relationships Table (F95921) contains the User, Role (formerly the Group for this user in the Library Lists – User table (F0092)), and Effective and Expiration Dates. Some of these values are based upon the values in the Processing Options.

Processing Options

See the recommended Processing Options values below:

- Final/Proof Modes

  J.D. Edwards recommends that the TC be run in Proof Mode first. This mode inserts records to the Role Relationships Table (F95921), but it does not remove the Group from the Users Profile. Once the UBE is successfully run in Proof Mode, check some of the records in the Role Relationships Table (F95921) 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 Library Lists – User table (F0092)), you want to use the date of the day that the TC is run. (When running in Final Mode, use the date that the TC was run in Proof Mode so you do not insert a new set of records into the Role Relationships Table (F95921.) This field must not be modified within the Role Relationship Record at a later date.

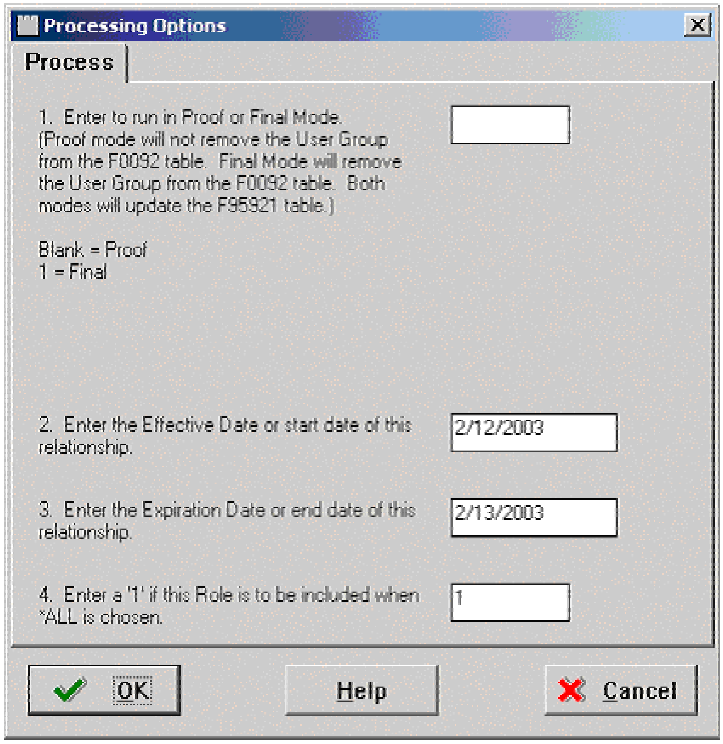
- Expiration Date

  The end date of the Role Relationship. If this date is left blank, the relationship never expires. With the current users (those in the Library Lists – User table (F0092)), you probably want to leave this blank so they do not expire from their current group or role.

  This field can be modified within the Role Relationship Record at a later date.

- Included In All

  This flag indicates that the security of this role is applied when the user chooses to enter ERP 9.0 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 at a later date.



- Performance

  The performance of this UBE directly depends upon how many user records are in the Library List – Users Table (F0092). It should finish quickly.

- Once Complete

  This processing option is a TC, so no PDF is produced. To verify that the TC completed (in Proof Mode), open the UTB and check the Role Relationships Table (F95921) for some of the users who were defined in the Library Lists – Users table (F0092). 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 Library Lists – Users table (F0092) through 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 Library List – Users table (P0092) Application exit "Sequence Roles." This application displays all of your 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-on, 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 the following 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 ERP 9.0.

[DB_SYSTEM SETTINGS]

DefaultRole=*ALL
```

Server Executables

Run a PortTest.

Set up Security

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

Run the UBE R98OWPU

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

Note

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

Processing Options

None

Performance

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

Once Complete

To verify that the UBE completed successfully, open the UTB and check the OneWorld System Users table (F98OWPU) for some of the Proxy Users that are in One World Security table (F98OWSEC).

Benefits

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

Run the UBE R98OWUP (Optional)

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

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

Processing 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 is the maximum number of days before the system requires a password change.

- Allowed Attempts

  The number of times that a user can unsuccessfully attempt to log on before his or her ERP 9.0 account is disabled.

- Enable/Disable User

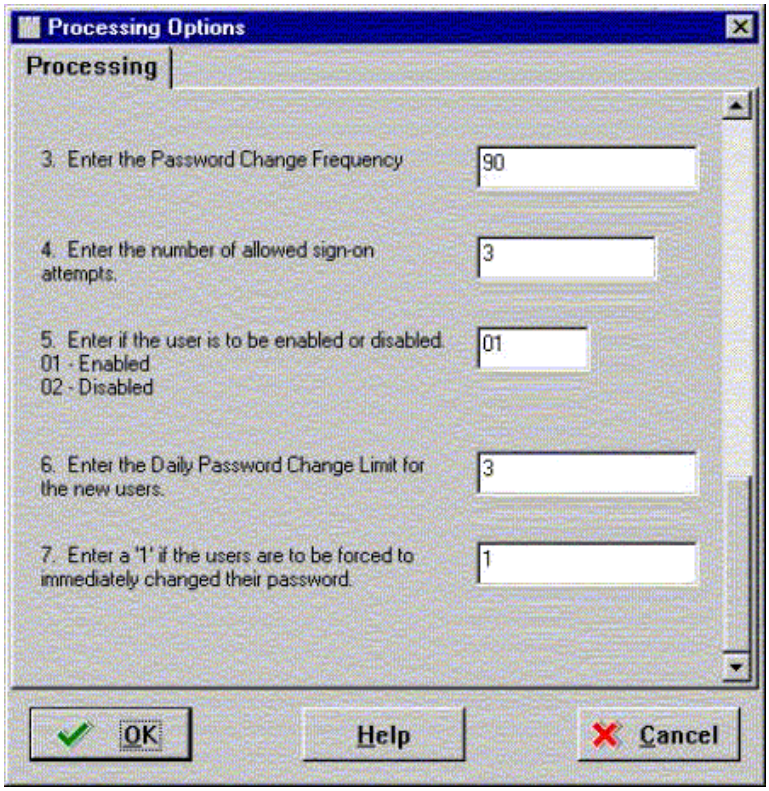
  Indicates if the user's account is enabled or disabled. A disabled account is not allowed into ERP 9.0.

- Daily Password Change Limit

The number of times that a user can change his or her 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 the user to immediately change his/her password. You probably do not want to set this option for all users.



Performance

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

Once Complete

To verify that the UBE completed successfully, go to the OneWorld 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 setting up your system, you must define the roles for users in your organization. These roles define the tasks that users see when they work in the Solution Explorer and

determine what authority the users have in ERP 9.0. After you have defined a role, you can associate users with it and apply security to it.

ERP 9.0 stores your role descriptions in the Anonymous User Access Table (F00926). If you previously defined roles using the user defined code (UDC) H95/RL table, you can run the Populate Role Descriptions From F0092 report (R89959211) to populate the Anonymous User Access Table (F00926) with those older role descriptions.

See Also

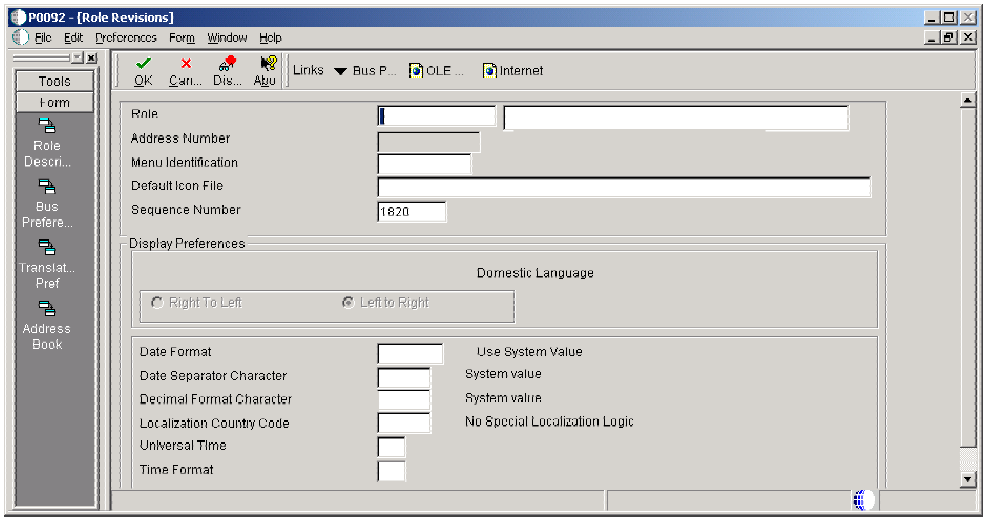
- *Task Setup* and *Applying Roles to a Task* in the *Solution Accelerator Suite Implementation Guide* for information about associating tasks and task relationships to a role
- *Working with Security Workbench* in the *System Administration Guide* for information about setting up security for roles

► To define a role

On the Systems Administration Tools menu (GH9011), choose User Profiles (P0092).

1. In the Work With User / Role Profiles form, on the Form menu, choose 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 the following 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/Roles 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 allows you to change the properties of the role, including its description, address number, and menu identification.

► To revise roles

On the Systems Administration Tools menu (GH9011), choose User Profiles (P0092).

1. On the Work With User/Roles Profiles form, choose the Roles Only option.
2. Choose a role that you want to revise and click Select.
3. On the Role Revisions form, make needed changes and click OK.

Sequencing Roles

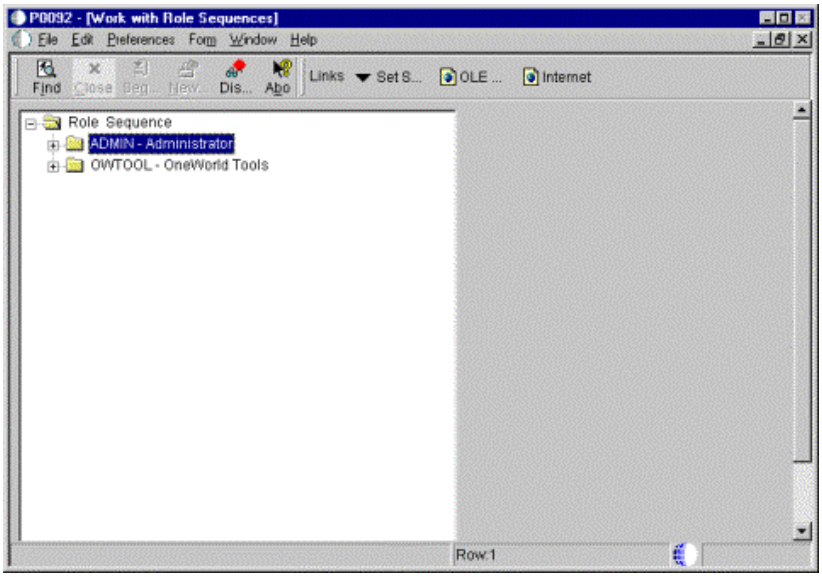
The Work With Role Sequences form contains all of the roles that you defined and allows you to assign a sequence to each role. The sequence defines a hierarchy of roles and determines which role is active when a security conflict exists among a user's roles.

To sequence roles, you use the User Profile Revisions application (P0092).

► To sequence roles

On the Systems Administration Tools menu (GH9011), choose User Profiles (P0092).

1. From the Form menu, click Role Sequence.



2. On the Work With Role Sequences form, choose a role from the tree structure and drag it to the point in the sequence that you want.
3. After you have set the order you want, choose Set Sequence from the Form menu and click Close.
4. If you decide you do not want to change the sequence, choose 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 (P0092). In this application, you can assign one or more environments to each role. Then when the user signs on to ERP 9.0, the Environment Chooser and Role Chooser presents 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 Also

- See *Choosing Roles for Display at Signon* in the *System Administration Guide* for further discussion of roles and environments

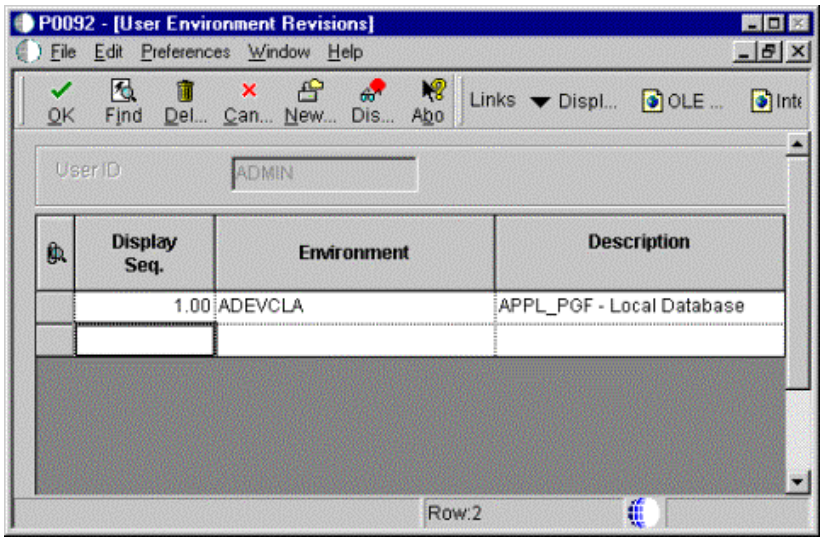
► To add an environment to a role

On the Systems Administration Tools menu (GH9011), choose User Profiles (P0092).

1. On the Work With User/Role Profiles form, choose 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. Choose a role from the detail area of the grid, and choose Environments from the Row menu.



3. On the User Environment Revisions form, complete the following fields and click OK:

   - Display Seq.

     This value specifies the order in which the environments will be presented in the Environment Chooser at ERP 9.0 log-on.

   - Environment

     You can choose from a list of valid 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 Role Relationships

A role relationship ties a user to 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 allows you to add, remove, or revise a role relationship for a user.

Creating a Role Relationship

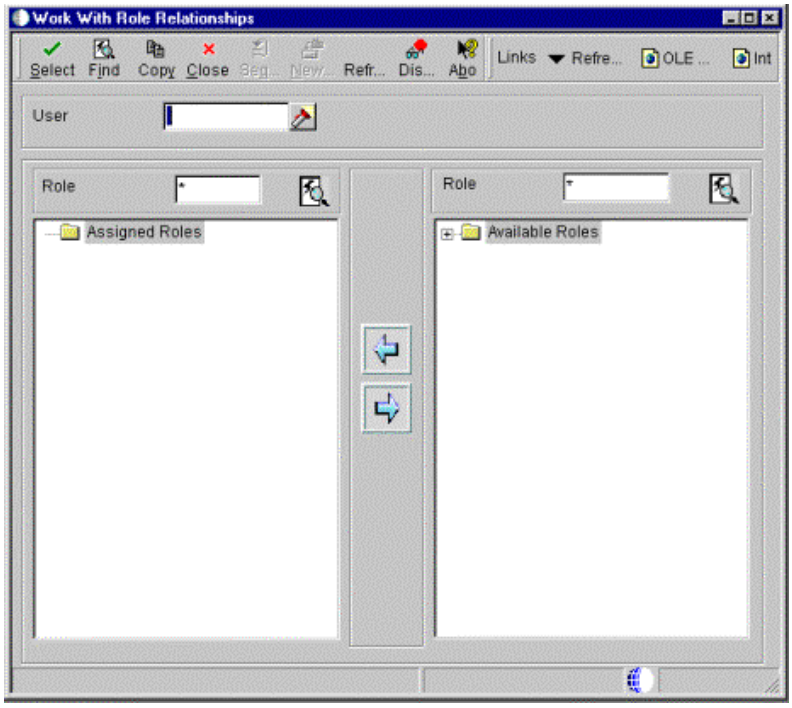
After you have defined a role, you use the Work With Role Relationships form to tie a user to the role. Adding the role to the user's list of assigned roles means that the user is able to choose the role at signon by using the Role Chooser. The Role Chooser is a visual assist button on the ERP 9.0 signon screen that displays a user's assigned roles. You can limit the freedom a user has to choose roles by disabling the Role Chooser. With the Role Chooser disabled, the user must enter ERP 9.0 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.

► To create a role relationship

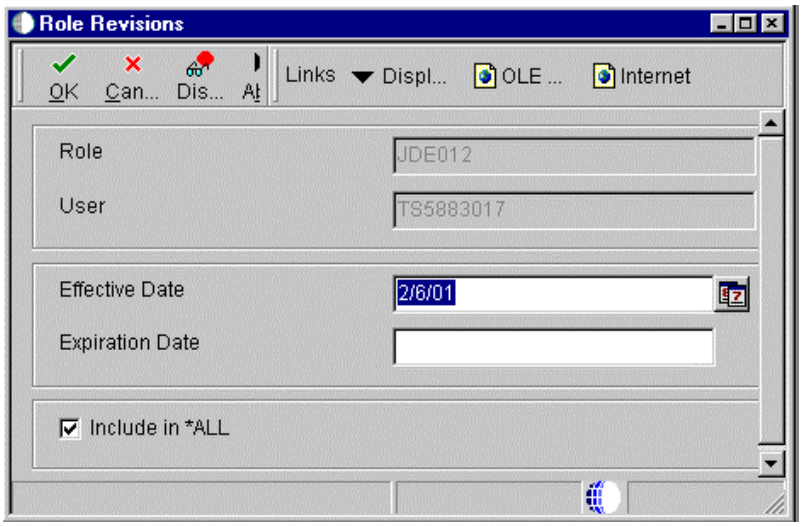
From the Fast Path In the Solution Explorer, launch the Roles Relationships application (P95921).



1. On Work With Role Relationships, complete the User field and click Find.

   ERP 9.0 displays the user's assigned roles and the available roles in separate tree controls.

2. Choose 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 or ERP 9.0 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.

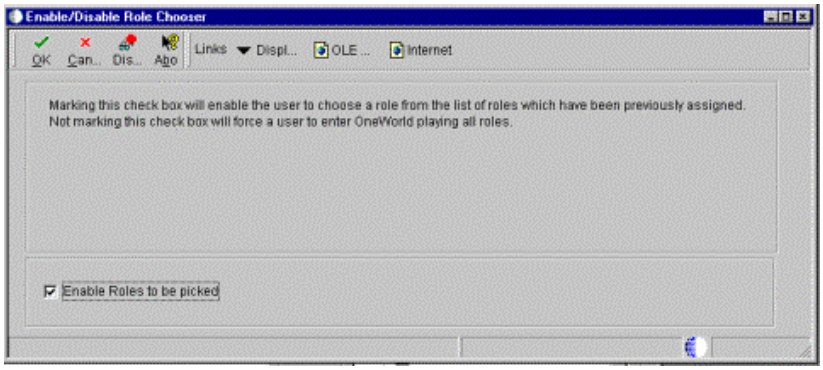
5. Turn on the Include in ALL* option if you want the role to be one that the user can play if he enters ERP 9.0 playing all roles, and click OK.

   If you do not choose the Include in *ALL option, this role will not be part of the active roles when the user enters ERP 9.0 using *ALL as his role at log-on. To activate a role not included in *ALL, the user must choose that particular role when logging on to the system. The chosen role will be the only active role during that session.

► To enable the role chooser

From the Fast Path In the Solution Explorer, launch the Roles Relationships application (P95921).

1. On Role Relationships, from the Form menu, choose Enable Role Chooser.



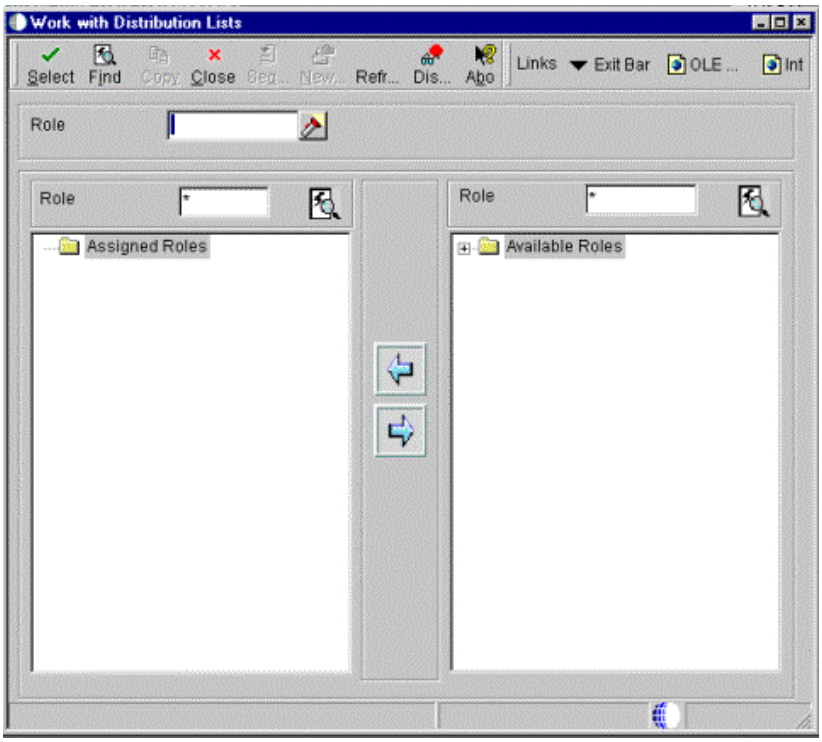
2. On Enable/Disable Role Chooser, turn on the Enable Roles to be picked option if you want the user to choose the new role from a list of all assigned roles at log-on, and click OK.

   If you do not choose this option, the user must enter ERP 9.0 playing all assigned roles (*ALL).

► To create role-to-role relationships

From the Fast Path In the Solution Explorer, launch the Roles Relationships application (P95921).

1. From the Form menu, chose 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, choose a role from the Available Roles tree control and click the left-arrow button.
4. On Role Revisions, complete the following 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. Choose the *ALL option if you want the role to be one that the user can play if she enters ERP 9.0 playing all roles.

   ERP 9.0 adds the role to the Assigned Roles tree control.

6. To remove a role from the distribution list, choose a role from the Assigned Roles tree control and click the right-arrow button.

Note
ERP 9.0 does not currently support multi-level 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.

► **To revise a role relationship**

From the Fast Path In the Solution Explorer, launch the Roles Relationships application (P95921).

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

Workstation Initialization File Parameters

At ERP 9.0 signon, users can choose one or more roles to play, depending on how many you have assigned to them. If users choose *ALL, they enter ERP 9.0, playing all assigned roles. Two parameters that relate to roles are in the workstation jde.ini file. The table below displays the parameters, the workstation .ini file section in which they are found, and the default settings:

Jde.ini Parameter	Jde.ini Section	Default Setting
LASTROLE	[SIGNON]	*ALL
Default Role	[DB SYSTEM SETTINGS]	*ALL

The LASTROLE parameter value defines the role that appears in the signon screen when ERP 9.0 is launched.

Note

See *Choosing Roles for Display at Signon* in the *System Administration Guide* for more information.

Choosing Roles for Display at Signon

Once the administrator has defined roles and created role relationships, users can sign on to ERP 9.0 by using the Role Chooser if this feature is activated. At the ERP 9.0 signon form, the user enters a user ID and password. The user must then enter a valid environment and role before entering ERP 9.0.

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.

The following table summarizes the scenarios that can occur when the user encounters the Environment and Role fields at signon, and ERP 9.0's behavior in each scenario:

Signon Scenario	ERP 9.0 Behavior
User enters values in both the Environment and Role fields.	ERP 9.0 validates the role against the environment. If the role is not valid for the chosen environment, the Environment Chooser appears; the user must choose an environment that is valid for the role.
User enters a value only in the Role field.	The Environment Chooser appears, containing only the valid environments for the chosen role.
User enters a value only the Environment field.	The Role Chooser appears, containing 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.	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. If you do not enter an environment, the Role Chooser displays the roles that are assigned to the default environment that is defined in the jde.ini file.

Delegating Roles

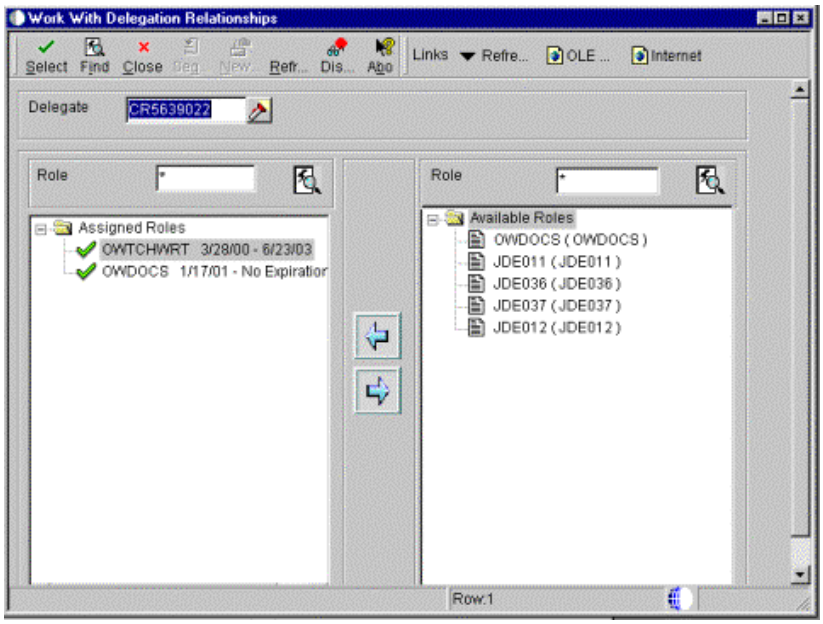
You can delegate your role relationship records to other users by using the Work With Delegation Relationships form. You might want to delegate one or more of your roles to another user if you are going to be out-of-town and you want your work to be taken care of while you are gone.

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

► To delegate roles

From the Fast Path In the Solution Explorer, launch the Roles Relationships application (P95921).

1. From the Form menu, choose 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, choose the role from the Available Roles tree control and click the left-arrow button.
4. Complete the following 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. Choose the *ALL option if you want the role to be one that the user can play if he enters ERP 9.0 playing all roles.

   ERP 9.0 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 attempt to remove a role that you did not delegate to the user, ERP 9.0 displays a dialog box notifying you that the action is invalid.

Creating Role-to-Role Relationships

The Work With Distribution Lists form enables you to create lists of roles that are subsets of a larger role. For example, you might create an ADMIN role that includes those users with the greatest number of administrative responsibilities and the broadest access to applications in ERP 9.0. You might also create several other roles that include individuals with more limited administrative responsibilities and access to fewer applications in ERP 9.0. If you create a distribution list that is 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.

Using the Work With Distribution Lists form, you can add or remove roles from the distribution list as needed.

Administering Roles

ERP 9.0 is used to administer defined roles for which you have created role relationship records. You can quickly 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 ERP 9.0 to specify the language that is used for the description of a new role.

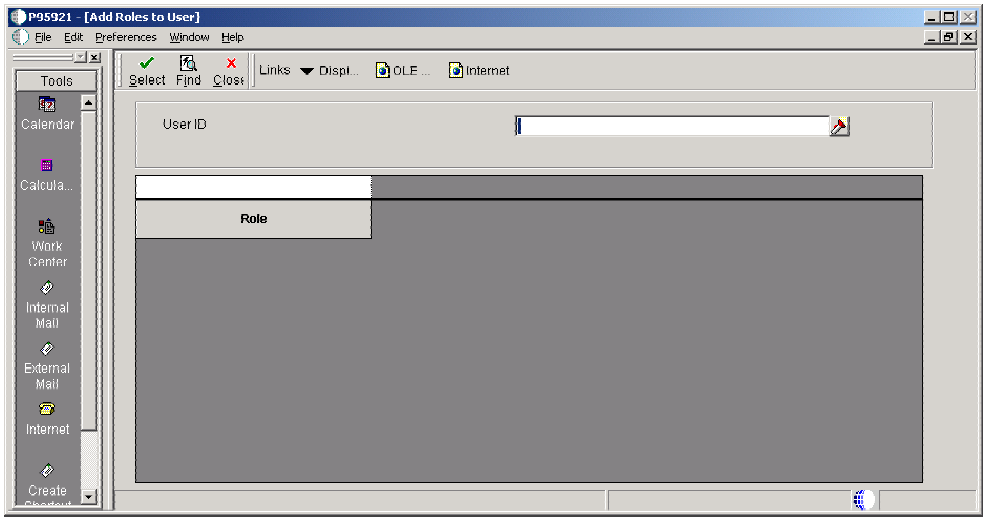
Adding Roles to a User

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

▶ To add roles to a user

From the Fast Path In the Solution Explorer, launch the Roles Relationships application (P95921).

1. From the Form Exit menu, choose Add Roles to User.



2. Complete the User ID field and click Find.
3. Choose the roles that you want to add to the user and click Select.

   Hold down the Control key to choose more than one role to add.

4. On the Role Revisions form, complete the following fields:

- Effective Date
  Enter a date if you want the effective date to be different than the current date.
- Expiration Date

5. Choose the *ALL option if you want the role to be one that the user can play if she enters ERP 9.0 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 you are adding.

Adding Users to a Role

The Add Users to Roles form allows you to add one or more users to a role relationship record. This action is particularly useful if you want to assign many users to a single role.

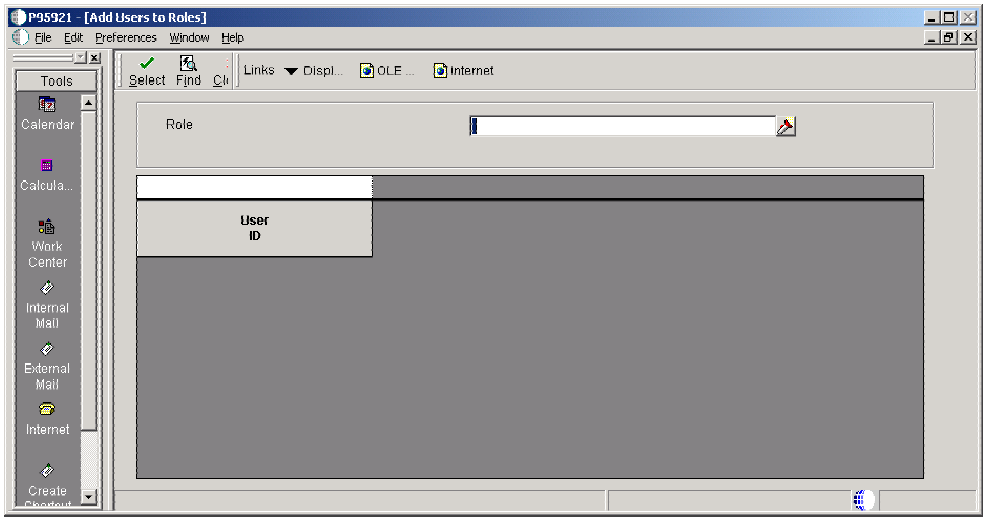
Copying User Roles

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 ERP 9.0 adds the copied records to the user's existing records; or you can copy and replace, which means that the copied records replace the user's existing records.

▶ To add users to a role

From the Fast Path In the Solution Explorer, launch the Roles Relationships application (P95921).

1. Choose Add Users to Roles from the Form menu.



2. Complete the Role field and click Find.
3. Choose the users that you want to add to a role and click Select.

   Hold down the Control key to choose more than one user to add.

4. In the Role Revisions form, complete the following fields:

- Effective Date

  Enter a date if you want the effective date to be different than the current date.

- Expiration Date

5. Choose the *ALL option if you want the role to be one that the user can play if he enters ERP 9.0 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.

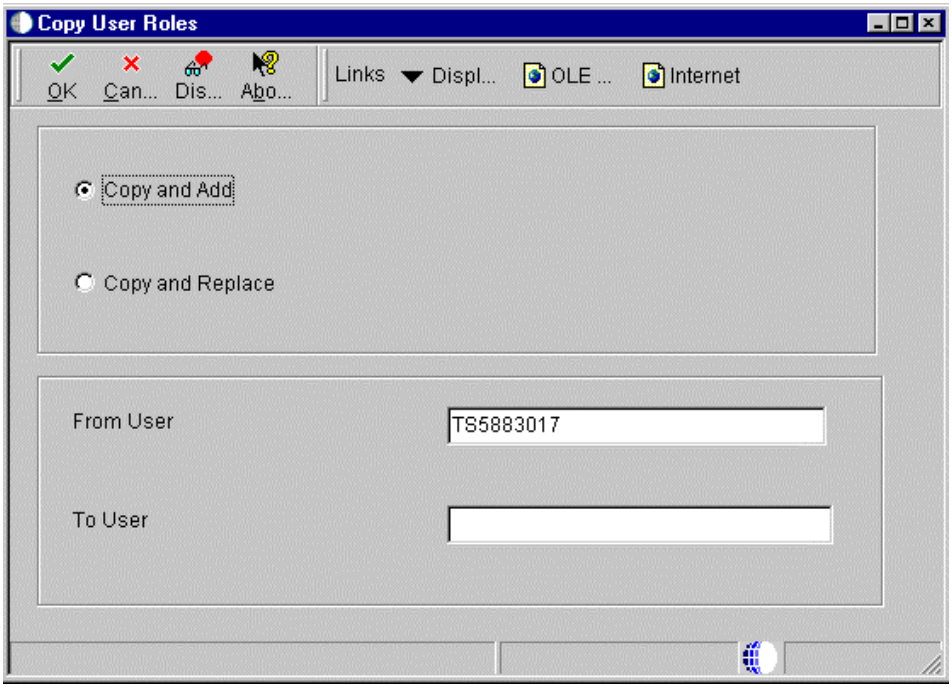
► To copy user roles

From the Fast Path In the Solution Explorer, launch the Roles Relationships application (P95921).

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, choose one of the following 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.

Revising Language Role Descriptions

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.

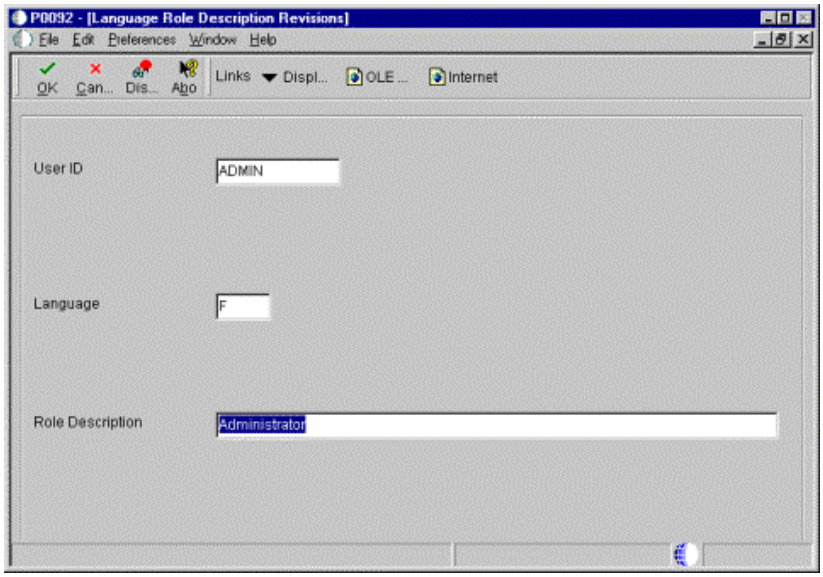
▶ To add a language translation to a role

On the Systems Administration Tools menu (GH9011), choose User Profiles (P0092).

1. On the Work With User / Role Profiles form, turn on the Roles Only option.

Note
The option Both Users and Roles option also allows you to perform this task.

2. Choose a role from the detail area of the grid and, from the Row menu, choose Role Description.
3. To add a language to a role, click Add.



4. On Language Role Description Revisions, complete the following 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

► To change a role description

On the Systems Administration Tools menu (GH9011), choose User Profiles (P0092).

1. Choose the Roles Only option from the Work With User / Role Profiles form.
2. Choose a role from the detail area of the grid and, from the Row menu, choose Role Descriptions.
3. On the Work With Language Role Descriptions form, click Find.
4. Choose 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.

Initialization File Modifications

At your ERP 9.0 signon, you can choose one or more roles to play, depending on how many have been assigned to you. If you choose *ALL, you enter ERP 9.0 playing all of the assigned roles that are flagged as Include in *ALL. Two parameters relate to roles in the workstation jde.ini file. The table below displays the parameters, the .ini file section in which they are found, and the default settings. These settings are defined by the administrator when ERP 9.0 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 signon.
Default Role	[DB SYSTEM SETTINGS]	*ALL

See Also

- *Choosing Roles for Display at Sigon* in the *System Administration Guide* for more information on choosing roles at signon

Security

ERP 9.0 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 the following features:

- Application security

  Controls access to or installation of specific applications.

- 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. Columns are represented in ERP 9.0 as a field on a form or report. Column security can be set on a table, form, or application.

- Processing option security

  Controls whether users can view or change the values for processing options, which affects how the associated application 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 Solution Explorer features.

- Miscellaneous security

  Controls Read Only Reports and Workflow status monitoring.

- User signon and database security

  Prevents user access to the database from outside of ERP 9.0.

- Portal security

  Controls access to Portal components.

The Security Workbench application (P00950) uses the Security Workbench Table (F00950).

The OneWorld Security application (P98OWSEC) uses the One World Security table (F98OWSEC).

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 the Security Workbench

The Security Workbench application (P00950) allows you to set up security for users, roles, and *PUBLIC. ERP 9.0 stores security information in the Security Workbench Table (F00950) and caches the security information in each workstation's memory. Changes that you make as an administrator to security are applied by each workstation after the user logs out and logs 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 an ERP 9.0 application. You can also secure objects within ERP 9.0, thus preventing some users from accessing forms or tables, and you can apply object-level security by user.

Understanding Users, Roles, and *PUBLIC

The ERP 9.0 security administrator can set up security for:

- A particular user

  This option controls security by a specific ERP 9.0 user ID.

- A user Role

  This option controls security by role, which allows you to group users who are 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 the ID type *PUBLIC in the User or Role field. The designation *PUBLIC is a special ID within ERP 9.0 that automatically includes all of the users within it. You can use this ID to apply security even if you do not specifically have a record set up for it in user profiles.

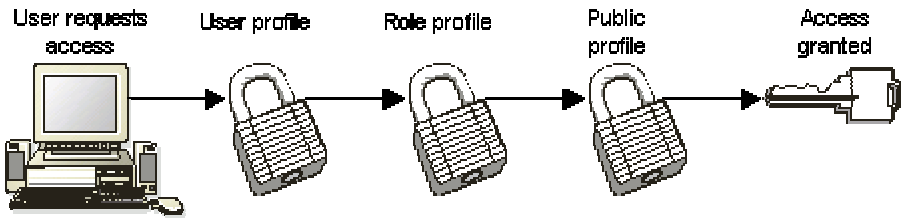
Understanding How ERP 9.0 Checks Security

When a user attempts to access an application or perform an action, ERP 9.0 checks for any security for that particular user ID. If security exists for that individual user ID, ERP 9.0 displays a message informing the user that he or she cannot proceed.

If that User ID has no security, ERP 9.0 checks the 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, ERP 9.0 lets the user continue.

ERP 9.0 also provides software license security through protection codes, and requires user validation at signon and when accessing new data sources.

Understanding How ERP 9.0 Checks Security



Understanding Cached Security Information

ERP 9.0 caches certain security information from the Security Workbench Table (F00950). This information is cached in the workstation's memory cache for ERP 9.0. If system administrators make changes to the Security Workbench Table (F00950), those changes are not immediately realized on workstations that are logged on while the changes are being made. Such workstations must log off and log back on before the security changes are enabled.

Understanding Security Types

At specific object levels, you can set the following levels of security, alone or in any combination, for users and groups:

Level of security	Description
Application security	Secures users from running, installing, or both, a particular application or a particular form within an application.
Action security	Secures users from executing a particular action, such as adding, deleting, revising, inquiring, or copying a record.
Row security	Secures users from accessing a particular range or list of records in any table. 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.
Column security	Secures users from viewing a particular field or changing a value for a particular field. This item can be a database or non-database field that is defined in the data dictionary, such as the work/calculated fields. 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 that user accesses that application.

Processing option security	Secures users from viewing or changing the values of processing options, or from prompting for versions and prompting for values for specific applications. 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. 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.
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 ERP 9.0 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 which is specified. All other security still applies.
External calls security	Secures users from accessing standalone executables that exist external to ERP 9.0. These external executables, which might include design tools, system monitors, and debugging tools, are specific to ERP 9.0.
Solution Explorer security	Secures users from accessing or making changes to the following Solution Explorer features: Solution Explorer 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 denies access to table I/O and business functions, and prevents users from writing to tables. Workflow Status monitors and controls access to the workflow status.

Understanding ERP 9.0 Object-Level Security

ERP 9.0 security is at the object level. This level means that you can secure specific objects within ERP 9.0, which provides flexibility and integrity for your security. For example, you can secure a user from a specific form; then no matter how the user tries to access the form (using a menu or any application that calls that form), ERP 9.0 prevents him or her from accessing that form. Though setting up good security is always a challenge, ERP 9.0 simplifies the process by allowing you to set security for hundreds of objects at a time by securing all objects on a specific menu, or securing all objects under a specific system code. But remember, only the objects are secured; ERP 9.0 does not support menu or system code security. Object security provides a higher integrity. For example, if you were to secure a specific menu to prevent users from accessing the applications on that menu, the users might still be able to access those applications through some other menu or some other application that accesses those applications that you were trying to secure.

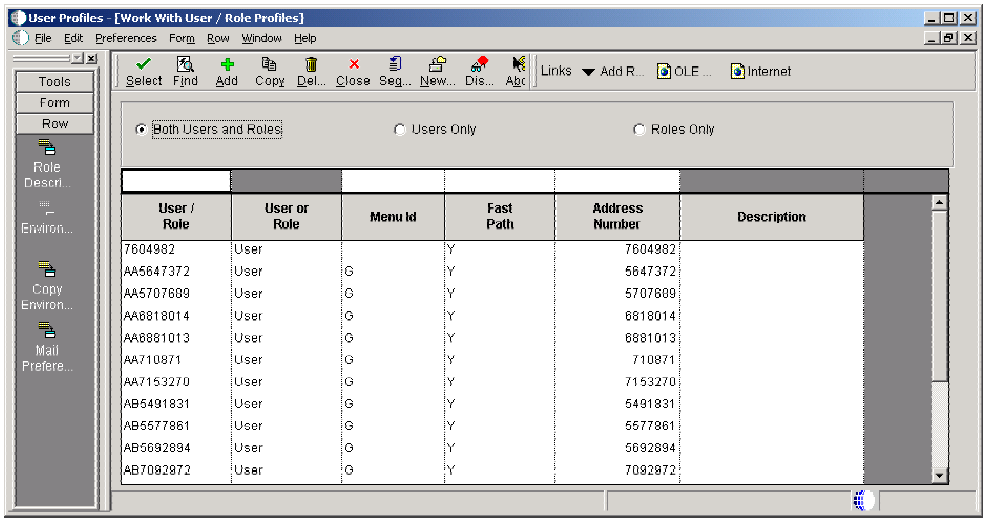
Identifying Users and Objects for Security

To set up security, you first need to identify the users and the objects that you want to secure.

► To identify users and objects for security

From the System Administration Tools menu (GH9011), choose User Profiles (P0092),

1. On the Work With User / Role Profiles, locate the users and group IDs for whom you want to set up security.



2. Identify what you want to secure:
   - For all security, identify which application, form, report, or table that you want to secure. This is the object name, such as F0101 for the Address Book Master file, P0101 for the Address Book application, or *ALL for all objects.
   - For only row and column security, also identify which columns (data items) that you want secured. This is the data dictionary item name, such as “Cost Center” for the Business Unit/Branch Plant field, or “Company” for the Company Name. Column security can apply to dictionary items that are not in database tables.

Working with Security Workbench

The Security Workbench application (P00950) allows you set up security for applications, actions, and processing options. You can set up security for users or roles.

See Also

- *Working with the Object Configuration Manager* in the *Configurable Network Computing Implementation Guide* for information about securing the query-by-example row
- *Setting Up User Profiles* in the *System Administration Guide* for information about securing the Fast Path tool

Managing Application Security

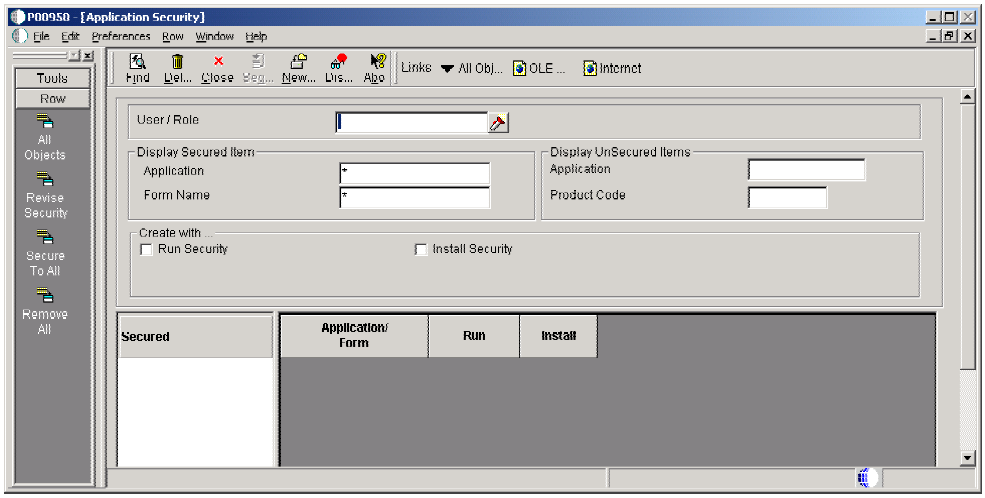
This section explains how to add, revise, and remove application security. You can secure users from running, installing, or both, a particular application or a particular form within an application. This task also explains how to add a *ALL object, how to change all of the applications for a particular user or role from unsecured to secured, and how to set security for all but one form in an application.

For example, to set run security on the Data Dictionary Application (P92001), click the Run Security option, and then drag the Data Dictionary node from the Unsecured node to the Secured node. The detail area reflects the run security that you set for this application. This situation means that the user whom you entered could *not* run the Data Dictionary Application (P92001).

► To set up application security

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. From the Form menu of Work with User/Role Security, choose Application.



2. On the Application Security form, complete the following fields and then click Find:

   - User/Group

     Enter a complete user or role, which includes *PUBLIC but not wildcards.

   - Application

     Enter an application name, such as P0101. You can also use *ALL to display all applications.

   - 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 expanding the node, the secured applications and forms also appear in the detail area.

3. Under the Display UnSecured Items heading, complete only one of the following fields that appear and then click Find:

    - Application

    You can enter *ALL in this field to choose *all* ERP 9.0 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 and forms from which to choose.

    Your search (application, product code, or menu) appears under the UnSecured node. Expand the node to view individual applications and forms that do not already have security set for them. After you expand the node, the individual applications and forms also appear in the grid.

4. Perform the following actions, as necessary, to add, change, or remove application security:

    - Add
    - Change
    - Delete**To add security to an application**

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On the Work with User/Group Security form, from the Form menu, choose Application.
2. On the Application Security form, under the Create With heading, click one or both of the following options:

    - Run Security
    - Install Security

    Use the Install Security option for just-in-time installation only.

3. Do one of the following:

    - Drag applications and forms from the UnSecured node to the Secured node.
    - From the Row menu, choose All Objects to move all applications to the Secured node.
    - From the Row menu, choose Secure to All to move all objects that are beneath the UnSecured node to the Secured node.

    The applications or forms now appear under the Secured node with the appropriate security.

► To change security for an application

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On the Work with User/Group Security form, from the Form menu, choose Application.
2. On the Application Security form, Under Display Secured Item, choose an application or form.
3. Click one or both of the following options:
   - Run Security
   - Install Security

   Caution
   Use the Install Security option for just-in-time installation only.

   The values under the Run and Install fields in the detail area change accordingly.
4. From the Row menu, choose Revise Security.

► To remove security from an application

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On the Work with User/Group Security form, from the Form menu, choose Application.
2. On the Application Security form, do one of the following:
   - Under the Secured node, choose an application or form and click Delete.
   - Drag an application or form from the Secured node to the UnSecured node.
   - On the Row menu, choose Remove All to move *all* applications and forms from the Secured node to the Unsecured node.

Securing Users to a Form in an Application

You might want to restrict one or more users to accessing 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.

► To secure users to a form in an application

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On Work with User/Role Security, in the User/Role field, enter a user or role ID and click Find.
2. Choose a row displaying Application Security in the Description column and click Select; or choose Application Security from the Form menu.

   The Application Security form appears.

3. In the Application field, under Display UnSecured Items, enter the name of an application and click Find.
4. Expand the UnSecured node and any child nodes to see the forms for the application.

   The names of the application forms appear.

5. Click the name of the form you want users to see, and drag it to the Secured node.

   Note
   Do not choose the Run Security and Install Security options to allow users to see the form.

6. Click Find.
7. Expand the UnSecured Node and choose the application you want to secure.
8. Choose the Run Security option to prevent users from accessing the application unless they want to run the unsecured form.

   Caution
   Do not choose the Install Security option. Doing so will prevent just in time installation (JITI) of anything necessary to run the application.

   After you complete these steps, users 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 explains how to add, revise, and remove action security. You can secure users from executing a particular action, such as adding, deleting, revising, inquiring, or copying a record. At the end of this task are additional topics explaining how to add a *ALL object, and how to move all of the applications for a particular user or role from unsecured to secured.

► To set up action security

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On Work with User/Role Security, from the Form menu, choose Setup Security and then choose Action.
2. On the Action Security form, complete the following fields and click Find:

   - User/Group

   Enter a complete user or role. You can enter *PUBLIC but not wildcards.

   The following fields are mutually exclusive:

   - Application

   Enter an application name, such as P0101. Enter *ALL to display all applications.

   - Form Name

Enter a form name, such as W0101G. 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 secured applications and forms. After expanding the node, the individual applications and forms that are secured also appear in the detail area.

3. To search on applications and forms that you want to secure, complete *one* of the following fields that appear under the Display UnSecured Items heading, and then click Find.

   You must perform this step before you can add new security, because this step provides a list of applications and forms from which to choose.

   - Application

     Enter an application name, such as P0101. Enter *ALL to display all applications.

   - Product Code

   Your search (application or product code) appears under the UnSecured node. Expand the node to view individual applications and forms. After expanding the node, the individual applications and forms also appear in the detail area.

4. Perform the appropriate actions to add, change, or remove action security.

► To add action security

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On Work with User/Role Security, choose an object and click Action on the Form menu.
2. On Action Security, under the Create With heading, choose any of the following options:
   - Change
   - Add
   - Delete
   - OK/Select
   - Copy
   - Scroll To End
3. After choosing one of the options, do one of the following:
   - Drag applications and forms from the UnSecured node to the Secured node.
   - From the Row menu, choose All Objects to move all applications to the Secured node.
   - From the Row menu, choose Secure to All to move all objects beneath the UnSecured node to the Secured node.

   For example, to set delete security on an application, click 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 these applications, which means that the user that you entered could *not* perform the delete action on any applications that you placed under the Secured node.

The applications or forms now appear under the Secured node with the appropriate action security.

► To change action security

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On Work with User/Role Security, choose an object and then click Action on the Form menu.
2. On Action Security, under the Secured node, choose an application or form and then choose any of the following options:
   - Change
   - Add
   - Delete
   - OK/Select
   - Copy
   - Scroll To End
3. From the Row menu, choose Revise Security.

   The values under the Add, Change, Delete, OK, Select, Copy, and Scroll to End fields in the detail area change accordingly.

► To remove action security

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On Work with User/Role Security, choose an object and then click Action on the Form menu.
2. On Action Security, do one of the following:
   - Under the Secured node, choose an application or form and click Delete.
   - Under the Secured node, drag an application or form from the Secured node to the UnSecured node.
   - On the Row menu, choose Remove All to move *all* applications and forms from the Secured node to the UnSecured node.

Managing Row Security

This section explains how to add and revise row security. You can 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

ERP 9.0 first looks for row security at the user level, then at the group level, and then *PUBLIC. If you set any security at a higher level, such as at the user level, ERP 9.0 ignores any security set at lower levels, such as at the group or *PUBLIC levels.

Before you set up row security for an item on a table, you should first verify that the item is actually in that table. For example, the Address Book Master table (F0101) 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 Address Book Master table (F0101) has no effect.

You set up row security on a table, not on a business view. You should verify that the object which 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 Environment Detail - One World table (F00941). You could secure the data item RLS (Release) because it is in the Environment Detail - One World table. On the other hand, the same item is not in the Library List Master File table (F0094). If you attempt to secure the item on the Library List Master File 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).

Before you can set up row security, you must turn on row security in Data Dictionary Design.

► To set up row security

On the Data Dictionary Design menu (GH951), choose Work With Data Dictionary Items (P92001).

1. On Work With Data Items, click Find.
2. Choose a data item that you want to secure, and click Select.

   Note
   You can enter search criteria in the Search Description field and the QBE row to narrow your search.

   The Data Item Specifications form appears.
3. On the Item Specifications tab, click the Row Security option and click OK.

   This option must be turned on for row security to work.
4. Click OK.
5. Exit the data dictionary application.
6. On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

   The Work with User/Role Security form appears.
7. From the Form menu, choose Setup Security and then Row.

8. On the Row Security Revisions form, complete the following field and then click Find to display current row security:
    - User / Role
9. Complete the following 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 your security information.

► To delete security on the Row Security Revisions form

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On Work with User/Role Security, choose an object, and click Row on the Form menu.
2. On the Row Security Revisions form, complete the following field and click Find:
    - User / Role

    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.

3. Choose the security record or records in the detail area, and then click Delete.
4. On Confirm Delete, click OK.
5. 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 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, or a form.

Setting Up Column Security on a Table

When you set up column security on a table, consider the following:

- Verify that the object which you want to secure is actually in the table.
- Verify that the object which you want to secure is part of an application that uses a business view over a table containing the object.
- Verify that the object whicht 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 Environment Detail – One World table (F00941), 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 Environment Detail – One World table (F00941) 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 Environment Detail – One World table (F00941).

Setting Up Column Security on an Application

When you set up column security on an application, consider the following:

- Verify that the object which you want to secure is actually in the application.
- Verify that you secure the correct data item in an applicationp because descriptions can be very similar, if not identical, for different data items.

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 appliction, you can apply security to the data item. However, note that data items UGRP, MUSE, USER, and USR0 all contain the identical data description User ID. Verify the item by its alias, not by its data description.

Applying column security on an application means that even if an application uses a business view that does not contain the data item which you want to secure, you can still secure it, as long as the item appears on forms in the application.

Setting Up Column Security on a Form

When you set up column security on a form, consider the following:

- Verify that the object which you want to secure is actually on the form.
- Verify that you secure the correct data item in a form because descriptions can be very similar for different data items.

Applying column security on a form means that even if the form uses a business view that does not contain the data item which you want to secure, you can still secure it, as long as the item appears on the form.

► To set up column security

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On Work with User/Role Security, from the Form menu, choose Setup Security and then choose Column.
2. On Column Security Revisions, complete the following field, and then click Find to display current column security:
    - User / Role
3. To add new security, go to the last row of the detail area and enter information into only *one* of the following fields:
    - Table
    - Application
    - Form Name

    You can enter *ALL in any of these fields; however, once *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 the following fields.
    - Data Item
    - View
    - Add
    - Change
5. To change security, change the row values in the detail area.
6. Click OK to save your security information.

► To delete security on the Column Security Revisions form

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On Work with User/Role Security, from the Form menu, choose Setup Security and then choose Column.
2. On the Column Security Revisions form, complete the following field, and then click Find:
    - User / Role

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 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 processing option values at all, 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, click 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.

► To add security to processing options

On the Security Maintenance (GH9052) menu, choose Security Workbench (P00950).

1. From the Form menu of Work with User/Role Security, choose Processing Option.
2. On the Processing Option Security form, complete the following fields and click Find:
   - User / Role

     Enter a complete user or role, which includes *PUBLIC but not wildcards.

   - Application

     Enter an application name, such as P0101. You can also enter *ALL to display all applications.

   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 expanding the node, the applications that are secured also appear in the detail area.

3. Complete *one* of the following fields that appear under the Display UnSecured Items heading, and click Find:

- Application
- Product Code

You must perform this step before you can add new security. This step provides a list of applications from which to choose.

Your search (application, product code, or menu) appears under the UnSecured node. Expand the node to view applications (interactive and batch) and/or menus with interactive or batch applications. After expanding the node, the applications also 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 appear after you expand the UnSecured node.

4. Under the Create With heading, click one or more of the following options, and then drag applications from the UnSecured node to the Secured node:
   - Change
   - Prompt for Values

     When you click this option, you automatically activate the Change option.
   - Prompt for Versions
   - OK Select
5. Do one of the following:
   - Drag applications from the UnSecured node to the Secured node.
   - From the Row menu, choose All Objects to move all applications to the Secured node.
   - From the Row menu, choose 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.

► To change security for processing options

On the Security Maintenance (GH9052) menu, choose Security Workbench (P00950).

1. From the Form menu of Work with User/Role Security, choose Processing Option.
2. On the Processing Option Security form, complete the following fields and click Find:
   - User / Role

     Enter a complete user or role, which includes *PUBLIC but not wildcards.
   - Application

     Enter an application name, such as P0101. You can also enter *ALL to display all applications.

   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 expanding the node, the applications that are secured also appear in the detail area.

3. Under the Secured node, choose an application, and click one or more of the following options:

    - Change
    - Prompt for Values

    When you click this option, you automatically activate the Change option.

    - Prompt for Versions
    - OK/Select

    The values under the Change, Prompt for Values, and Prompt for Versions fields in the detail area change accordingly.

4. From the Row menu, choose Revise Security.

► To remove security from processing options

On the Security Maintenance (GH9052) menu, choose Security Workbench (P00950).

1. From the Form menu of Work with User/Role Security, choose Processing Option.
2. On the Processing Option Security form, complete the following fields and click Find:

    - User / Role

    Enter a complete user or role, which includes *PUBLIC but not wildcards.

    - Application

    Enter an application name, such as P0101. You can also enter *ALL to display all applications.

    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 expanding the node, the applications that are secured also appear in the detail area.

3. Do one of the following:
    - Under the Secured node, choose an application and click Delete.
    - Under the Secured node, drag an application from the Secured node to the UnSecured node.
    - On the Row menu, choose Remove All to move *all* applications from the Secured node to the UnSecured node.

Managing Tab Security

This section describes how to add, change, and remove security for forms as tabs. 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, click 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.

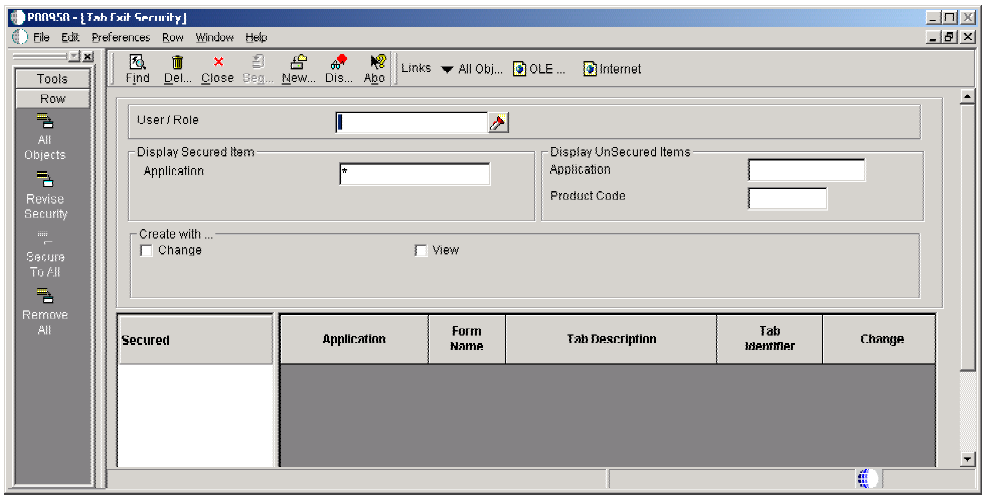
Note

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.

► To add security to a tab

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. From the Form menu of Work with User/Role Security, choose Set Up Security and then choose Tab Security.



2. On Tab Exit Security, complete the following 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 expanding the node, the secured tabs also appear in the grid.

3. Complete *one* of the following fields that appear in the Display UnSecured Items heading and click Find:

   - Application

     You can use *ALL in this field to choose *all* ERP 9.0 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 choose.

Your search (application or product code) appears under the UnSecured node. Expand the nodes to view applications (interactive and batch) and the associated tabs. After expanding 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 appear after you expand the UnSecured node.

4. Under the Create With heading, choose one or more of the following options:

   - Change

   Turn on this option to prohibit a user or role from changing information on that tab page.

   - View

   Turn on this option to hide the tab from the user or the role.

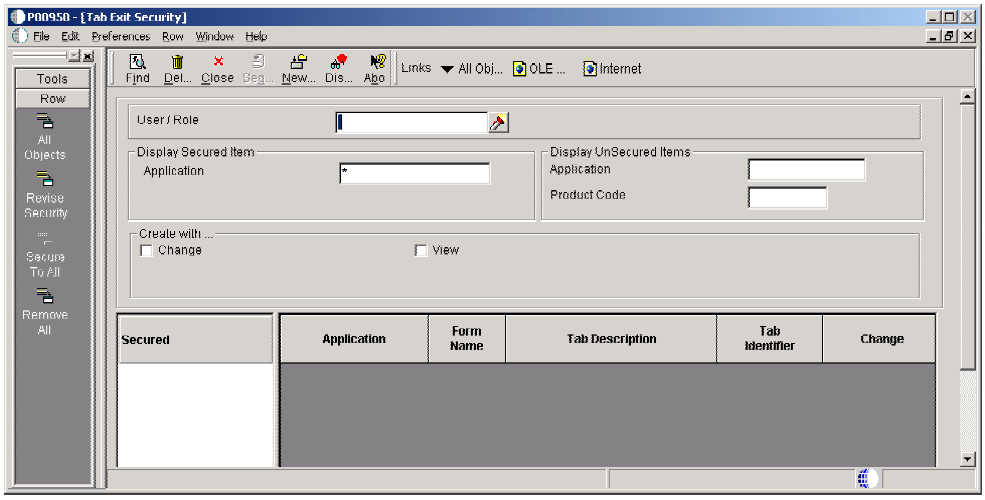
5. Drag tabs from the UnSecured node to the Secured node.

   The tabs that you dragged appear under the Secured node.

► To change security for a tab

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. From the Form menu of Work with User/Role Security, choose Set Up Security and then choose Tab Security.



2. On Tab Exit Security, complete the following 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 expanding the node, the secured tabs also appear in the grid.

3. Under the Secured node, choose a tab and choose one or more of the following options:

   - Change

     Turn on this option to prohibit a user or role from changing the name of the tab.

   - View

     Turn on this option to hide the tab from the user or the role.

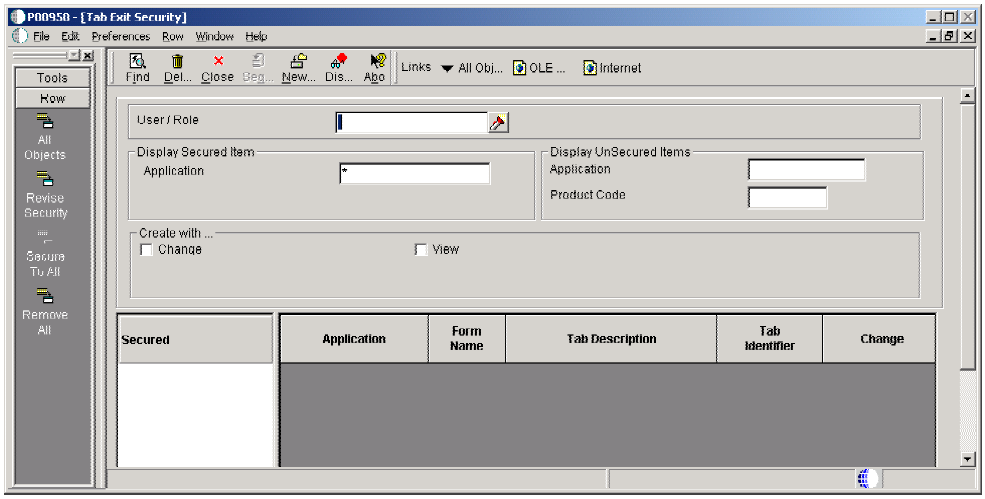
4. From the Row menu, choose Revise Security.

   The values under the Change and View fields in the detail area change accordingly.

► To remove security from a tab

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. From the Form menu of Work with User/Role Security, choose Set Up Security and then choose Tab Security.



2. On Tab Exit Security, complete the following 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 expanding the node, the secured tabs also appear in the grid.

3. Do one of the following:
   - Under the Secured node, choose 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, choose Remove All to move all tabs from the Secured node to the UnSecured node.

Managing Exit Security

This section describes how to add, change, and remove security for the menu bar exits on ERP 9.0 forms. These exits call applications and allow users to manipulate data. Exit security also provides restrictions for the menu options.

► To set up exit security

On the Security Maintenance (GH9052) menu, choose Security Workbench (P00950).

1. From the Form menu of Work with User/Role Security, choose Setup Security, and then choose Exit Security.
2. Complete the following 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. You can also use *ALL to display all applications.

   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 interactive and batch. After expanding the nodes, the secured hyper-button exits also appear in the detail area.

3. Complete only one of the following fields that appear in the Display UnSecured Items heading, 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 choose.

Your 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 expanding 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 appear after you expand the UnSecured node.

4. Perform actions as necessary to add, change, or remove exit security.

► To add security to an exit

On the Security Maintenance (GH9052) menu, choose Security Workbench (P00950).

1. On the Work with User/Role Security form, from the Form menu, choose Exit Security.
2. Complete the following 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. You can also use *ALL to display all applications.

   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 interactive and batch. After expanding the nodes, the secured hyper-button exits also appear in the detail area.

3. Complete *one* of the following fields that appear 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 choose.

   Your 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 expanding 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 appear after you expand the UnSecured node.

4. Under the Create With heading, turn on the following option:
   - Run Security

The exits that you dragged appear under the Secured node.

5. Drag exits one at a time from the UnSecured node to 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.

► To change security for an exit

On the Security Maintenance (GH9052) menu, choose Security Workbench (P00950).

1. On Work with User/Role Security, click the Form menu and choose Exit Security.
2. Complete the following fields and click Find:
   - User/Group

     Enter a complete user or Role ID, which includes *PUBLIC but not wildcards.

   - Application

     View security for a specific application. You can also use *ALL to display all applications.

   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 interactive and batch. After expanding the nodes, the secured hyper-button exits also appear in the detail area.

3. Under the Secured node, choose an exit and click the following option:
   - Run Security
4. From the Row menu, choose Revise Security.

   The values under the Run field in the detail change accordingly.

► To remove security from an exit

On the Security Maintenance (GH9052) menu, choose Security Workbench (P00950).

1. On Work with User/Role Security, click the Form menu and choose Exit Security.
2. Complete the following fields and click Find:
   - User/Group

     Enter a complete user or Role ID, which includes *PUBLIC but not wildcards.

   - Application

     View security for a specific application. You can also use *ALL to display all applications.

   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 interactive and batch. After expanding the nodes, the secured hyper-button exits also appear in the detail area.

3. Do one of the following:
   - Under the Secured node, choose an exit, and click Delete.

- Under the Secured node, drag an exit from the Secured node to the UnSecured node.
- On the Row menu, choose Remove All to move all exits from the Secured node to the UnSecured node.

Managing Exclusive Application Security

This section describes how 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, but 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. ERP 9.0 still secures the user from all other applications where that salary information might appear.

► To add access with exclusive application security

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. From the Form menu of Work with User/Role Security, choose Setup Security, and then choose Exclusive Application.
2. Complete the following field:
   - User/Group

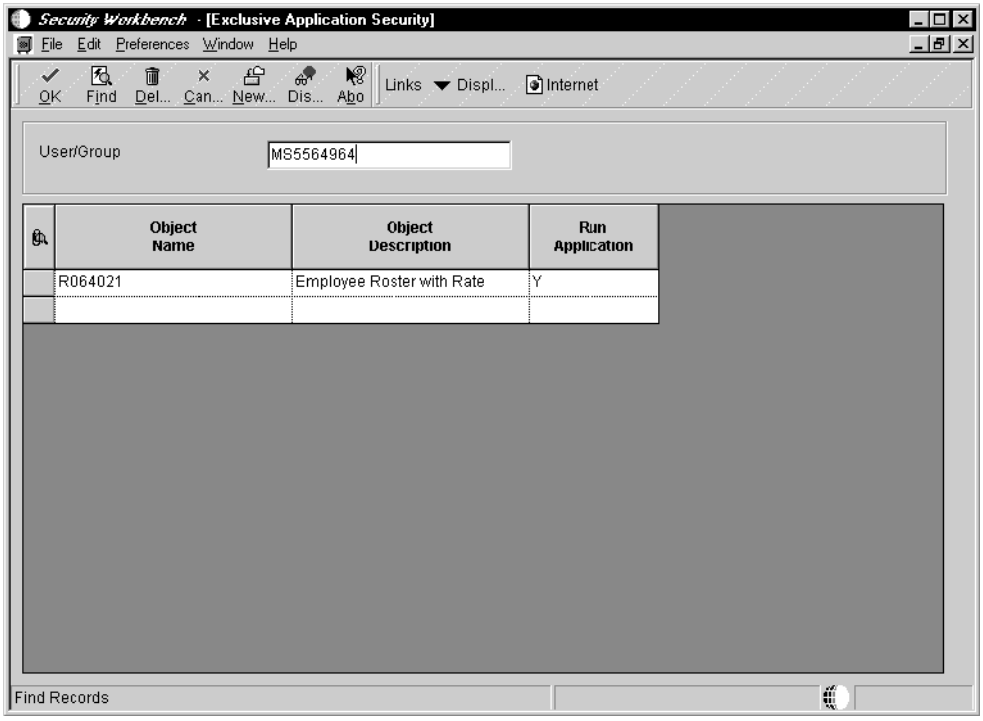
   Enter a complete user or role, which includes *PUBLIC but not wildcards.
3. Complete the following fields in the detail area:
   - Object Name

   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.

► To delete access on the Exclusive Application Security form

1. On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).



2. On Work with User/Role Security, click the Form menu and then choose Exclusive Application.
3. On the Exclusive Application Security form, complete the following field and click Find:
    - User / Role

    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.

4. Highlight the security records in the grid and click Delete.
5. On Confirm Delete, click OK.
6. Click OK when you finish deleting exclusive application security.

    If you do not click OK after you delete the security records, ERP 9.0 does not save the deletion.

Managing External Calls Security

This section describes how to secure users and roles from access to external call applications. In ERP 9.0, certain applications exist that are not internal to ERP 9.0; 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 \B9\SYSTEM\Bin32 directory.

► To set up security for external calls

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. From the Form menu of Work with User/Role Security, choose Setup Security and then choose External Calls.
2. Complete the following 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.

Notes
For instructions on adding security, see *To add security to an application* in the *System Administration Guide*.

For instructions on changing security, see *To change security for an application* in the *System Administration Guide*.

For instructions on removing security, see *To remove security from an application* in the *System Administration Guide*.

► To add security to an application

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. From the Form menu, choose External Calls.
2. Complete the following fields, and click Find:

   - User/Group

   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, ERP 9.0 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 Create With heading, click the following option:
    - Run Security
4. Do one of the following:
    - Drag applications from the UnSecured node to the Secured node.
    - To move all applications to the Secured node, choose 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, turn on 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 you entered could *not* run the Business Function Design application.

► To change security for an application

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On the Work with User/Group Security form, click the Form menu and then choose External Calls.
2. Complete the following fields, and click Find:
    - User/Group

    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, ERP 9.0 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.

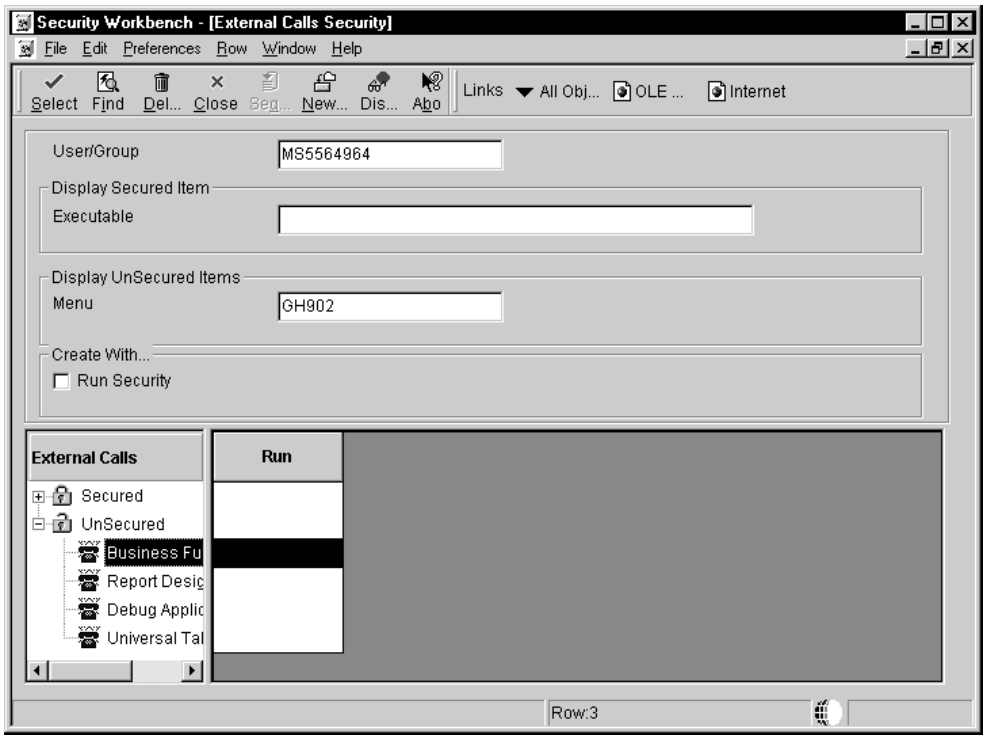
3. Under the Secured node, choose an application, and then click the following option:
    - Run Security
4. From the Row menu, choose Revise Security.

    The values for the Run field in the detail area change accordingly.

► To remove security from an application

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On the Work with User/Group Security form, click the Form menu and then choose External Calls.



2. On External Calls Security, complete the following fields and click Find:

   - User/Group

     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, ERP 9.0 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 the following:

   - Under the Secured node, choose an application and click Delete.
   - Under the Secured node, drag an application from the Secured node to the UnSecured node.
   - On the Row menu, choose Remove All to move *all* applications from the Secured node to the UnSecured node.

► To copy all security records for a user or a role

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. From the Form menu of Work With User/Role Security, choose Copy Security.
2. Turn on one of the following options:

- Copy and Add

  When you copy and add security settings, you do not overwrite pre-existing security for user or role.

- Copy and Replace

  When you copy and replace security settings, ERP 9.0 deletes the security information for a user or role, and then copies the new security information from the selected user or role.

3. Complete the following 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 Security for a User or a Role

You can copy the security information for one user or role, and 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.

► To copy a single security record for a user or a role

On the Security Maintenance menu (GH9052), choose Security Workbench (P00950).

1. On Work With User/Role Security, locate a security record.
2. Click the security record row that you want to copy, and then from the toolbar, click Copy.
3. Complete the following field and click OK:
   - To User / Role

The system saves the security information and returns you to the Work With User/Role Security form.

Deleting Security on the Work with User/Role Security Form

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.

► To delete user security

On the Security Maintenance menu (GH9052), choose User Security (P98OWSEC).

1. On the Work with User Security form, find the user or role, choose the appropriate record in the tree structure, and then click Delete.

Note
If you choose 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.

► To delete security on the Work with User/Role Security form

On the Security Maintenance menu (GH9052), choose User Security (P98OWSEC).

1. On the Work with User Security form, click Find, choose a record in the grid, and then click Delete.

Note
You can enter search criteria in the QBE line to narrow your search.

2. On Confirm Delete, click OK.

   Security Workbench deletes the security record and refreshes the grid.

Understanding Signon Security

ERP 9.0 security runs on a logic server in a dedicated internal process. You create a security table on your data server that stores information, such as:

Value	Description
ERP 9.0 User	The user ID that is used to sign on to ERP 9.0.
ERP 9.0 Password	The user's password that ERP 9.0 validates when signing on to ERP 9.0.
System User and System Password	The system user and password is the actual user and password that is used to connect to all database management systems (DBMS). If the ERP 9.0 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 that is required by ERP 9.0.
Last Change	The date that the ERP 9.0 password was last changed.

You must define a security record for each ERP 9.0 user either by group or individual. J.D. Edwards recommends that you map multiple ERP 9.0 users to the same system user. For example, each user can use the same system user that ERP 9.0 uses to connect to ERP 9.0 database management systems. By setting up your security in this manner, you can simplify database administration of users and passwords.

You can also set up unified logon with ERP 9.0 to simplify sign-on security. When you set up unified logon for ERP 9.0, ERP 9.0 uses Windows NT Authentication to verify ERP 9.0 security. This verification allows ERP 9.0 signon security to use the network signon

information that a user supplies when signing on to Windows; ERP 9.0 does not require the user to enter another user ID and password when signing on to ERP 9.0.

Security Table Access

Provided that you keep the system user and password secure, no users have direct access to the ERP 9.0 One World Security table (F98OWSEC). The exception to this situation is for ERP 9.0 system administrators who maintain the security information. The ERP 9.0 security server has access to the ERP 9.0 One World Security table through JDENet.

You must perform all of the validation and changes of ERP 9.0 passwords through a JDENet message to the enterprise server with the security table. Upon validating an ERP 9.0 password, the JdeNet message returns the system user and password that you enter. These words are encrypted across the network. Internally, all connections to databases are done by using this system password.

Using your database management system, you should place database security on the ERP 9.0 One World Security table. You should also assign ERP 9.0 object security to OneWorld Security (P98OWSEC) so that users cannot access the object except to enter User Password Revisions (W98OWSECD).

See Also

- *Working with User Security* in the *System Administration Guide* for information on setting up user security

Password Encryption

You can enter the initial ERP 9.0 signon password for each user in a number of ways, such as:

- Manually typing it in
- Using a default password that is established through the signon security processing options
- Having ERP 9.0 enter it automatically because the user already has an existing security record

When manually entering a password, or when using the processing option default password, you cannot see the password for a new user because you are typing it in. But when you revise this record at another time, ERP 9.0 encrypted 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 has been entered. ERP 9.0 stores the actual password on the security server in the ERP 9.0 One World Security Table (F98OWSEC) within a binary object. ERP 9.0 accesses the binary object when the user security application requests a change or inquiry.

Security Setup

The following checklist presents an overview of the steps that are required to set up security:

1. Ensure that the One World Security table (F98OWSEC) is located on your enterprise server in the system data source and that the table is mapped to the correct data source through the Object Configuration Manager.

If your system data source resides on your enterprise server, the security table should reside in the system data source. However, if your system data source is located on the deployment server (or other servers), the security table should be moved to the server map data source for your enterprise server.

If you have more than one logic server, J.D. Edwards recommends that you use only one as your security server.

2. From within your database management system (DBMS), place database security on this table to prevent a user from accessing the object, except to enter passwords through User Password Revisions.
3. Place security on the logic server's jde.ini file. This step is required because the DBMS user ID and password to the ERP 9.0 Sign On Security table are stored in this file.
4. Create security records for individual users. This step includes assigning the following:
   - Data source
   - System user
   - System password
   - ERP 9.0 password
   - User Status
   - Allowed number of invalid sign-on attempts (optional)
   - Change frequency (optional)

   Note
   If you intend to use a unified logon, every user in the ERP 9.0 security database requires a unique user ID.

5. Verify and modify the jde.ini file on your ERP 9.0 logic server for your platform environment.

   If you use a unified logon, you need to change the settings for a unified logon in the [SECURITY] section, in addition to the normal ERP 9.0 [SECURITY] settings.

6. If you use a unified logon with your ERP 9.0 security, set up a unified logon server for each instance of ERP 9.0 on each server. For example, if you have an NT server with multiple releases of ERP 9.0, you need a unified logon server for each release on the server.

   The unified logon server differentiates between instances of ERP 9.0, based on the port numbers for these instances. For example, if the port number for ERP 9.0 is 6104, the port number for the associated unified logon server is also 6104. Other instances and unified logon servers use different port numbers.

7. Verify and modify the jde.ini file that will be deployed to your server's workstation installations.
8. Require signon security for all machines.

Process Flow for ERP 9.0 Signon Security

ERP 9.0 provides signon security with an architecture that is designed to provide user security for ERP 9.0 and the logically attached database management systems. The security architecture prevents you from viewing your database or system password, and therefore, bypassing ERP 9.0 applications to view and change data.

The following text explains the process flow for standard sign-on security:

1. ERP 9.0 workstations sign on to ERP 9.0 by using their ERP 9.0 user ID and password. These workstations can be networked or standalone workstations, laptop computers, or other ERP 9.0 hosts.

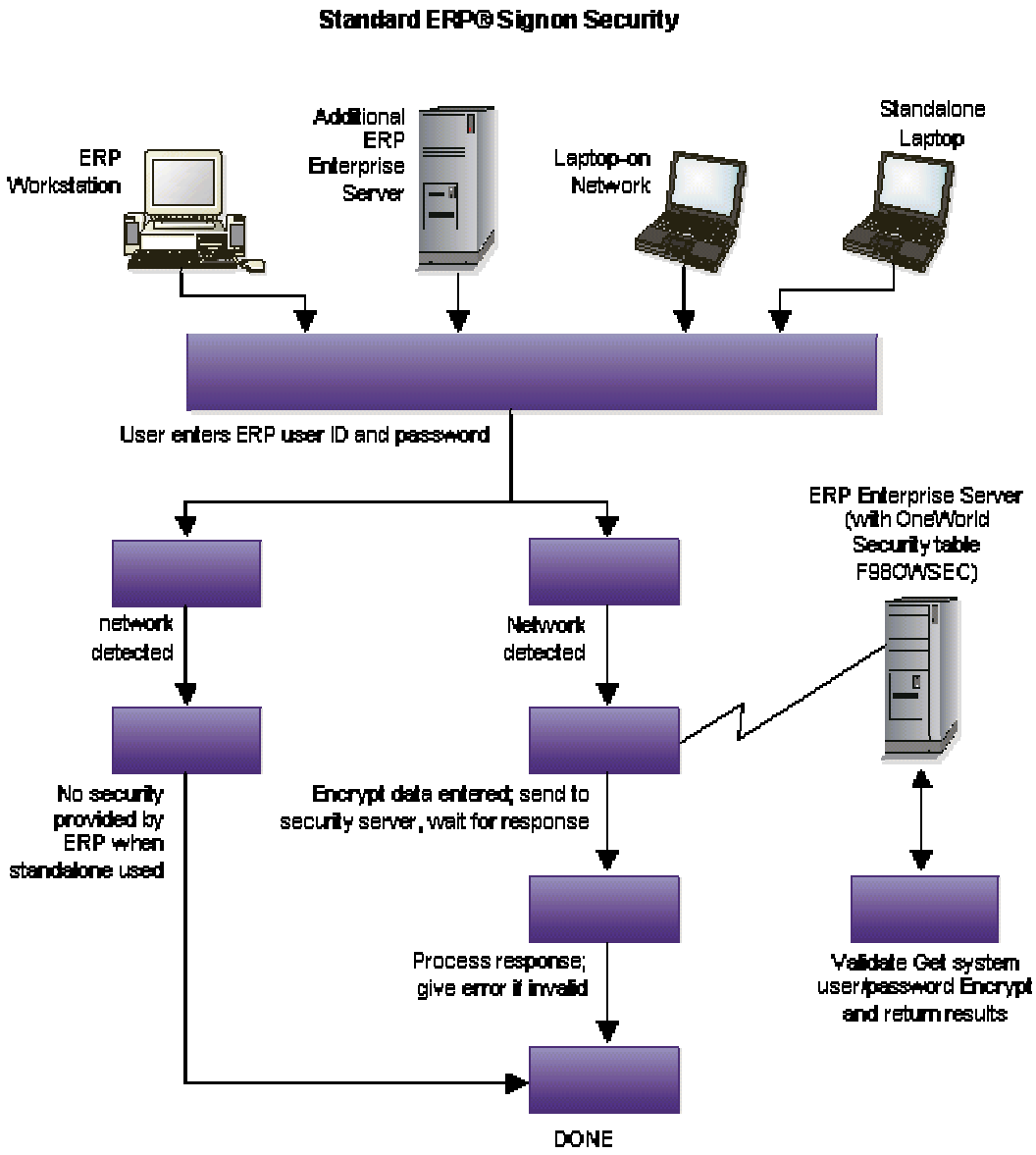
   If you enter a valid user ID and password, as validated against the local ERP 9.0 installation, the start-up process continues.

2. As ERP 9.0 starts up, it tries to detect an operational network environment.

   If a network is not detected, ERP 9.0 allows local operation in a store-and-forward mode. Because the workstation or laptop computer is not connected to a network or an ERP 9.0 enterprise server, no validation can be performed against the security table. Therefore, security is limited to that provided by the local workstation or laptop installation.

   If a network is detected, ERP 9.0 encrypts the password information and sends it over the network to the ERP 9.0 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, ERP 9.0 accepts the signon 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.

The following graphic shows a process flow model for standard ERP 9.0 signon security:



The following text explains the process flow for signon security with a unified logon:

3. A user starts up ERP 9.0 on a workstation.
4. ERP 9.0 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; rather, it is a device that verifies signon security against the domain signon security that is maintained by Windows NT.

During jdesnet initialization, jdesnet activates the unified logon server thread. The unified logon server ends automatically when jdesnet ends.

5. 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 ERP 9.0 enterprise server.
6. The ERP 9.0 enterprise server verifies that the response from the unified logon server matches the security information in the One World Security table (F98OWSEC).
7. If the security information from the user list on the unified logon server matches the security information in table F98OWSEC on the enterprise server, the start-up process continues.
8. The first time that a user signs on to ERP 9.0 with the unified logon, the Environment Selection appears. The user must enter an environment in the Environment field. Click the option to set the environment as the default, and avoid the Environment Selection form on subsequent signon attempts.

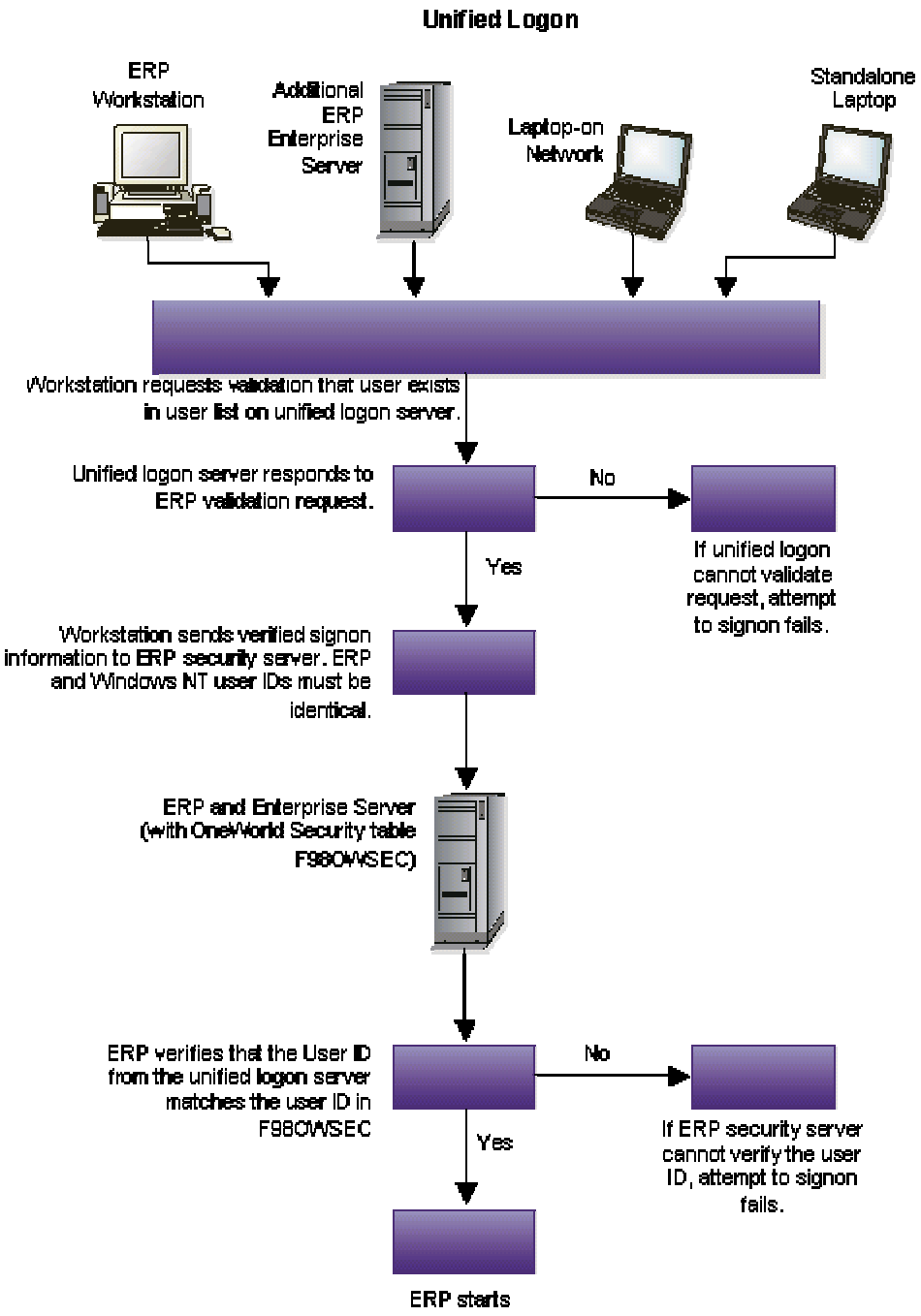
Note

The ShowUnifiedLogon setting in the [SECURITY] section of the jde.ini file allows users to reset whether the Environment Selection form appears at signon. This feature allows users to change the environment later. The following example describes the jde.ini file setting:

```
 [SECURITY]
ShowUnifiedLogon=0 or 1
```

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 on to ERP 9.0, the Environment Selection form appears and allows the user to choose an environment. This setting is the default for ShowUnifiedLogon.

The following illustration shows the process flow for unified logon:



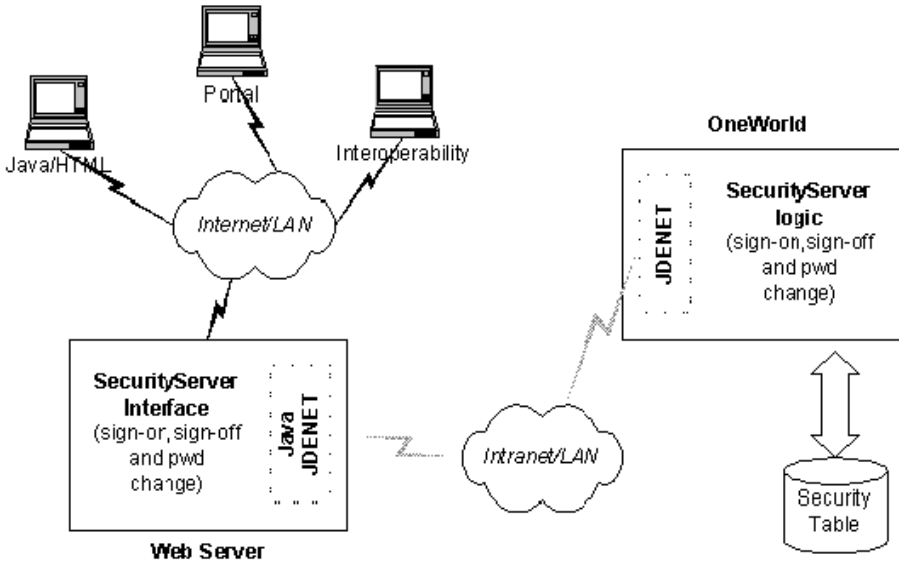
Signon Security for Web Users

The ERP 9.0 security server and the F98OWSEC table authenticate Java/HTML, Portal, and Interoperability users who log on to ERP 9.0 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 ERP 9.0 security server.

When Web users sign on, sign off, or make a password change, the JAS server sends the request via a JDENET message to the ERP 9.0 security server, which, in turn, accesses the F98OWSEC table. The ERP 9.0 security server then returns the authentication via a JDENET message to the JAS security server. If the user is authenticated, the security info is cached to the JAS security server.

In summary, the JAS security server acts as an intermediary between the Java/HTML, Portal, and Interoperability client; and the ERP 9.0 security server.

The following graphic shows a process flow model for ERP 9.0 signon security with unified logon for Web users:



As the security intermediary, the JAS security server handles the following tasks:

- Connects to the ERP 9.0 security server for user security authentication and password when a Web user signs on.
- Fails over to a secondary ERP 9.0 security server when the primary server is down, provided that the proper jas.ini settings have been defined.
- Notifies Java/HTML, Portal, and Interoperability client workstations when a user password has expired. If an Interoperability user's password has expired, signon simply fails without notification of the cause.
- Sends error message to user log after the Web user has attempted unsuccessfully to sign on *x* number of times to ERP 9.0, where *x* is the number of sign-on attempts defined in the F98OWSEC table.
- Allows Java/HTML and Portal users to change name and password.
- Encrypts JDENET messages sent between the JAS security server and the ERP 9.0 security server.
- Keeps a valid user session open until the user signs off or the ERP 9.0 session expires.

To the ERP 9.0 Web user, signon and signoff look the same as they do to a ERP 9.0 user on a Windows NT, UNIX, or AS/400 platform.

To set up security for Web users through the ERP 9.0 security server, you add the following parameters to those already existing in the jas.ini file:

[SECURITY] parameter in jas.ini file	Parameter value
NumServers	The total number of ERP 9.0 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 signon is handled by the primary security server.
SecurityServer	The name of the primary security server.
SecurityServerN	The 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 signon to fail over to a secondary server if users cannot sign on 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 at the next signon. If the value is FALSE, the feature is disabled.
#CookieLifeTime unit	The unit of time that is 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	The 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, your jas.ini file [SECURITY] settings look like the following 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, signon fails over to the secondary server if the primary server is down. If both the primary ERP 9.0 security server and a secondary server as defined in the jas.ini file fail, the JAS server fails the user signon.

If you do not define a server number or any secondary servers, your jas.ini [SECURITY] settings look like the following example:

```
 [SECURITY]

SecurityServer=JDED

UseLogonCookie=TRUE

CookieLifeTime unit is "day"

CookieLifeTime=7
```

Setting Processing Options

The User Security (P98OWSEC) application has the following 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

Password

Working with User Security

Use the OneWorld Security application (P98OWSEC) to create, test, and change user security for ERP 9.0 and the logically attached database management systems. The security architecture prevents you from viewing your database or system password and, therefore. having the ability to bypass ERP 9.0 applications to view and change data. J.D. Edwards uses an encryption algorithm to ensure that applications other than ERP 9.0 security cannot access passwords that are transmitted across the ERP 9.0 network.

You can also set up a unified logon server for an ERP 9.0 server. The unified logon server enables ERP 9.0 to use the domain logon information to determine user security for ERP 9.0 in a ERP 9.0 unified logon scenario, a user only needs to enter a user ID and a password at network logon.

Creating and Revising User Security

You can create security records one at a time for each of your users, you can set security for a group of users, 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

J.D. Edwards recommends that you create a "model" user with security information that you can copy to create other ERP 9.0 users. Typically, users within a specific role use similar security information.

You should keep user security simple. Managing ERP 9.0 user IDs and system (database) user IDs can become complicated quickly. The simplest way to set up user security is to have

all ERP 9.0 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, ERP 9.0 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 a ERP 9.0 application, ERP 9.0 searches for a security record for that user and that specific data source where the table resides. If ERP 9.0 does not find a specific record, then ERP 9.0 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 ERP 9.0 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 normal system user needs.

See Also

- *Changing Your User Options* in the *Foundation Guide* for details about how to change a password at the end-user level

Before You Begin

- Create user profiles. See *User Profiles* in the *System Administration Guide* for instructions to set up user profiles.

► To create user security

Before you can create user security, you must first set up all user and role records in the Address Book (P01012) application, create a user profile in the User Profile Revisions (P0092) application, and attach the proper Address Book record to the user or role profile. You should also review and set the appropriate processing options before using the OneWorld Security (P98OWSEC) application for the first time.

Note

For more information about processing options, see *To Set Processing Options for Signon Security* in the *System Administration Guide*.

J.D. Edwards recommends that you 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.

On the Security Maintenance menu (GH9052), choose User Security (P98OWSEC).

1. On the Work With User Security form, click Add.
2. Complete one of the following 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 gray and unavailable for data entry.

3. Complete the following 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.

   Note
   See *Data Sources* in the *Configurable Network Computing™ Implementation Guide* for more information about data source usage.

   - System User
   - OneWorld Password

   J.D. Edwards recommends 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 choose.

4. Under User Status, turn on one of the following options:

   - Enabled

   With User Status enabled, security allows the user to log on. This option is the default setting when you create user security.

   - Disabled

   With User Status disabled, security prohibits the user from logging on 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 log on. Also, 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 the following 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 her or his password.

6. Click OK to save the current user security information.
7. When you finish, click Cancel.

► To copy user security

Note

J.D. Edwards recommends that you 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.

A user profile must already exist for a user before you can create user security records for the user. Also, 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.

On the Security Maintenance menu (GH9052), choose User Security (P98OWSEC).

1. On the Work With User Security form, find the user, and then do one of the following:
   - To copy all user security records for a user or role, choose the user or role in the tree structure, and click Copy.
   - To copy a single user security record for a user or role, choose the security record row in the detail area, and choose Copy Record from the Row menu.
2. On the Copy User Records form, complete the following field and click OK:
   - To User

   Type a valid user in this field.

► To revise user and role security

On the Security Maintenance menu (GH9052), choose User Security (P98OWSEC).

1. On Work with User Security, complete the following field.
   - User ID / Role
2. Click Find.
3. Choose the appropriate record in the tree structure, and then choose Revise Security from the Row menu.
4. On Security Detail Revisions, complete the following fields, as necessary:

   Note
   For a role, choose the appropriate option from the Change box to enable each field.

   - User Status

   Under User Status, you can enable or disable a user profile.

- Password Change Frequency
- Allowed Password Attempts

5. Click OK.

► To revise all user security

On the Security Maintenance menu (GH9052), choose User Security (P98OWSEC).

1. On the Work with User Security form, from the Form menu, choose Revise All.
2. On Security Detail Revisions, in the Change box, click any of the following options to enable the related field:
   - User Status
   - Frequency
   - Attempts
   - Change Limit
3. Complete any of the following 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

     Requires user to change the password on next logon.

► To change a signon password (administrators only)

On the Security Maintenance menu (GH9052), choose Administrative Password Revisions (P98OWSEC).

Note

You can also access Administrative Password Revisions from the User Security application. On Work with User Security, find the user, choose the user in the tree structure, and then choose Password Revisions from the Row menu.

1. On the Administration Password Revisions form, complete the following 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 checked.

   - New Password

     On this form, the system does not restrict your password choices. Any password is valid.

   - New Password - Verify

- Force Immediate Password Change

  Requests user to change password during the next logon.

2. Click OK.

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 OneWorld Security application (P98OWSEC). 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.

Before You Begin

- The [SECURITY] section in your server jde.ini must include the following setting for the system to record security history:

```
 [SECURITY]
History=1
```

► To review security history

On the Security Maintenance menu (GH9052), choose User Security (P98OWSEC).

1. On Work With User Security, from the Form menu, choose Security History.
2. On Work With Security History, click Find.
3. Review the security history records that appear in the detail area.

► To require signon security

Note

Use this feature to require all machines to use J.D. Edwards signon security. This procedure only enables mandatory security for the environment that you are signed onto when making this change.

On the Security Maintenance menu (GH9052), choose User Security (P98OWSEC).

1. On the Work With User Security form, choose 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 your 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 your secured tables.

Managing Data Sources for User Security

You add data sources to user and role records in user security to authorize users and roles to access J.D. Edwards databases. You can also revise the system user and system password for existing data sources.

► To add a data source to a user, a role, or all users

On the Security Maintenance menu (GH9052), choose User Security (P98OWSEC).

1. On the Work With User Security form, from the Form menu, choose Add Data Source.
2. Complete one of the following 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

   Click this option to add a data source to all users.
3. Complete the following 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

► To revise a data source for a user, a role, or all users

1. On the Work with User Security form, complete the following field, and then click Find.
   - Data Source

Note
You can also enter both a Data Source and User ID / Role. If you choose just a data source, your change will affect all users.

2. Choose the data source in the tree structure and then, from the Row menu, choose 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 following field, and click OK:

   - System User

   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.

► To remove a data source for a user, a role, or all users

1. On the Work With User Security form, complete the following field, and then click Find.

   - Data Source

2. Choose the appropriate record in the tree structure, and then click Delete.

   Note
   For a user, you can also choose 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.

   Caution
   If you performed your 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.

Changing the jde.ini File for User Security

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 your J.D. Edwards 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.

► To change the workstation jde.ini file for security

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:

\\Bxxx\CLIENT\MISC\jde.ini

Where xxx is the installed release level of the software, for example, B9.

1. Using a text editor such as Notepad, view the jde.ini file to verify the following setting:

```
 [SECURITY]
SecurityServer=Enterprise Server Name
DefaultEnvironment=Default Environment
```

The following table explains the variable values:

Setting	Value
Security Server	The name of your ERP 9.0 enterprise server. In order 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. The following example shows how you your jde.ini file might look:

```
 [SECURITY]
NumServers=Numeric Value
SecurityServer=Enterprise Server Name (primary)
SecurityServer2=Enterprise Server Name (auxiliary)
SecurityServer3=Enterprise Server Name (auxiliary)
```

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*n*	The name of a J.D. Edwards enterprise server. Your 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 log on to and run batch reports from the enterprise server. The variable value *x* can be a number between 1 and 10. This number defines the auxiliary security server.

Changing the Time-Out Value Due to Security Server Communication Error

You might need to change a setting in your workstation jde.ini file if you receive an error such as:

> Failure to Communicate with Security Server.

Change the following section:

```
[JDENET]
connectTimeout=30
```

► To change the enterprise server jde.ini file for security

To change the enterprise server jde.ini file for security, you should verify your server jde.ini file settings as shown in this task. You use these settings to specify the internal security parameters, valid users and passwords, environments, and data sources.

1. Locate your enterprise server's jde.ini file.
2. Using an ASCII editor, such as Notepad, view the jde.ini file to verify the following 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
```

The following table explains the variable values:

Setting	Value
dispatchDLLName	Valid values for enterprise server host platforms are: • HP9000, libjdeknet.sl • RS/6000, libjdekrnl.so • Windows NT (Intel), jdekrnl.dll • Windows NT (Compaq AlphaServer), jdekrnl.dll • AS/400, JDEKRNL For UNIX platforms, values are case-sensitive.
SecurityServer	The name of your J.D. Edwards 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 OneWorld Security table (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 OneWorld Security table (F98OWSEC). This is the password used to connect to the DBMS; therefore, this value must match that of the target DBMS.
ServerPswdFile	This parameter is valid for J.D. Edwards servers operating under UNIX operating systems. The setting of this parameter determines whether the system uses special password handling for batch reports running on the server. Set the value to TRUE to instruct the system to enable special handling of passwords. Set the value to FALSE to disable special handling. 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. As a security measure, you can enable special handling by the ERP 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.
DefaultEnvironment	The name of a valid environment for accessing the security table. For example, PD9.

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. Your settings for the auxiliary security servers might look like the following example:

```
 [SECURITY]
NumServers=Numeric Value
SecurityServer=Enterprise Server Name (primary)
SecurityServer2=Enterprise Server Name (auxiliary)
SecurityServer3=Enterprise Server Name (auxiliary)
```

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*x*	The name of a J.D. Edwards enterprise server. Your 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. The variable value *x* can be any number between one and ten. This number defines the auxiliary security server.

Verifying Security Processes in the Server JDE.INI

J.D. Edwards recommends that you 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 your server jde.ini file, verify that the following parameter is set:

```
 [JDENET_KERNEL_DEF4]
maxNumberOfProcesses=1
```

Running a Security Analyzer Report

This process generates two separate reports that provide you with an analysis of ERP/SCM 9.0 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 ERP 9.0 One World Security table (F98OWSEC).

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 ERP 9.0 One World Security table.

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 following columnar data is displayed:

- 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 ERP 9.0 uses to connect to the database management system (DBMS) that you specified as the data source. The system user that is shown here must match the user value which is defined in the DBMS.

- Change Frequency

  Indicates the number of days before ERP 9.0 requires that a user change his or her ERP 9.0 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 signon 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 on to ERP 9.0. Valid values are 01 (enabled) and 02 (disabled).

- Status

  Displays the status of the User Status field.

► To run the Security Analyzer by Data Source Report (R98OWSECA)

On the Security Maintenance menu (GH9052), choose Security Analyzer by Data Source (R98OWSECA).

1. On the Work With Batch Versions – Available Versions form, choose 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, choose any of the following options:

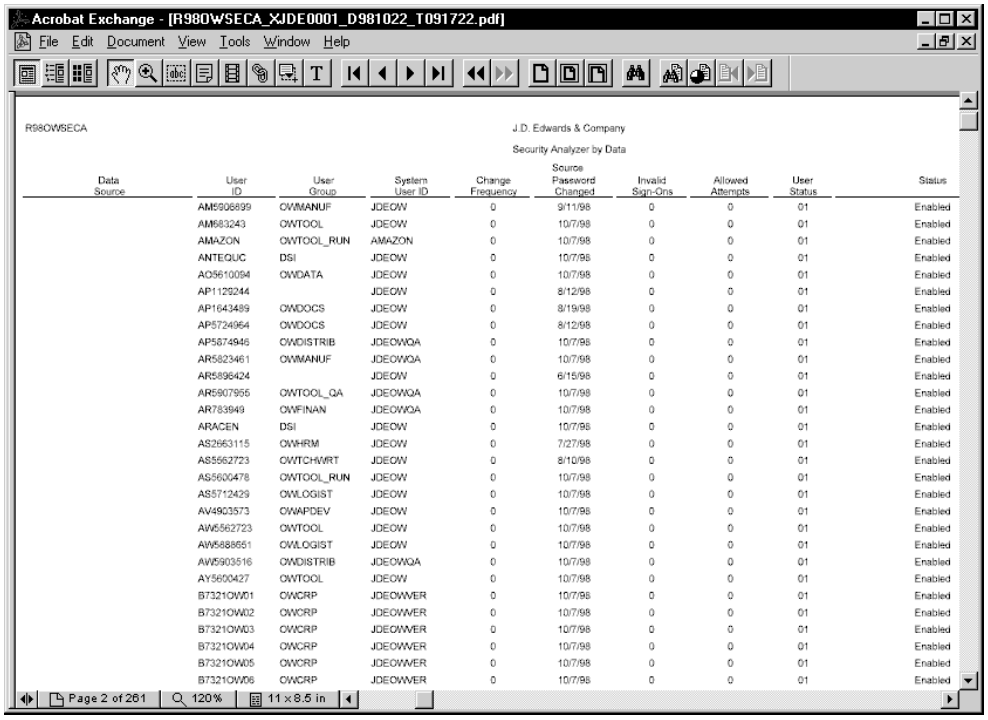
   - On Screen
   - To Printer

- Export to CSV

4. If desired, set the following option and enter a name in the box that appears below.
    - OSA Interface Name
5. Click OK.

Example: Security Analyzer by Data Source Report (R98OWSECA)

This example shows an excerpt from the Security Analyzer by Data Source report (R98OWSECA):



Data Source	User ID	User Group	System User ID	Change Frequency	Source Password Changed	Invalid Sign-Ons	Allowed Attempts	User Status	Status
	AM5906899	OWMANUF	JDEOW	0	9/11/98	0	0	01	Enabled
	AM683243	OWTOOL	JDEOW	0	10/7/98	0	0	01	Enabled
	AMAZON	OWTOOL_RUN	AMAZON	0	10/7/98	0	0	01	Enabled
	ANTEQUC	DSI	JDEOW	0	10/7/98	0	0	01	Enabled
	AO5610094	OWDATA	JDEOW	0	10/7/98	0	0	01	Enabled
	AP1129244		JDEOW	0	8/12/98	0	0	01	Enabled
	AP1643489	OWDOCS	JDEOW	0	8/19/98	0	0	01	Enabled
	AP5724964	OWDOCS	JDEOW	0	8/12/98	0	0	01	Enabled
	AP5874946	OWDISTRIB	JDEOWQA	0	10/7/98	0	0	01	Enabled
	AR5823461	OWMANUF	JDEOWQA	0	10/7/98	0	0	01	Enabled
	AR5896424		JDEOW	0	6/15/98	0	0	01	Enabled
	AR5907955	OWTOOL_QA	JDEOWQA	0	10/7/98	0	0	01	Enabled
	AR783949	OWFINAN	JDEOWQA	0	10/7/98	0	0	01	Enabled
	ARACEN	DSI	JDEOW	0	10/7/98	0	0	01	Enabled
	AS2663115	OWHRM	JDEOW	0	7/27/98	0	0	01	Enabled
	AS5562723	OWTCHWRT	JDEOW	0	8/10/98	0	0	01	Enabled
	AS5600478	OWTOOL_RUN	JDEOW	0	10/7/98	0	0	01	Enabled
	AS5712429	OWLOGIST	JDEOW	0	10/7/98	0	0	01	Enabled
	AV4903573	OWAPDEV	JDEOW	0	10/7/98	0	0	01	Enabled
	AW5562723	OWTOOL	JDEOW	0	10/7/98	0	0	01	Enabled
	AW5688651	OWLOGIST	JDEOW	0	10/7/98	0	0	01	Enabled
	AW5903516	OWDISTRIB	JDEOWQA	0	10/7/98	0	0	01	Enabled
	AY5600427	OWTOOL	JDEOW	0	10/7/98	0	0	01	Enabled
	B7321OW01	OWCRP	JDEOWVER	0	10/7/98	0	0	01	Enabled
	B7321OW02	OWCRP	JDEOWVER	0	10/7/98	0	0	01	Enabled
	B7321OW03	OWCRP	JDEOWVER	0	10/7/98	0	0	01	Enabled
	B7321OW04	OWCRP	JDEOWVER	0	10/7/98	0	0	01	Enabled
	B7321OW05	OWCRP	JDEOWVER	0	10/7/98	0	0	01	Enabled
	B7321OW06	OWCRP	JDEOWVER	0	10/7/98	0	0	01	Enabled

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 choose. The following columnar data is displayed on the report:

- User ID
- Role
- Password Change Frequency

Indicates the number of days before a user must change his or her ERP 9.0 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 which is defined in the DBMS.

► To run the Security Analyzer by User or Group Report (R98OWSECB)

On the Security Maintenance menu (GH9052), choose Security Analyzer by User or Group (R98OWSECB).

1. On the Work With Batch Versions – Available Versions form, choose 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, choose any of the following options:
   - On Screen
   - To Printer
   - Export to CSV
5. If desired, click the following option and type a name in the field that appears.
   - OSA Interface Name
6. Click OK.

Managing Unified Logon

For configurations that use a Windows NT enterprise server, to set up unified logon, you only need to modify the [SECURITY] section of the jde.ini file. When a user signs on, these settings alert ERP/SCM 9.0 to use unified logon.

When your enterprise server is on a non-Windows NT platform, you need to set up a Windows NT service for unified logon. This service identifies the unified logon server for ERP/SCM 9.0. You also need to set the unified logon settings in the [SECURITY] section of the jde.ini file.

Caution

When you use unified logon, you need to use the same user ID for the Windows NT domain and ERP/SCM 9.0 so that the records for each are synchronized. For example, if the user ID for a user in the Windows NT domain is USER1, the user ID for ERP/SCM 9.0 must also be USER1. If the user IDs are different, unified logon does not work for the user.

► To modify the jde.ini setting to enable or disable unified logon

Locate the jde.ini files on the server and on the workstation.

1. In the server jde.ini file, add the following settings in the [SECURITY] section:

```
 [SECURITY]
SecurityMode=0, 1 or 2
```

Value	Description
0	Accepts only users set up for standard signon security.
1	Accepts only users set up for unified logon.
2	Accepts users set up for both unified logon and standard signon security.

2. In the workstation jde.ini file, add the following 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.

► To set up a service for unified logon

If your enterprise server is not a Windows NT server, J.D. Edwards recommends that you set up services for unified logon on your deployment server. Your deployment server is always a Windows NT server.

1. On your deployment server, in Windows Explorer, go to the `\Unified Logon` directory and run the file `UniLogonSetup.exe`.

The Unified Logon Server Setup form appears. On this form, you define the Windows NT service for unified logon servers. You can also remove these services on this form.

2. Complete the following fields:

   - Unified Logon Service Name

     Enter the name for your unified logon server.

   - ERP 9.0 Port Number

     The port number for your unified logon server should match the ERP 9.0 port number of the ERP 9.0 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.

3. The default user list contains all authenticated network users. If you need 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 NT 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.

► 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, choose a unified logon server, and then click the Uninstall Service button.

Solution Explorer Security

Use the Security Workbench application (P00950) to set up security for 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. Beyond the Solution Explorer, you can set security for the following features:

- Internet
- Documentation
- Fine Cut
- Favorites
- Effectivity Dating (date of release)
- Fast Path
- Rough Cut
- Universal Director

Understanding Security Settings for Solution Explorer

The following table summarizes the security settings available for many of the Solution Explorer features and the meanings of each:

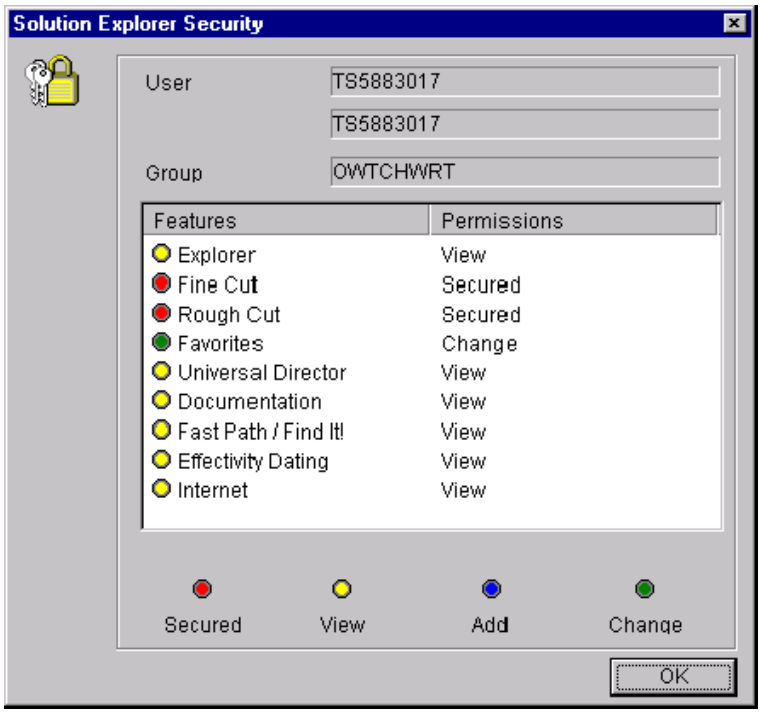
Security Setting	Meaning
Secured	Restricts the user from accessing the feature
View	Allows the user read-only access to the feature with no modification capability
Add	Allows the user to add data to the system, but does not allow the user to delete data
Change	Gives the user full access to the feature with no restrictions on changing, adding, or deleting data

Viewing Solution Explorer Security Settings

Viewing security settings in Solution Explorer allows you to check the permissions for each feature for any user in the system. You view the settings by logging onto the Solution Explorer as the user whose settings you want to view, and then click the security button in the status bar of the Solution Explorer Home Page, which launches the Solution Explorer Security form. Keep in mind that you cannot change the security settings on this form.

► To view Solution Explorer security settings

1. From any view in Solution Explorer, double-click the Security button (the lock icon) in the status bar.



2. On the Solution Explorer Security form, check the permissions for each feature and then click OK to close the form.

Configuring Solution Explorer Security

You can set different levels of security for different groups or individuals within your system.

► To configure Solution Explorer security

From the Security Maintenance menu (GH9052), launch Security Workbench (P00950).

1. On the Work With User/Group Security form, from the Form menu choose Setup Security, and then choose Solution Explorer.
2. On the Work with Solution Explorer Security Revisions form, enter the user or group ID for which you want to configure security in the User/Group field.

   To find a user or group, use the Visual Assist to bring up the User Search & Select form.

3. Choose security setting options for each feature, and then click OK.
4. If you want to automatically apply settings to a group or to an individual user, click one of the Preset buttons.
5. Repeat steps 2 through 4 for each user or group for which you want to configure security.

Note

If you secure the Fast Path parameter, users cannot use the Find It! feature to search for ERP 9.0 objects. In addition, with Fast Path secured, you cannot add new tasks to the Favorites task view with the Insert New Task function.

Using Default Security Settings for Solution Explorer

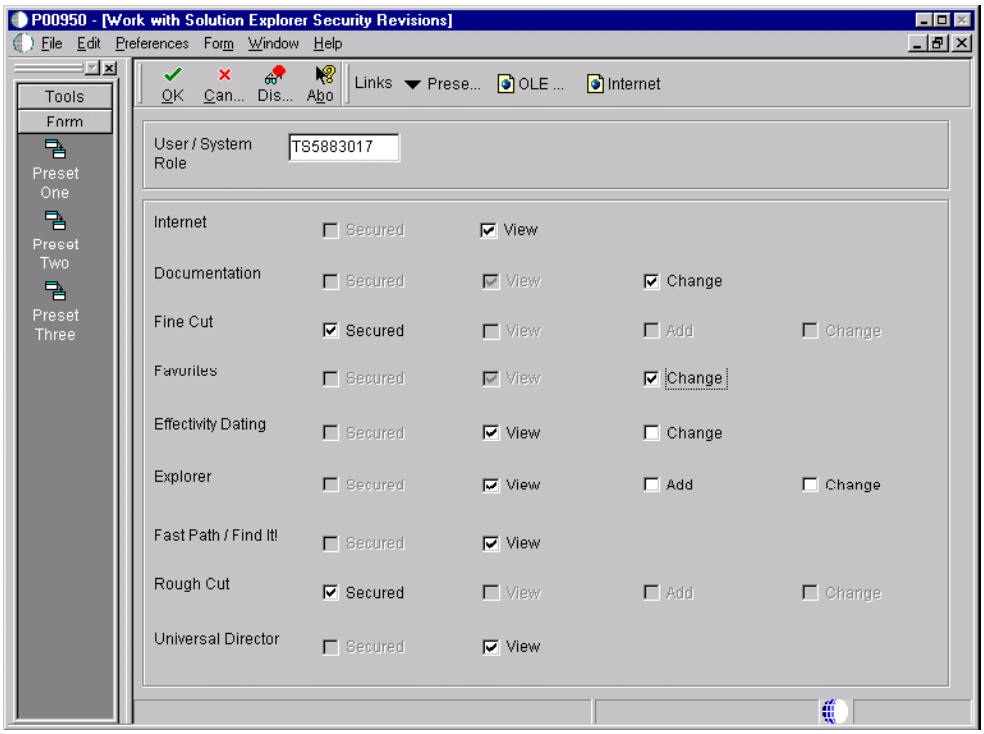
The Work With Solution Explorer Security Revisions form contains Preset buttons on the exit bar that represent default security settings for different types of users in your system. These user types correspond to novice (Preset 1), intermediate (Preset 2), and expert (Preset 3) users. If you click one of these Preset buttons, 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 laborious 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.

► To use default security settings

1. On the Work With User/Group Security form, click Add to set up security for a new user or locate the task and click Select for an existing user.
2. From the Work with Solution Explorer Security Revisions form, choose one of the following options from the Form menu:
   - Preset 1
   - Preset 2
   - Preset 3

   Based on the Preset button that you clicked, Solution Explorer automatically chooses the default security options.


P00950 - [Work with Solution Explorer Security Revisions]
File Edit Preferences Form Window Help
Tools
Form
Preset One
Preset Two
Preset Three
OK Can... Dis... Abo
Links Prese... OLE ... Internet
User / System Role
TS5883017
Internet Secured View
Documentation Secured View Change
Fine Cut Secured View Add Change
Favorites Secured View Change
Effectivity Dating Secured View Change
Explorer Secured View Add Change
Fast Path / Find It! Secured View
Rough Cut Secured View Add Change
Universal Director Secured View

3. Click OK.

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 your next ERP 9.0 software update.

Because the Vocabulary Overrides application (P9220) affects the user interface throughout ERP 9.0, it is important that you secure this application from most of your users. When you work with Vocabulary Overrides for an interactive or batch application, Vocabulary Overrides simulates an application check out from your central objects repository, just as if you checked out the application using Object Management Workbench. This is done so that, while you are working on the application in Vocabulary Overrides, no one can check out the application.

Note

When the Object Management Workbench line is written for Vocabulary Overrides, no specifications are brought down 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 your users. If the only change to an application is because of vocabulary overrides, you do not need to rebuild the application before building it into a package.

Accessing Vocabulary Overrides

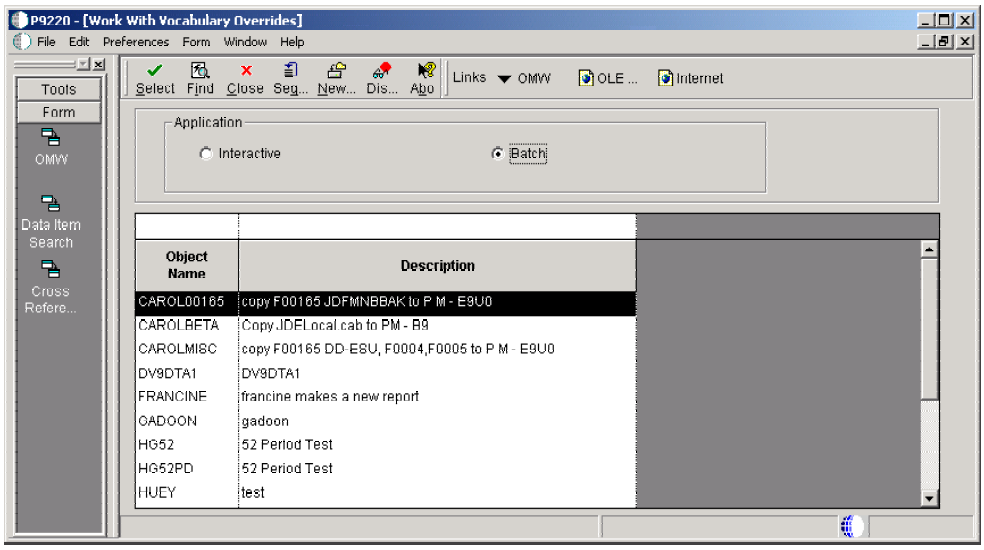
You can access the Vocabulary Overrides application from either an ERP 9.0 Explorer menu (System Administration Tools) or from within Object Management Workbench.

► To access Vocabulary Overrides from System Administration Tools

From System Administration Tools (GH9011), choose Vocabulary Overrides (P9220).

1. On Work With Vocabulary Overrides, click Interactive or Batch and click Find.

   Use the query by example fields to refine your search.



2. Choose an application and click Select.

   If the application you chose is checked out, you will get 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 will have to create vocabulary overrides for this application at another time or contact the users of the application to see if they can check in or erase their checkout.

3. If the SAR Requirement form appears, complete the following field:

   - SAR Number

   Enter a SAR number. 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.

► To access Vocabulary Overrides from Object Management Workbench

In the Fast Path, type OMW and press Enter.

1. On the Object Management Workbench form, click Find and then click Objects.
2. Choose an interactive or batch application, and then click the Design button.

The Object Librarian Interactive Application Design form or the Object Librarian Batch Application Design form appears.

3. On the Design Tools tab, click Vocabulary Overrides.

   The following Vocabulary Override Warning appears: 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 on the Vocabulary Override Warning.
5. If the SAR Requirement form appears, complete the following field:

   - SAR Number

     Enter a SAR number. This form 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

You can create vocabulary overrides to customize your interactive and batch ERP 9.0 applications. After you make vocabulary override changes, use an update package to push these changes to your 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 your users.

You do not need to rebuild the application before building it into a package if the only change to the application is due to vocabulary overrides.

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.

► To create interactive vocabulary overrides

Note

To access the Vocabulary Overrides form, see *Accessing Vocabulary Overrides* in the *System Administration Guide*.

1. To work with a language other than the domestic language, on Interactive Vocabulary Overrides, complete the following field, and then click Find:
   - Language
2. Enter a language code. Leave this field blank if you are creating vocabulary overrides in your domestic language.
3. Double-click the + icon 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 + icon 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), choose the data item row and, from the Row menu, choose 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 check out the application to the local client machine and run it. Do this by clicking either the Check Out or Get button in the Object Management Workbench.

See Also

- *Object Management Workbench* and *Checkout Log* in the *Development Tools Guide* for more information about how ERP 9.0 checks objects in and out

► To create batch vocabulary overrides

Note

To access the Vocabulary Overrides form, see *Accessing Vocabulary Overrides* in the *System Administration Guide*.

1. To work with a language other than the domestic language, on Batch Vocabulary Overrides, complete the following field, and then click Find:
   - Language
2. Enter a language code. Leave this field blank if you are creating vocabulary overrides in your base (domestic) language.
3. Double-click the + icon 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 plus (+) sign icon 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.

Reviewing Vocabulary Overrides

You can use vocabulary overrides to review every location in ERP 9.0 where someone has overridden a data item. You can view the override locations from a form or from a report.

► To review Vocabulary Overrides

From System Administration Tools (GH9011), choose Vocabulary Overrides (P9220).

1. On Work With Vocabulary Overrides, from the Form Exit menu, choose Data Item Search.
2. On the Overridden Data Item Search form, complete the following fields, and then click OK:
   - Data Item

   Enter a Data Item to search for.
3. Complete one of the following to choose a scope for the Application search:
   - Interactive Application
   - Batch

- Both

4. Choose one of the following options for your output results:

   - Interactive

     If you choose to view your search 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 choose to view your search using the printed report, an Adobe Acrobat Portable Document Format (PDF) file is created, which you can view or print.

Resetting Vocabulary Overrides

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, ERP 9.0 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).

Before You Begin

- ❑ Access the Vocabulary Overrides application. See *Accessing Vocabulary Overrides* in the *System Administration Guide*.

► To reset a vocabulary override

1. On the Work With Vocabulary Overrides form, click one of the following options and click Find:

   - Interactive
   - Batch

2. Choose an application and click Select.

   Depending on the application type, one of the following forms appears:

   - If you chose an interactive application, the Interactive Vocabulary Overrides form appears. The forms associated with the application appear in the detail area of this form.
   - If you chose a batch application, the Batch Vocabulary Overrides form appears. The versions associated with the application appear in the detail area of this form.

3. Double-click the + icon in the row header for one of the forms or versions in the detail area, and then double-click the + icon 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.

4. Choose the data item that you want to reset, and then, from the Row menu, choose Reset Description.

   Note
   The Reset Description menu option is inactive if a vocabulary override does not exist for the data item.

5. 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.

► To reset all vocabulary overrides on a form (interactive)

1. On the Work With Vocabulary Overrides form, click the Interactive option and then click Find.
2. Choose an application and click Select.

   The detail area of the Interactive Vocabulary Overrides form displays all forms within the application.

3. Choose a form and then, from the Row menu, choose Reset by Form.

   ERP 9.0 clears all vocabulary overrides from the form and resets the data items to the data dictionary definitions.

   Caution
   When you choose the Reset by Form menu option, the decision is final; ERP 9.0 does not provide a confirmation box or a proof mode.

► To reset all vocabulary overrides in a version (batch)

1. On the Work With Vocabulary Overrides form, click the Batch option and then click Find.
2. Choose an application and click Select.

   The detail area of the Batch Vocabulary Overrides form displays all versions for the application.

3. Choose a version and then, from the Row menu, choose Reset by Version.

   ERP 9.0 clears all vocabulary overrides from the version and resets the data items to the base definitions. If no base definition exists for a data item, ERP 9.0 resets the data item to the default data dictionary definition.

Caution
When you choose the Reset by Version menu option, the decision is final; ERP 9.0 does not provide a confirmation box or a proof mode.

► To reset all vocabulary overrides in an application (interactive and batch)

1. On the Work With Vocabulary Overrides form, click one of the following options and then click Find:
   - Interactive
   - Batch
2. Choose 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, choose the Reset by Application menu option for interactive applications or the Reset by Batch menu option for batch applications.

   ERP 9.0 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, ERP 9.0 resets the data item to the default data dictionary definition.

Caution
When you choose either the Reset by Application or the Reset by Batch menu option, the decision is final; ERP 9.0 does not provide a confirmation box or a proof mode.

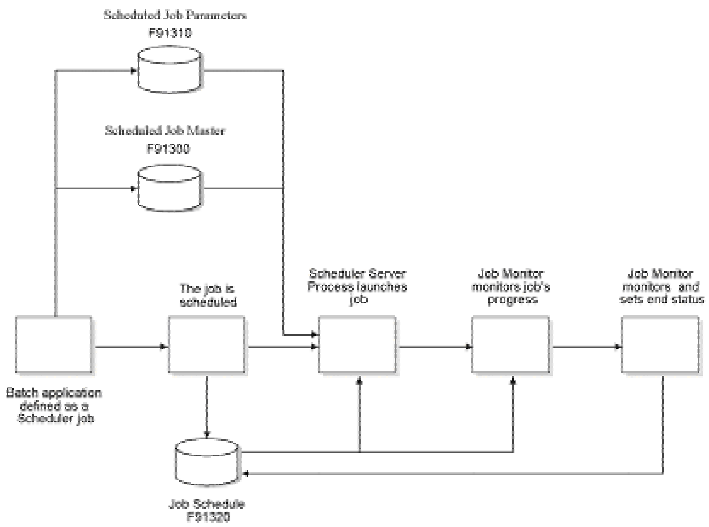
The Scheduler Application

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:



When you define a scheduled job, the parameters of that job are stored in the Schedule Job Master table (F91300).

After the job is scheduled, the system writes records to the Job Schedule table (F91320), 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.

Scheduling Jobs

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 schedule jobs in the local time of the server on which the job will run.

See Also

See the following topics in the *System Administration Guide*:

- *Scheduling a Recurring Job* for information about automating the job schedule
- *Working with Job Properties* for information about changing the properties of a job
- *Entering Scheduler Processing Options* for information about changing the Scheduler options

Before You Begin

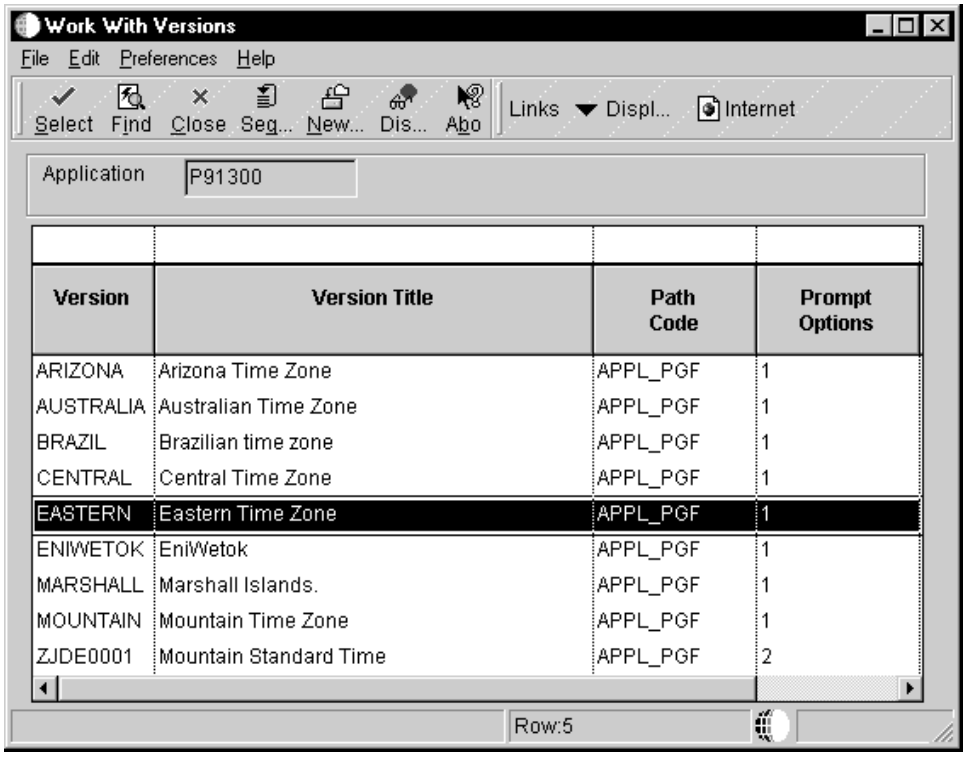
- To use a server's time zone, you must first specify the time zones that you want to use. To do this, copy the Scheduler processing options (version ZJDE0001 on the Work with Versions form) and modify them according to your needs. If you use more than one time zone, you should modify the processing options to display the Work with Versions form each time that you invoke the Schedule Jobs application. That way, you can choose the correct version for the time zone in which you want to schedule the job.

Scheduling a Job

When you schedule a job, you choose the version of Scheduler that specifies the time zone in which the job will be run, and then you define the parameters of the job. For example, if you want to submit a job from your workstation in Germany that will run on a server in Australia, you would choose the version that specifies the time zone for Australia so that the job runs at the intended time.

► To schedule a job

From the System Administration Tools menu (GH9011), choose Job Scheduler (GH9015), and then choose Schedule Jobs (P91300). The Work With Versions form appears.

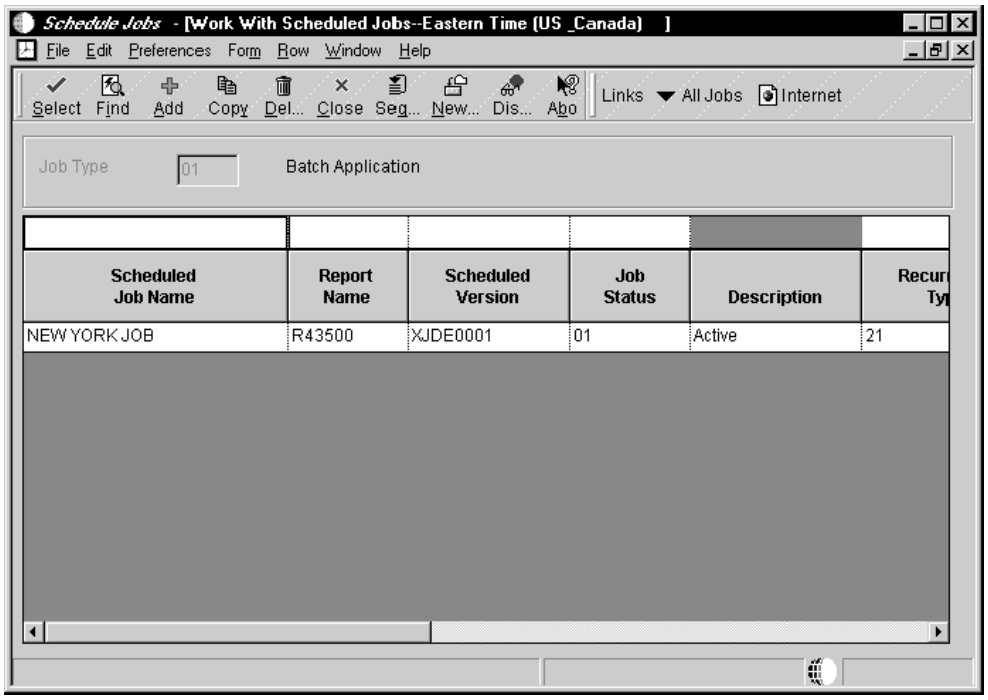


Note
If you use only one time zone, you might not be prompted to choose a version. In this case, the Work With Versions form does not appear and you can skip the following step. You can delete the Work With Versions form in the menu properties for P91300. We ship GH9015/P91300 to prompt for the version.

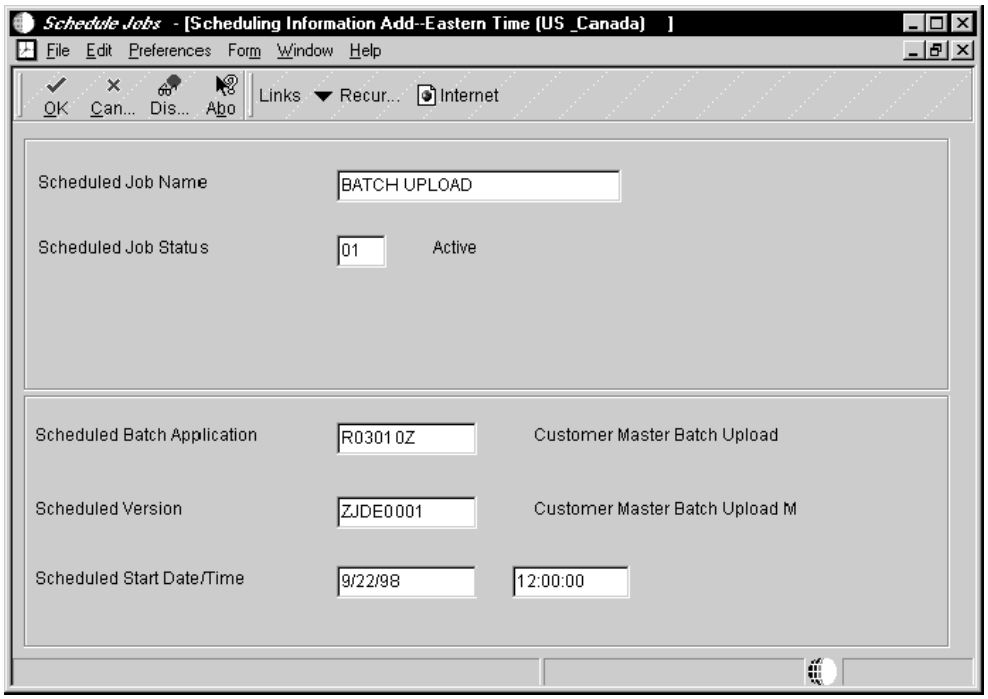
1. On Work With Versions, double-click the version that specifies the time zone in which the scheduled job will run.

   For example, you might choose the version that specifies the Eastern Time Zone to run jobs in Eastern Standard Time (EST).

Note
When you choose version ZJDE0001, you can enter Scheduler processing options. For more information about entering processing options, see *Entering Scheduler Processing Options* in the *System Administration Guide*.



2. On Work With Scheduled Jobs, click Add.



3. On the Scheduling Information Add form, complete the following fields:
    - Scheduled Job Name

- Scheduled Job Status
- Scheduled Batch Application
- Scheduled Version
- Scheduled Start Date/Time

4. Click OK.

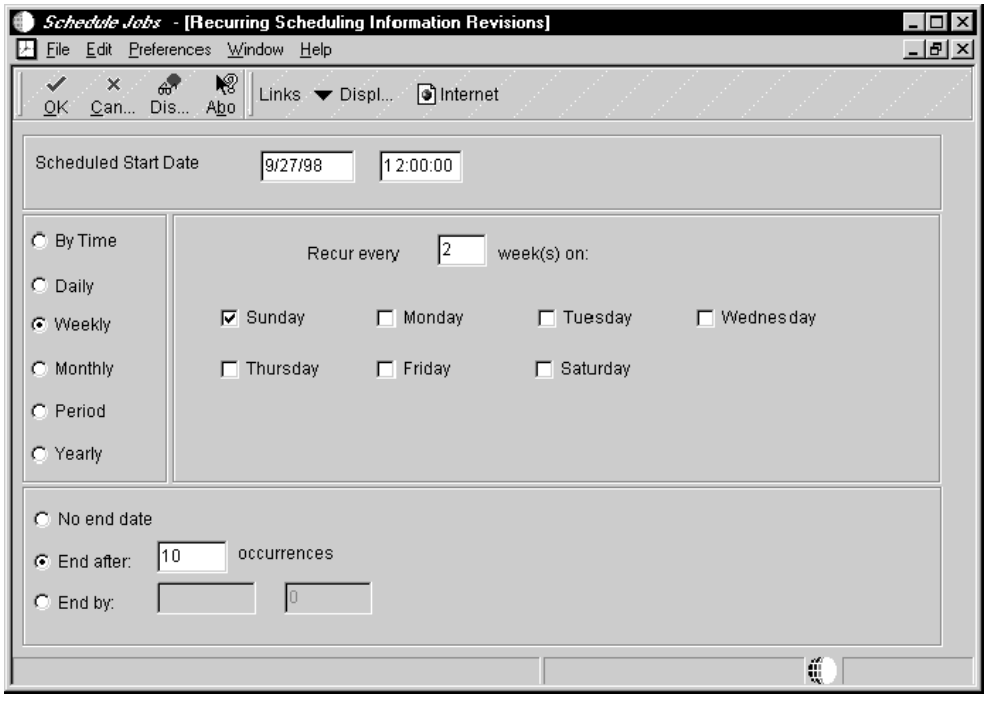
Scheduling a Recurring Job

You might need to run jobs more than once. You can set the frequency of recurrence for a scheduled job so that it runs hourly, weekly, biweekly, monthly, and so on. 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.

► To schedule a recurring job

From the System Administration Tools menu (GH9011), choose Job Scheduler (GH9015), and then choose Schedule Jobs (P91300).

1. On the Work With Versions form, 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 the Schedule Information Add form, choose Recurrence from the Form menu.



4. On Recurring Scheduling Information Revisions, choose one of the following options and complete the accompanying fields that appear after you choose an option:
   - By Time

Every *n* days OR

Every weekday

Run the job at the specified time interval. For example, run the job every 40 minutes or every 8 hours.

- Daily

Run the job at the specified interval of days or every weekday. For example, run the job every 7 days or every weekday.

- Weekly

Recur every *n* week(s) on

Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday

Run the job at the specified weekly interval on the specified day of the week. For example, run the job every 2 weeks on Monday.

- Monthly

Day *n* of every *x* month(s) or

The [first, last, and so on] [day, Sunday, Friday, and so on] of every *n* month(s)

Run the job on the specified day of every *n* month or on a specific day of every *n* month. For example, run the job on day 1 of every 4 months or on the last Friday of every second month.

- Period

Day *n* of every *x* period(s) OR

The [first, last, and so on] [day, Sunday, Friday, and so on] of every *n* period(s)

- 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. For example, run the job every January 1 or on the first Monday of June or on day 15 of the last period or on the second Tuesday of the fourth period.

5. Specify when you want the Scheduler to stop submitting the job by turning on one of the following options:
    - No end date

- End after:

Where *x* is the number of occurrences of that job that can run before it expires.

- End by:

  Enter the month, day, and year on which you want the job to expire.

6. Click OK.

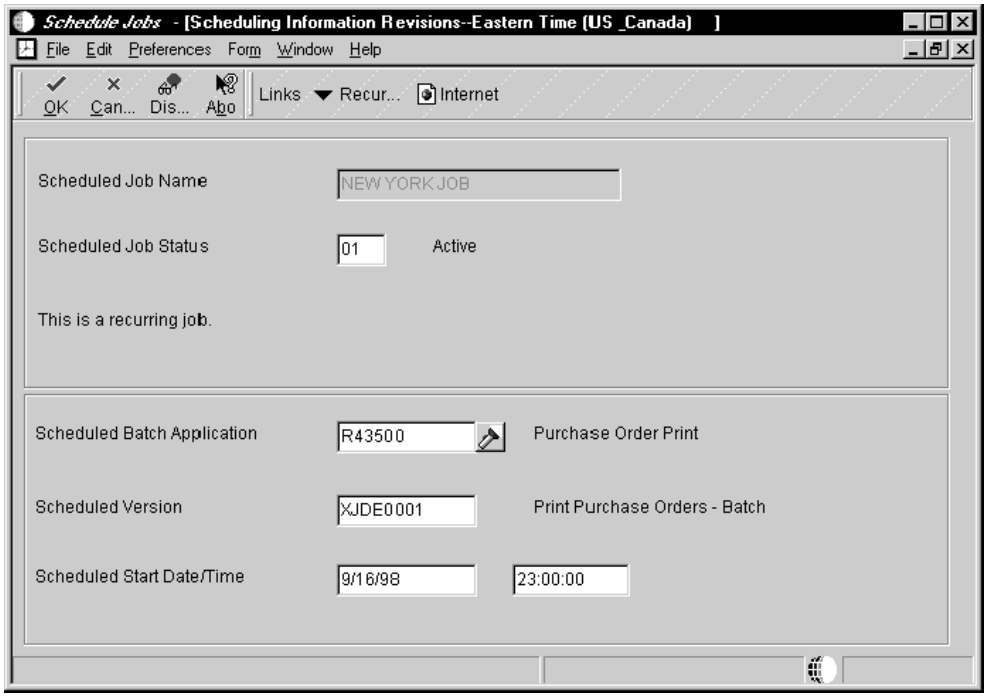
Revising a Scheduled Job

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; or you might want to enter a new batch process as the scheduled job, or change the job start date and time.

► To revise a scheduled job

From the Job Scheduler menu (GH9015), choose Schedule Jobs.

1. On Work With Versions, choose the version that specifies the time zone in which the job will run and click Select.
2. On Work with Scheduled Jobs, choose the job that you want to revise, and then choose 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 Application

- Scheduled Version
- Scheduled Start Date/Time

4. If you want to remove recurrence from a scheduled job, choose Remove Recurrence from the Form menu.
5. If you want to add category codes to the scheduled job, choose Category Codes from the Form menu.

   The form appears.

   386869]
6. On Scheduler Category Codes, if you want to revise the advanced options for this job, choose Advanced Options from the Form menu.

   The Scheduling Advanced Options form appears.

   709764]

Notes

For information about entering advanced options, see *Working With Job Properties* in the *System Administration Guide*.

You can also activate or inactivate a job by choosing the job on Work With Scheduled Jobs, and then choosing Change Status from the Row menu.

Entering Scheduler Processing Options

The Scheduler processing options enable you to specify preferences and defaults for time zone, job recurrence, and job type. You can enter or change processing options two ways:

- Choose version ZJDE0001 from the Work With Versions form.
- From the Job Scheduler menu (GH9015), highlight Schedule Jobs, right-click, and then select Prompt for Values.

The Scheduler processing options form has three tabs that allow you to change the following parameters:

Display

Enter time zone information.

Process

Enter information about schedule records.

Defaults

Enter information about job type, job occurrences, and job resubmissions.

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 would protect the Local Jobs choice and allow you to choose only All Jobs.

► To review all jobs or local jobs

1. On the Work With Scheduled Jobs form, choose Display from the Form menu.
2. Choose either All Jobs or Local Jobs.

Working with Job Properties

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

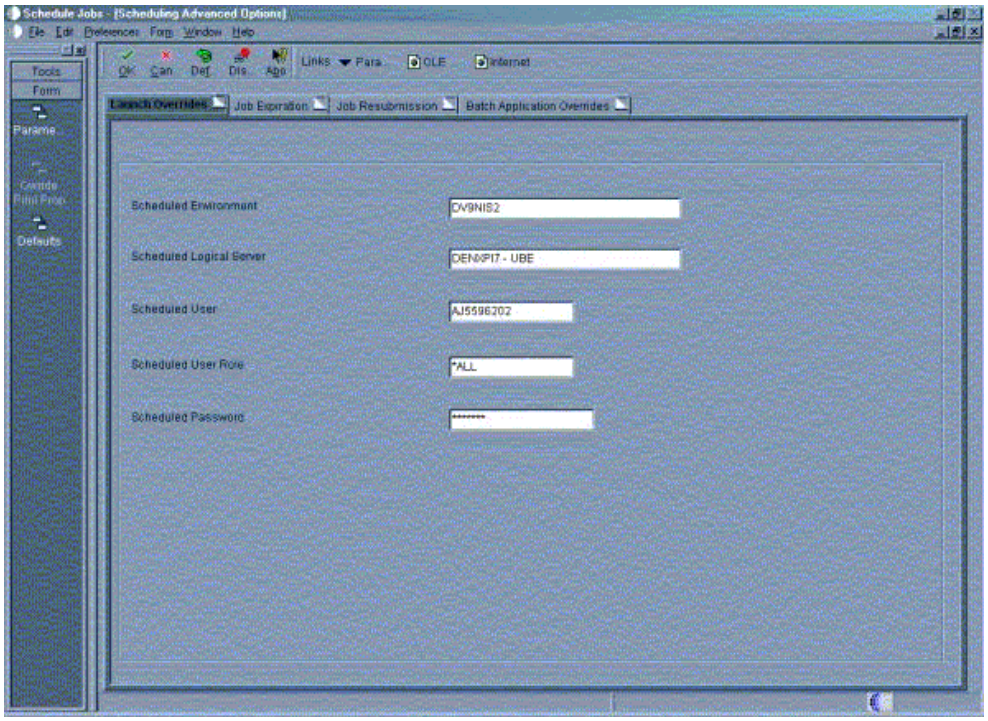
To restore the default values in the advanced options application, click the default button on Scheduling Advanced Options.

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.

► To override the environment

1. On the Work With Scheduled Jobs form, choose the job.
2. Choose Advanced Options from the Row menu.



3. On Scheduling Advanced Options, complete the following fields on the Launch Overrides tab as necessary:
    - Scheduled Environment
    - Scheduled Logical Server
    - Scheduled User
- Scheduled User Role
    - Scheduled Password

    Type the password of the scheduled user in this field.

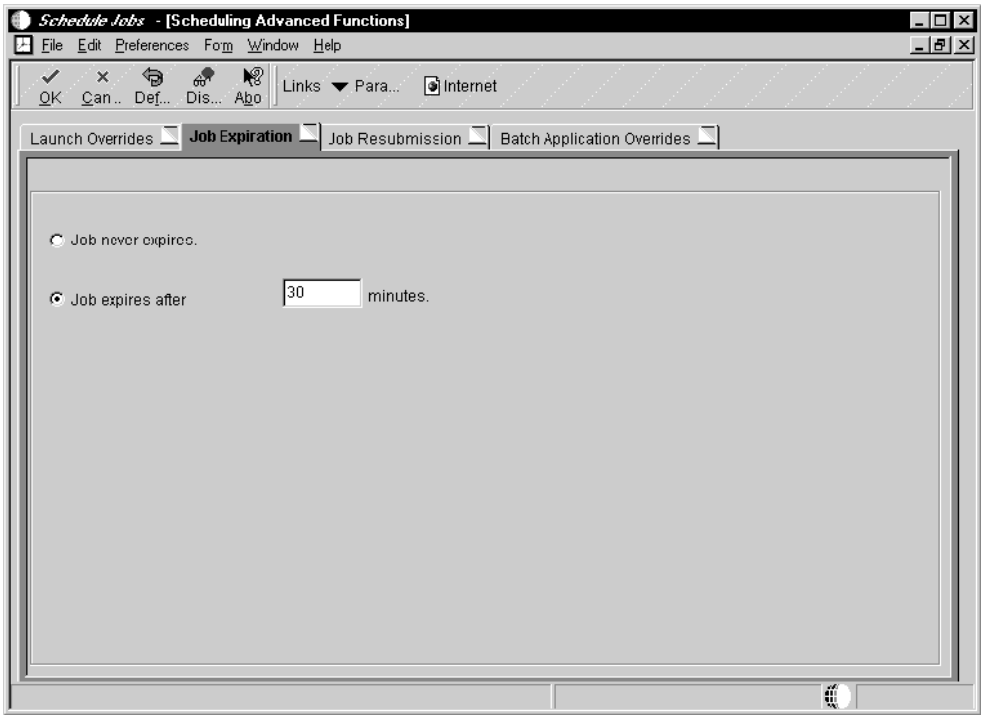
Overriding Job Expiration Specifications

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, will expire in 30 minutes (12:30 a.m.), so that if the server does not come back up within 30 minutes, the job will expire.

► To override job expiration specifications

1. On the Work With Scheduled Jobs form, choose the job, and then choose Advanced Options from the Row menu.
2. On the Scheduling Advanced Options form, click the Job Expiration tab.



3. Indicate whether you want the job to never expire or to expire after a specified time has elapsed.
4. Click OK.

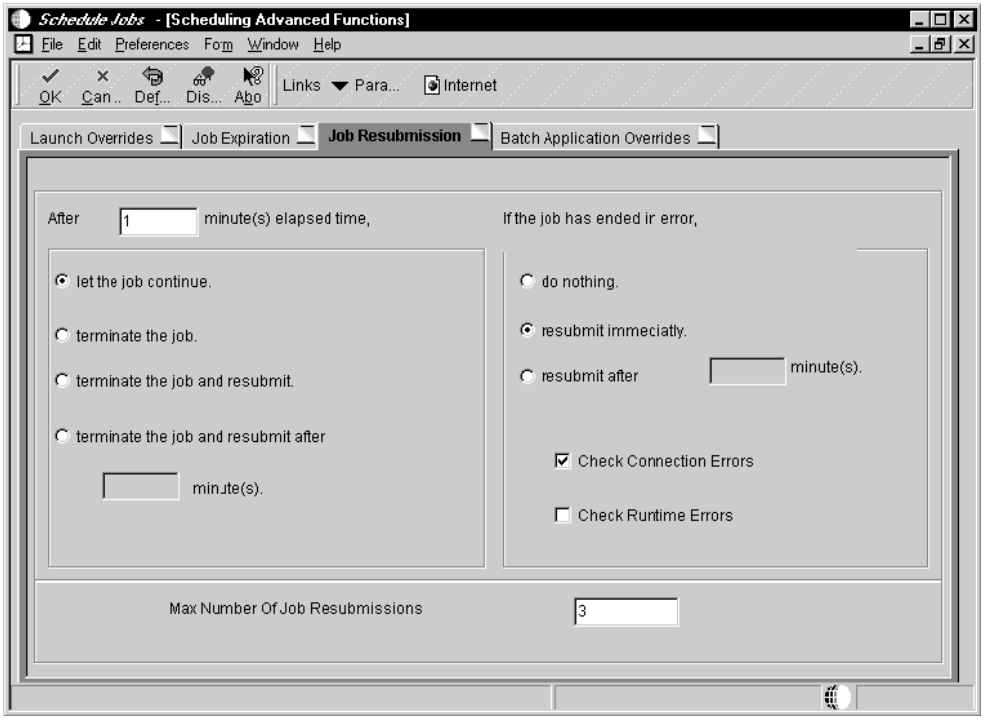
Defining When the Scheduler Resubmits a Job

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 run-time errors when the job runs. Connection errors occur when the system fails to connect to the server to submit the job. Run-time 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.

► To define when the system resubmits jobs

1. On the Work With Scheduled Jobs form, choose the job and then choose Advanced Options from the Row menu.
2. On Scheduling Advanced Options, click the Job Resubmission tab.



3. Specify the number of minutes that elapse before the job continues or terminates, and then turn on one of the following options:
    - let the job continue.
    - terminate the job.
    - terminate the job and resubmit.
4. If you want to terminate the job and resubmit it after a certain period of time, choose the following option and enter the number of minutes that you want to elapse before the system resubmits the job:
    - terminate the job and resubmit after
5. Choose one of the following options that apply when the job ends in error:
    - do nothing.
    - resubmit immediatly.
    - resubmit after
6. Specify whether you want the system to check for connection errors, runtime errors, or both.
7. Complete the following field:
    - Max Number Of Job Resubmissions

    Specify the maximum number of times that you want the job to be resubmitted.
8. Click OK.

Overriding Batch Application Specifications

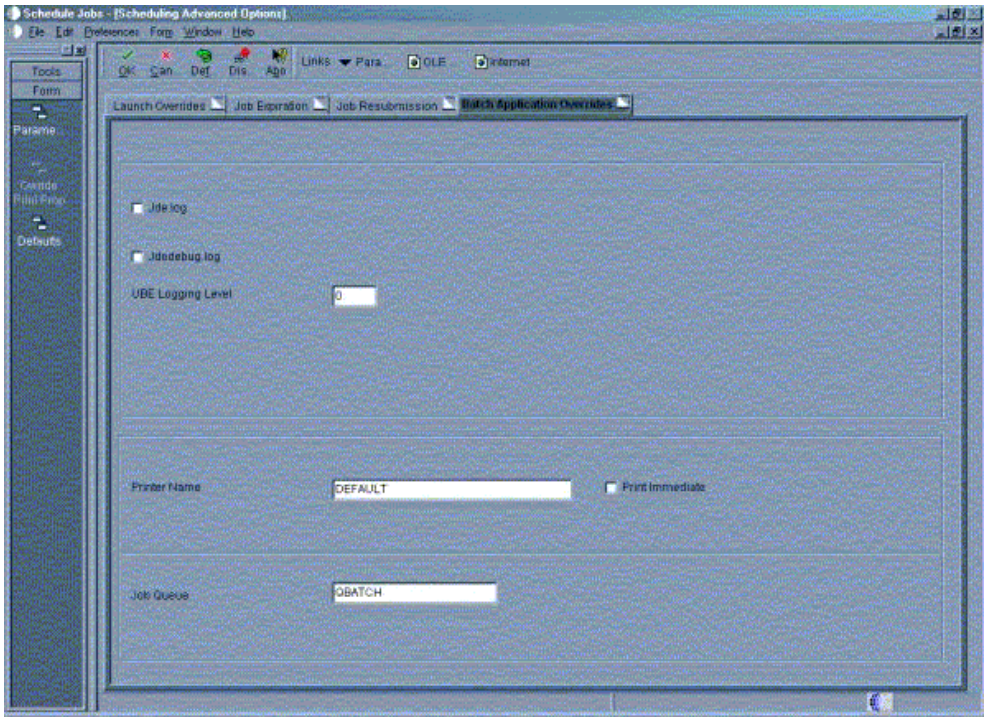
You can specify if you want errors written to the `jde.log`. If you want errors written to the `jdedebug.log`, you can set the trace level to determine what types of errors to include in the log.

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 whether the job should be 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.

► To override batch application specifications

1. On the Work With Scheduled Jobs form, choose the job, and then choose Advanced Options from the Row menu.
2. On Scheduling Advanced Options, click the Batch Application Overrides tab.



3. Choose one or more of the following options:
   - `Jde.log`
   - `Jdedebug.log`

     If you choose jdedebug.log, you must also choose the jde.log option.
4. Complete the following fields:

- UBE Logging Level

  If you choose jdedebug.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 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, turn on the Print Immediate option.

- Job Queue

  Enter the name of the job queue to which you want the job output sent.

5. Click OK.

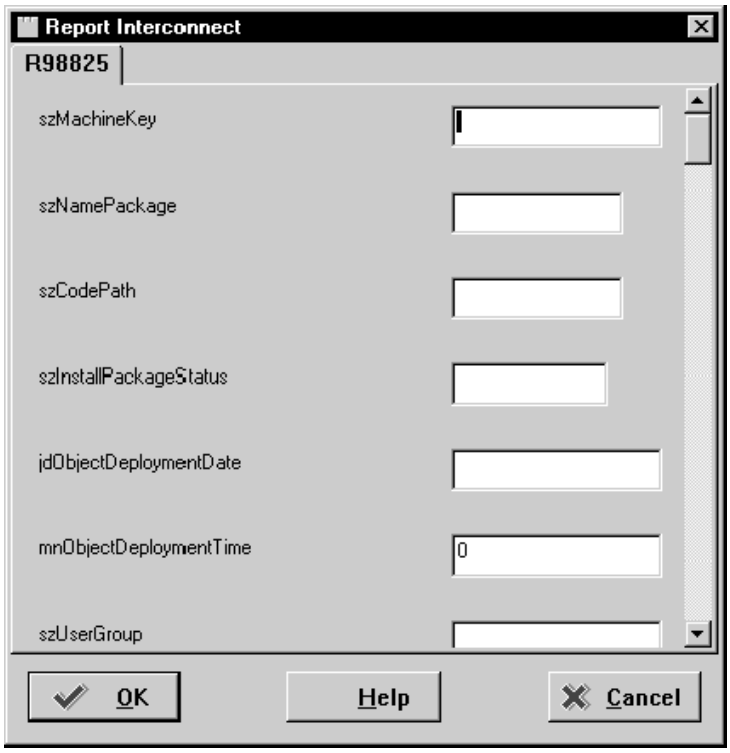
Adding Values to a Report Interconnect

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.

► To add values to a report interconnect

1. On the Work With Scheduled Jobs form, choose the job and then choose Advanced Options from the Row menu.
2. On Scheduling Advanced Options, choose Parameters from the Form menu.

   The system displays the Report Interconnect form with the parameters for that particular batch process.



3. Enter the values that you want to pass to the batch process when the process runs.
4. Click OK.

Working with the Job Schedule

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 Job Schedule table (F91320). The Job Schedule 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 job schedule table is also used for audit information, you can modify or delete only jobs that have not yet run.

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.

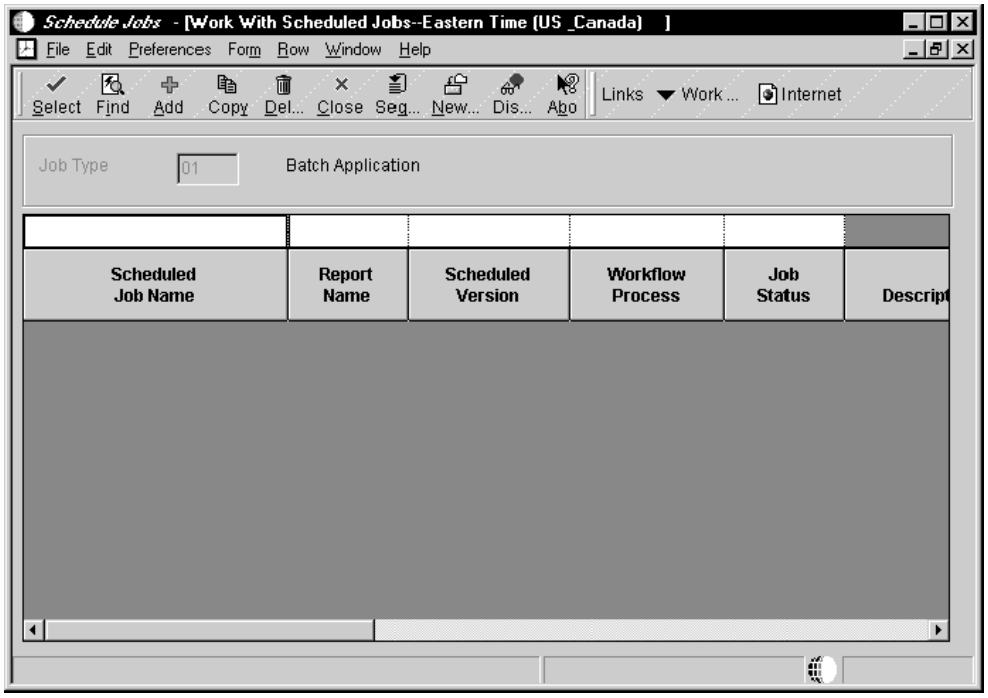
You can filter the job instances that you want to review by launch date, start date, and time. For example, you can review all of the job instances for today's date by entering that date in the Scheduled Start Date field. Or you can review all job instances that were launched on a certain date by entering 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.

See Also

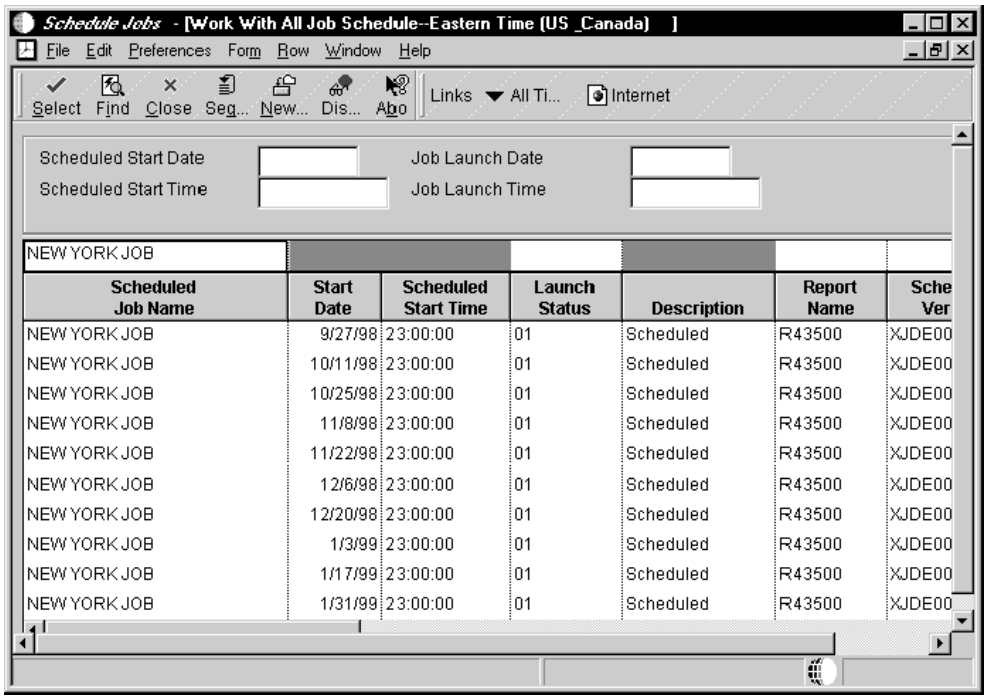
- *Revising a Scheduled Job* in the *System Administration Guide* for more information about revising the job schedule

► To review all job schedules

From the Job Scheduler menu (GH9015), choose Schedule Jobs.



1. On Work With Scheduled Jobs, choose All Schedules from the Form menu.



2. On Work With All Job Schedule, filter by start date or start time by completing the following fields:
    - Scheduled Start Date
    - Scheduled Start Time
3. To filter by launch date or launch time, complete the following fields:
    - Job Launch Date
    - Job Launch Time
4. To filter by job name, launch status, report name, or scheduled version, complete the following fields:
    - Scheduled Job Name
    - Launch Status
    - Report Name
    - Scheduled Version
5. To view all scheduled jobs in all time zones, choose All Time Zones from the Form menu.
6. To view all scheduled jobs in the local time zone, choose Local Time Zone from the Form menu.

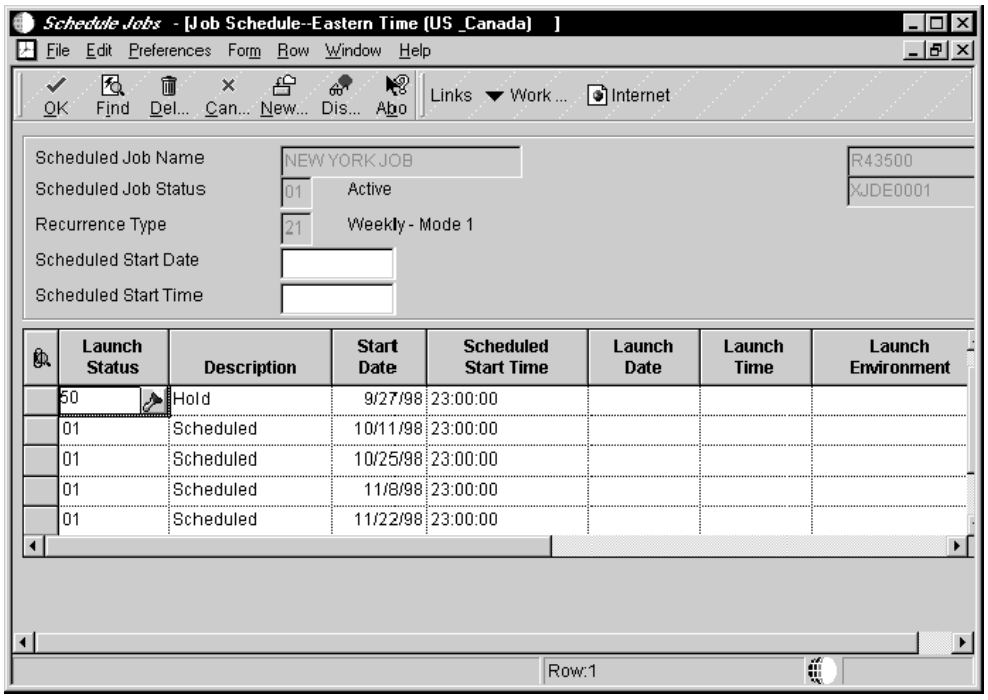
Changing the Launch Status of a Job

You can change the launch status of a job. You might need to put a job on hold or reschedule a job.

► To change the job launch status of a job

From the Job Scheduler menu (GH9015), choose Schedule Jobs.

1. On Work With Versions, choose 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, choose Job Schedule.



4. On Job Schedule, choose the job instance whose launch status you want to change, and then enter a new status in the Launch Status field.

   Enter 1 for Scheduled or 50 for Hold.

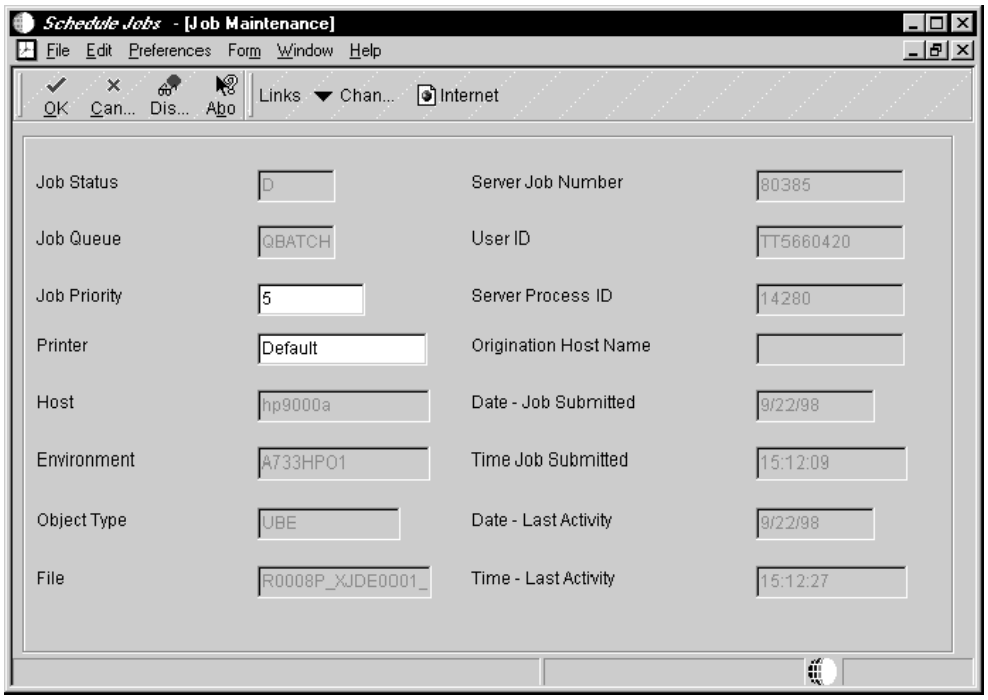
5. Click OK.

Viewing Job Details

On the Job Maintenance form, you can 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.

► To view job details

1. On the Job Schedule form, choose the job and then choose 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

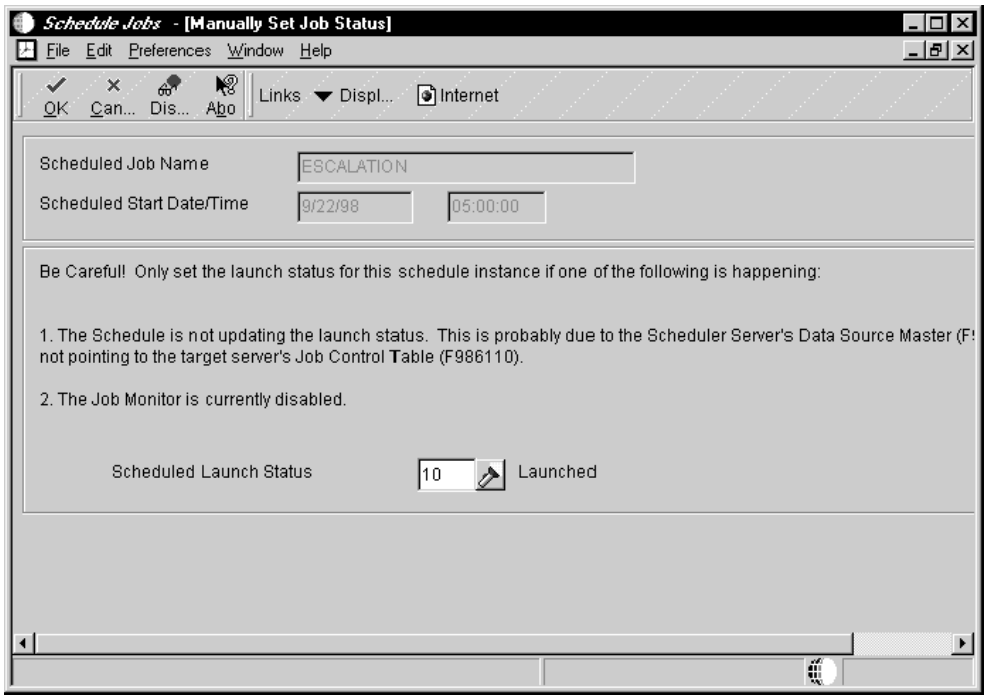
If you need to stop a job, choose Work with Servers from the Form menu on the Work with Scheduled Jobs form.

Caution

You should secure other users from accessing the Set Status option. Only the ERP 9.0 administrator should have access to this option.

► To set the job status manually

1. On the Work With Scheduled Jobs form, choose the job and then choose Job Schedule from the Row menu.
2. On Job Schedule, choose the job instance for which you want to manually set the job status, and then choose Set Status from the Row menu.



3. On Manually Set Job Status, complete the following field:
    - Scheduled Launch Status

Resetting the Job Schedule

If you customize a job schedule and then change your mind, you can remove the changes and regenerate the job schedule using the previously defined recurrence pattern. The job schedule will be reset to the way that it was before you made the changes.

► To reset the job schedule

1. From the Job Schedule form, choose Reset Schedule from the Form menu.

   The following warning message appears: 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.

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/user combination, based on the information in the Schedule Job Master table (F91300). 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).

See Also

- *Creating a Report Interconnection* in the *ERP 9.0 Development Tools Guide*
- *Debug Tracing* in the *ERP 9.0 Development Tools Guide* for information about setting trace levels

Control Record

A control record is a job record in the Schedule Job Master table (F91300). 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 will set 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 will find the flag, reset both flags, and end.

If the system does not find the control record when it is fetched, the record is re-created by P91300 when entering the Scheduler Server Control form. In addition, if the record is corrupt, the function above is called to re-create it. The sleep times for the job monitor will be reset to 15 minutes, and the audit information in this record will be 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) will be set to the difference between the current time and the start of the next job. If the fetch fails, the NST will be set to zero, which indicates that this function should be run the next time that any record is added to or updated by the Job Schedule table (F91320). 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

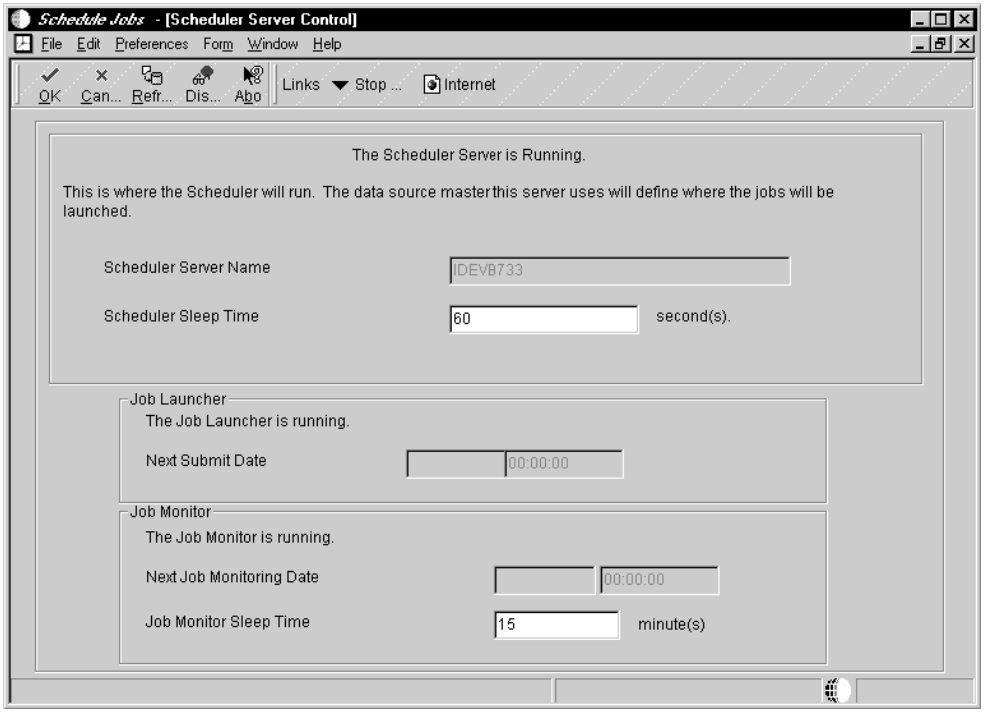
The job monitor loop monitors the ending statuses of the launched jobs and re-launches those that end in error if requested to do so by the user. This loop cycles through the internal job list that the job launch loop populates. In addition, it terminates jobs that run too long, if requested to do so. 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.

► To stop or restart the Scheduler server

From the Job Scheduler menu (GH9015), choose Schedule Jobs (P91300).

1. On Work with Versions, choose the version that specifies the time zone in which the scheduled jobs run, and then click Select.
2. On Work with Scheduled Jobs, choose Scheduler Server from the Form menu.



3. On Scheduler Server Control, do one of the following:
   - To stop the server, choose Stop Scheduler from the Form menu.
   - To restart the server, choose Start Scheduler from the Form menu.
4. Click OK.

► 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 that you submit jobs to 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, choose Pause Job Launcher from the Form menu to pause the job launcher.
2. To pause the job monitor, choose Pause Job Monitor from the Form menu.
3. Click OK.

► 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 choose Reset to refresh the settings on the server.

1. On Scheduler Server Control, choose Reset from the Form menu.
2. Click OK.

► 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 kind of internal 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, choose Refresh from the Form menu.
2. Click OK.

► To modify the Scheduler server and monitor sleep time

Note

Sleep time is the time that the Scheduler server or monitor is idle.

1. On Scheduler Server Control, complete the following fields, as necessary:
    - Scheduler Sleep Time
    - Job Monitor Sleep Time
2. Click OK.

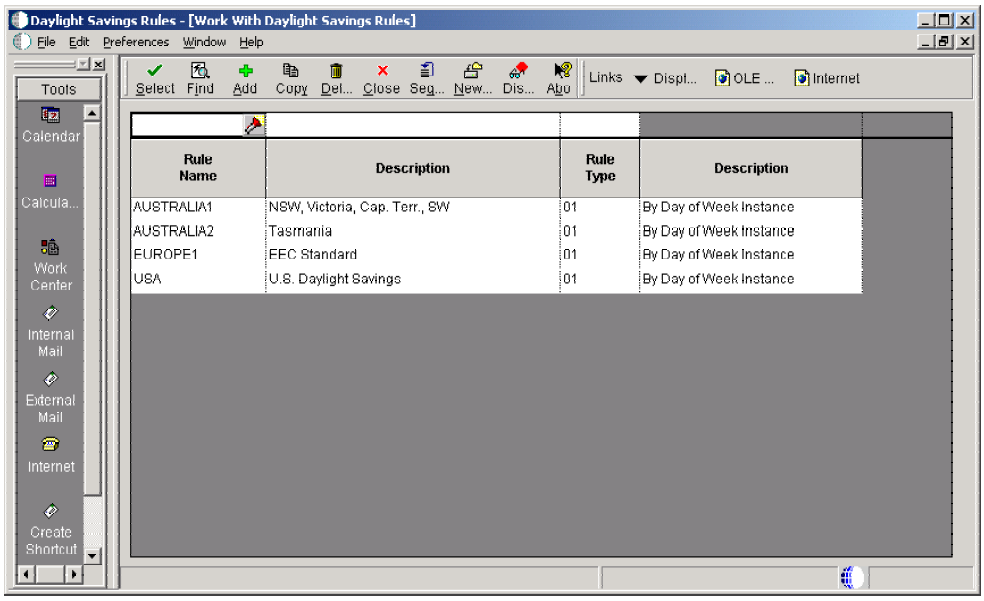
Modifying Daylight Savings Rules

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 be run on a particular server.

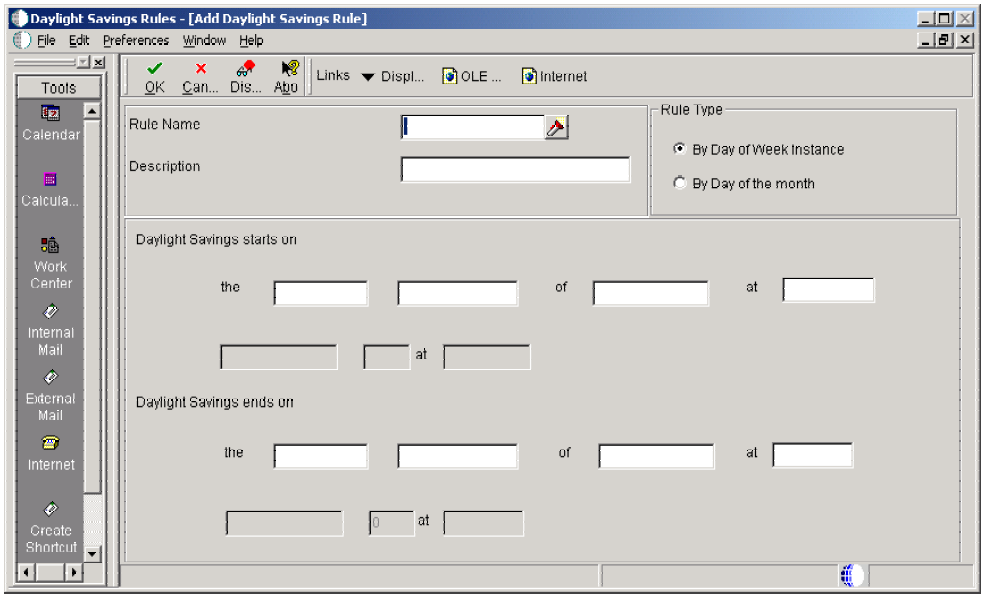
You can add a new daylight savings rule or modify an existing one.

► To add a new daylight savings rule

From the Job Scheduler menu (GH9015), choose Daylight Savings Rules (P00085).



1. On Work With Daylight Savings Rules, click Add.

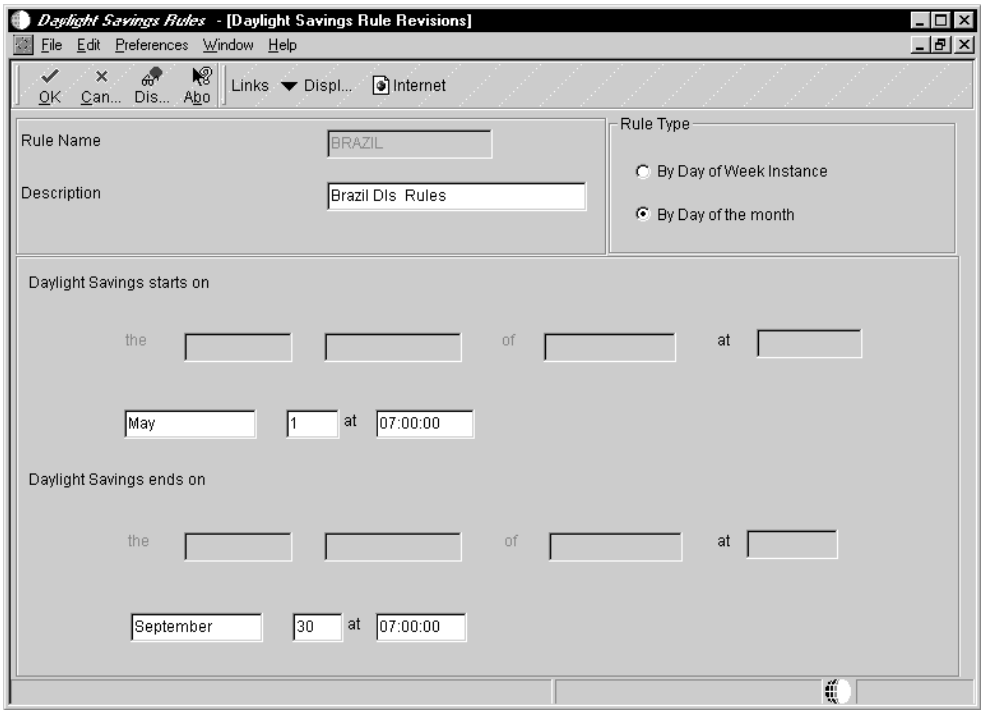


2. On Add Daylight Savings Rule, complete the following fields:
    - Rule Name
    - Description
3. Choose one of the following rule types:
    - By Day of Week Instance
    - By Day of the month
4. Enter the dates that daylight savings time begins and ends, and then click OK.

► To modify an existing daylight savings rule

From the Job Scheduler menu (GH9015), choose Daylight Savings Rules (P00085).

1. Choose the rule that you want to modify, and then click Select.



2. On Daylight Savings Rule Revisions, add a new description, if necessary, in the following field:
    - Description
3. Choose one of the following rule types:
    - By Day of Week Instance
    - By Day of the month
4. Modify the dates and times that daylight savings time begins and ends, and then click OK.

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 Universal Coordinated Time (UCT) or local time. You also can adjust for daylight savings time.

If you want to purge records from the Job Schedule table (F91320), run the Scheduler Purge program. You can run the purge program in proof mode and final mode.

See Also

- *Submitting a Report* in the *Enterprise Report Writing Guide* for general information about reports

► To print the Scheduled Jobs or Purge Scheduled Jobs report

From the Job Scheduler menu (GH9015), choose Print Scheduled Jobs (R91300A) or Purge Scheduled Jobs (R91300B).

1. On the Work With Batch Versions form, choose a version in the detail area, and then click Select.
2. On Version Prompting, choose one or both of the following options, and then click Submit:
    - Data Selection
    - Data Sequencing
3. On Report Output Destination, choose one of the following options, and then click OK:
    - On Screen
    - To Printer

Working with the Scheduler Server

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 turn on or turn off 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 that the Scheduler server is running on 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 Job Schedule table (F91320) to determine if it should restart on that particular 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 ERP 9.0 administrators only. You should secure users from accessing the Scheduler server application.

See Also

- *The jde.ini File* in the *System Administration Guide* for more information about the autostart function
- *Security* in the *System Administration Guide* for more information about security

Media Objects and Imaging

ERP 9.0's media objects and imaging features allow you to attach useful information to an application, including information that might currently exist as a paper-based document. The media objects feature allows you to attach the information to ERP 9.0 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.

What Are Media Objects?

Media objects link information to applications, either to individual rows in a detail area or to a form. The types of information that you can attach to a grid row or a form are described below:

Text

Media objects provide a word processor that lets you create a text-only attachment. For example, you could 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 Joint Photographic Experts Group (JPG) files. These files might represent electronically created files as well as scanned images of paper-based documents.

Object Linking and Embedding (OLE)

Media objects can be files that conform to the OLE standard. OLE allows you to create links between different programs. Using these links, you can create and edit an object from one program in a different program. ERP 9.0 provides the links that you need to attach OLE objects.

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.

You can only use OLE objects that you properly register and install as OLE objects through ERP 9.0.

JDE Shortcuts

A JDE shortcut is a link that opens an ERP 9.0 application. Within media objects, you can only attach ERP 9.0 shortcuts; that is, you cannot attach Windows shortcuts to media objects.

Uniform Resource Locations (URL)/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. Also, you might create a shortcut in the template to provide access to an application that uses data which is specific to the information that you add to the template.

What Is Imaging?

The imaging capabilities available in ERP 9.0 allow you to link to a third-party imaging product. Imaging systems allow 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. ERP 9.0 imaging integration includes a Media Objects viewer and a third-party product that provides scanning and searching interfaces to allow you to find and display images. ERP 9.0's implementation of imaging also provides a view of integrated images using the viewer of the native imaging product.

Enabling ERP 9.0 to Use Media Objects

To use media objects, ERP 9.0 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 ERP 9.0 objects (rows, forms, and reports)
- Indicating which ERP 9.0 objects have attachments
- Creating or viewing attachments

ERP 9.0 provides standard processing for media objects, which allows 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 does the following:

- Standardizes the usage of media objects across forms
- For any detail area, places a paper clip icon on the row header if a media object is defined for that row
- For a form, places an icon in the status bar if a media object is defined for the form
- Allows you to attach documents to the form or to a row in the detail area
- Allows you to double-click on the paper clip in a row to view media objects for that row
- Allows you to click on 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 your own system for handling media objects by using existing event rules or event rules that you develop.

ERP 9.0 uses the Media Objects Storage table (F00165) to store link records for media objects and imaging. You must define your media object data structure using a unique key structure so that the Media Objects Storage table can store data correctly. The layout of this table is as follows:

```
GT || F4211Keys || The media object text
```

Where:

`GT` (generic text) 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.

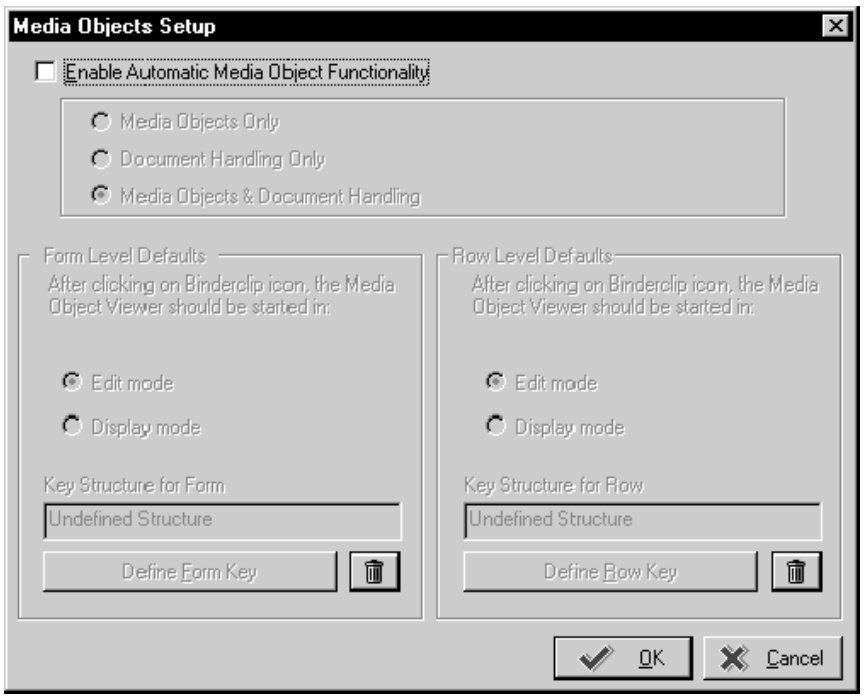
In addition to the media object categories provided by ERP 9.0, you can define as many as 40 more. Users can associate these categories with a media object to group certain media objects and to enable other users to search for specific media objects. User-defined categories reside in the Media Object Categories table (F00166) 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.

Before You Begin

- To see the media object paper clip column on a form, turn off the Hide Row Headers option on the Grid properties for the form.

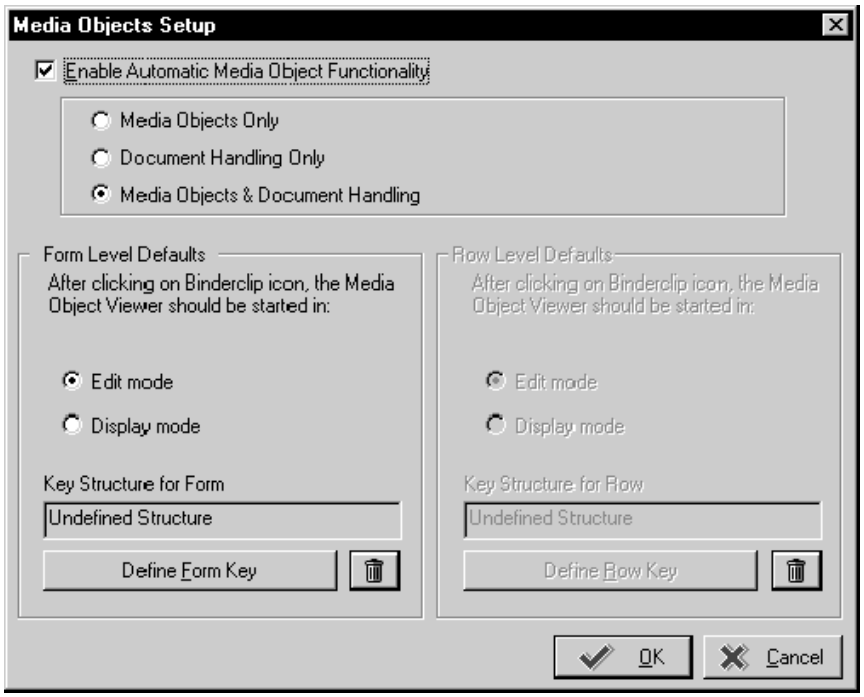
► To enable ERP 9.0 to use media objects

1. From Form Design Aid, right-click in the grid portion of an existing or newly created form and choose Properties.
2. On Grid Properties, turn off the Hide Row Headers option to enable you to see the media object paper clip column on a form.
3. From the form menu, choose Media Objects Setup.



4. On Media Objects Setup, turn on the Enable Automatic Media Object Functionality option.

   Turning on this option enables imaging and activates the other fields on the form.



5. On Media Objects Setup, click one of the following 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 ERP 9.0.

   - Document Handling Only

     Choose this option if you are developing a form that is enabled for media objects via functionality in event rules and you want to bypass standard processing.

   - Media Objects & Document Handling

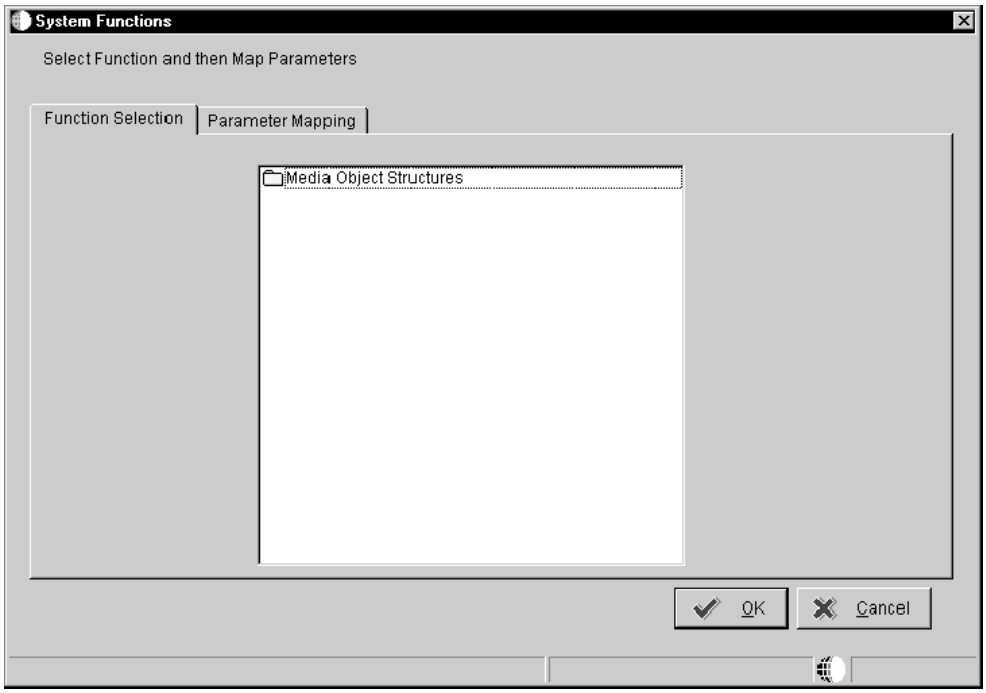
     Choose this option if you want to enable standard processing later. You must delete all of the event rules for media objects when you choose this option.

6. Click Edit mode or Display mode.

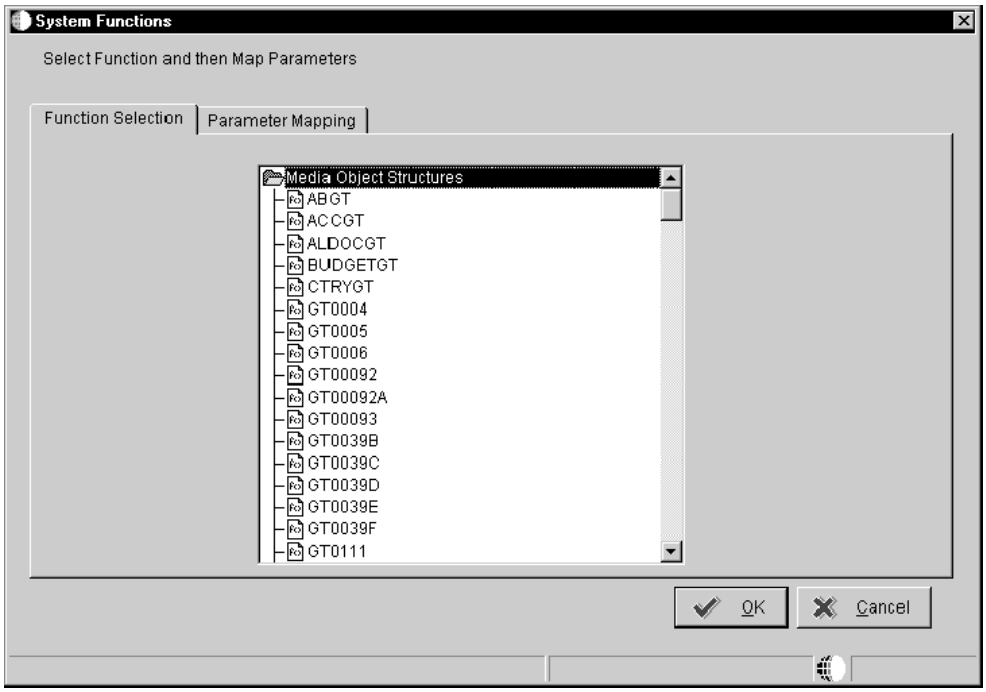
   Edit mode allows the user to make changes; display mode is read-only.

7. 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 only the Media Object Structures header is displayed.



8. On the Function Selection tab, double-click the Media Object Structures folder.
   A list of all currently defined data structures for Media Objects appears.



9. Choose the appropriate structure and define it.

Working with Media Object Queues

ERP 9.0 media object queues allow 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 your server can change, and the change is reflected in only one place in ERP 9.0.

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 ERP 9.0. Within ERP 9.0, 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 the following 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 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 using an OLE-compliant application outside of ERP 9.0. In ERP 9.0, 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 ERP 9.0 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 might 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 uniform resource locations (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 ERP 9.0 media object files, such as OLE objects and images. The two media object tables are Media Object Queues (F98MOQUE) and Imaging Constants (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 Media Objects Storage table (F00165). Media object characterization properties are stored in the Media Object Categories table (F00166). The Media Object Category Constant table (F00167) stores information indicating which categories the system activates for any given data structure.

ERP 9.0 Text Items

Text items are items that you create using the ERP 9.0 media objects word processor. They do not require media object queues. The Media Objects Storage table (F00165) 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 ERP 9.0 (for example, Microsoft Word or Wordpad) must be stored as OLE objects.

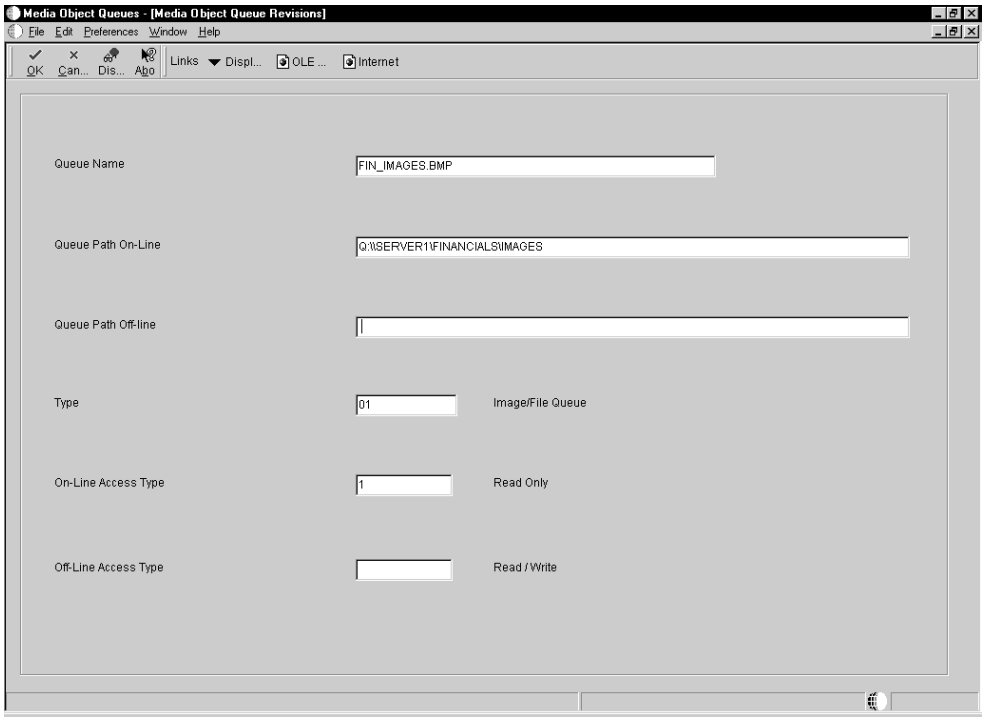
Working with media object queues includes the following tasks:

- Adding a media object queue
- Defining the location of a media object queue
- Deleting a media object queue

► To add a media object queue

On System Administration Tools (GH9011), choose Media Objects and then Media Object Queues (P98MOQUE).

1. On Work With Media Object Queues, click Add.



2. On Media Object Queue Revisions, complete the following fields:
    - Queue Name
    - Queue Path On-Line
    - Queue Path Off-line
    - Type
    - On-Line Access Type
    - Off-Line Access Type
3. Click OK.

► To define the location of a media object queue

On System Administration Tools (GH9011), choose Media Objects and then Media Object Queues (P98MOQUE).

1. If an OLE queue does not exist, click Add.
    a. On Media Objects Queue Revisions, complete the following fields:
        - Queue Name
        - Queue Path On-Line
        - Queue Path Off-line
        - Type
        - On-Line Access Type
        - Off-Line Access Type

b. Click OK.

2. If you want to change an existing media object queue, click Find to display a list of queue names and their paths.
3. Choose the queue name that you want to modify and click Select.

   386898]

4. On Media Object Queue Revisions, change the information in the Queue Path On-Line field to reflect the new location and then click OK.

► To delete a media object queue

On System Administration Tools (GH9011), click Media Objects and then choose Media Object Queues (P98MOQUE).

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

One way to attach images to ERP 9.0 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 J.D. Edwards Web site for a complete list of imaging vendors partnered with J.D. Edwards.

ERP 9.0 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, ERP 9.0 meets the following 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 ERP 9.0. 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 ERP 9.0 currently supports can design custom OLE automation servers for interfacing purposes. The OLE server can be written in any OLE-compliant language. J.D. Edwards 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 ERP 9.0.

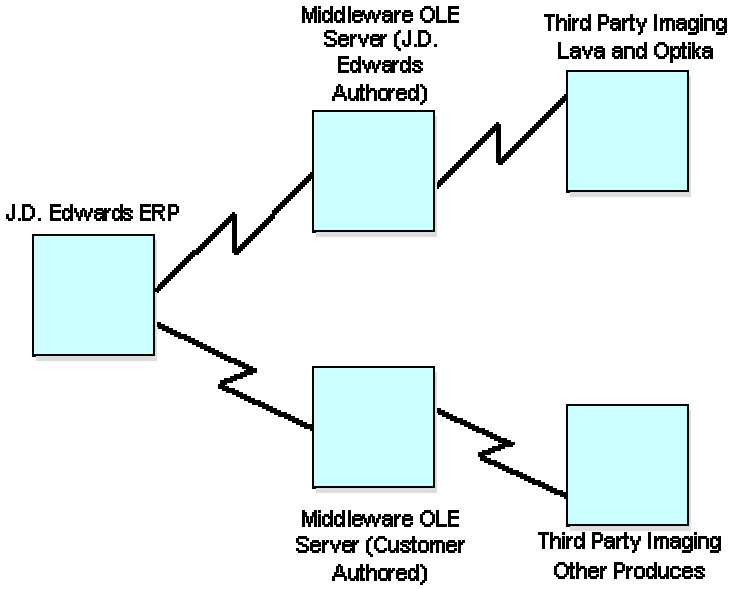
Understanding Flow for Imaging Systems

You can use imaging with a document handling system. The imaging system allows 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.

ERP 9.0 has the ability to retrieve and view documents based on selection criteria that are defined by the user. A linking system associates the ERP 9.0 transaction to the document for later retrieval and reference. You can attach an ERP 9.0 transaction identifier with the scanned image in the document handling system to allow 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 Imaging Constants table (F98101).

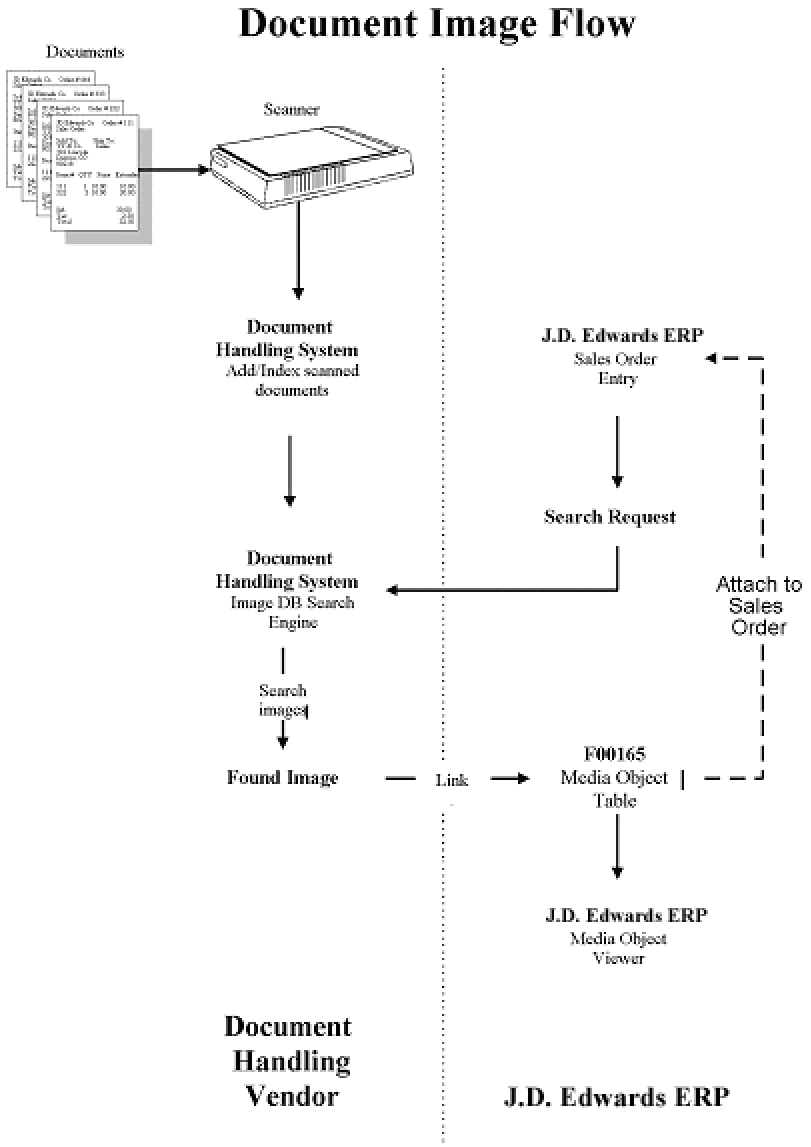
The following illustration shows how ERP 9.0 supports third-party imaging products through a middleware OLE server layer. Customers also can create their own OLE servers to support additional imaging systems.



Cnc/Imaging

Imaging Process Flow

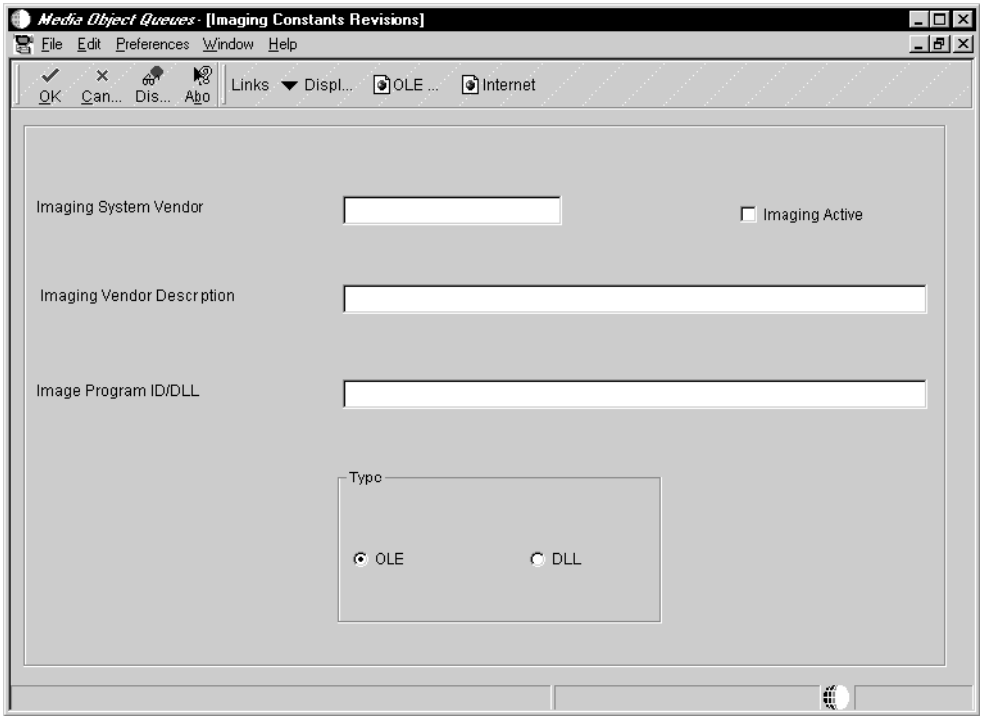
The following diagram shows a typical imaging scenario:



► To enable media objects

On System Administration Tools (GH9011), choose Media Objects and then Media Object Queues (P98MOQUE).

1. On Work With Media Object Queues, from the Form menu, choose Imaging.



2. On Imaging Constants Revisions, complete the following fields:
    - Imaging System Vendor
    - Imaging Vendor Description
    - Image Program ID/DLL
3. Turn on the following options:
    - Imaging Active
    - OLE

Universal Table Browser

If you want to view the data in tables in different databases, you can use the ERP 9.0 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

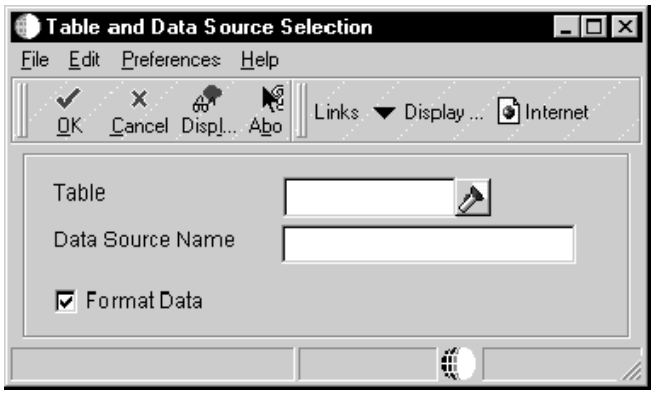
If you want to view the data in tables in different databases, you can use the ERP 9.0 Universal Table Browser. This tool lets you verify the existence of data in a table as well as determine the structure of the table. The Universal Table Browser uses JDEBASE APIs to retrieve data from the database, making it independent of the database you access.

Note

All column and row security that you set up through Security Workbench applies to the Universal Table Browser.

► To view the data in tables

1. On Cross Application Development Tools (GH902), choose Universal Table Browser.
2. On Universal Table Brower, choose Open Table from the File menu.



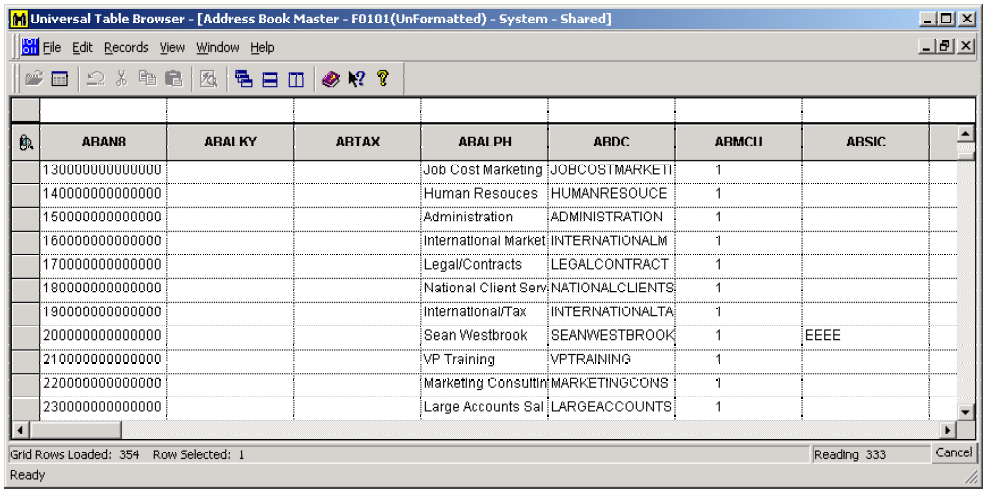
3. On Table and Data Source Selection, complete the following required fields:
    - Table
    - Data Source
4. Turn on the following option:
    - Format Data

The Query By Example (QBE) function is operable as in any other ERP 9.0 application. For example, you can enter ">50" in the ABAN8 column QBE to display records with an Address Book Number greater than 50. You also could 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 functions are operable as in any other ERP 9.0 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.

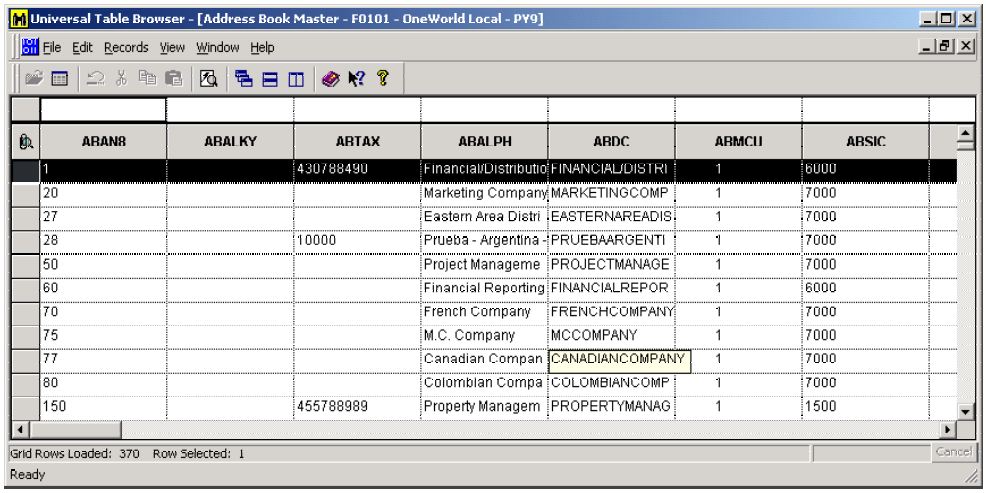
Example: Universal Table Browser (Unformatted Data)

In the following example, a database table is shown as if opened with the Format Data option turned off. Notice that the structure of the information in the ABAN8 column of table F0101 is not formatted; it is shown exactly as it is stored in the database.



Example: Universal Table Browser (Formatted Data)

In the following example, a database table is shown as if it was opened with the Format Data option turned on. Notice that the structure of the information in the ABAN8 column of the Address Book Master table (F0101) is formatted by using the data dictionary specifications.



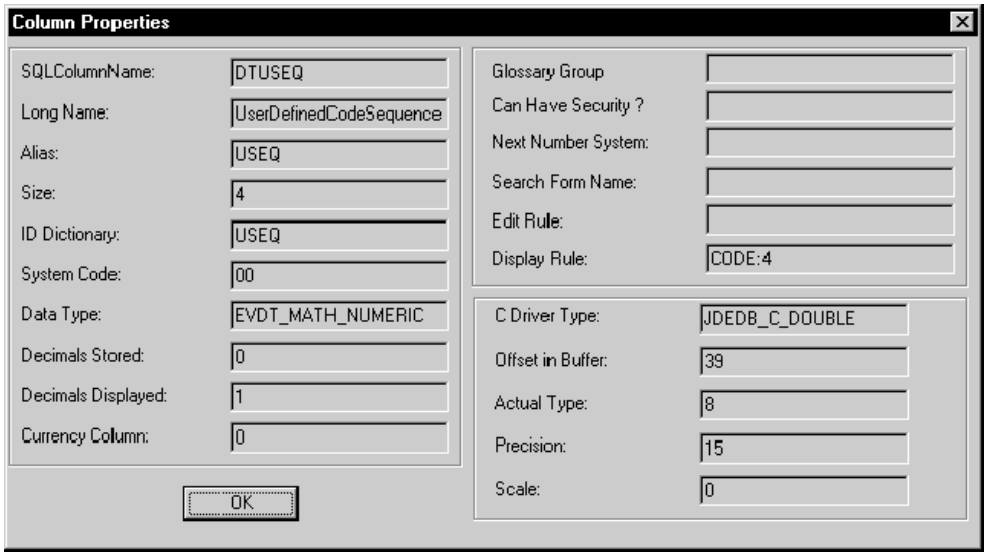
► To view column properties in a table

1. On Universal Table Browser, view a table as described in the task *Viewing the data in tables*.
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.

Example: Column Properties

In this example, the column properties are shown for ERP 9.0 data dictionary item USEQ. The SQL database name for this ERP 9.0 item is DTUSEQ.



Work with Flat File Encoding

Because PeopleSoft 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, based on the user or role, the program id, the program version, and the environment. When the preprocessing or postprocessing intercept occurs, the intercept program calls the table, searches it, and applies the record. The search goes from more specific to less specific records.

The primary users for 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 your primary character set, set up a default flat file encoding record for your 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.

The following list shows the character sets, from UDC H95/FE, that are currently supported:

Code	Description	.ini Setting for Xe
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
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	

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's role, the program ID, the program version, and the environment.

After you add the flat file encoding record, you must activate it.

► To add a flat file encoding record

From the System Administration Tools menu (GH9011), choose Unicode Flat File Encoding Configuration.

1. On Work With Flat File Encoding (P93081), click Add.
2. On Flat File Encoding Revisions, complete the following 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 is *DEFAULT, which 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 is *DEFAULT, which 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.

See Also

- *API Flat File Conversion Setup* in the *Table Conversion Guide* for a list of currently defined encoding files

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.

► To activate or deactivate a flat file encoding file

On System Administration Tools (GH9011), choose Unicode Flat File Encoding Configuration.

1. On Work With Flat File Encoding (P93081), click Find to display the defined flat file encoding files.
2. Highlight the flat file encoding file to activate or deactivate.
3. From the Row menu, choose Change Status.

   The status of the flat file encoding becomes active (AV) or inactive (NA).

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 Sale Order Entry program (P4210) uses the UTF8, Unicode, character set, except when the user JL5534221 runs version JDE0001 in the PDEVCLA environment, when it 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 table below illustrates 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

From the System Administration Tools (GH9011) menu, select Unicode Flat File Encoding Configuration.

4. On Work With Flat File Encoding, click Add.
5. On Flat File Encoding Revisions, complete the following 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

6. Repeat step 2 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

7. Click Cancel to return to Work With Flat File Encoding.
8. Click Find to display all of the flat file encoding records.
9. Highlight the first record and from the Row menu, choose Change Status to activate the recode.
10. Repeat step 6 to activate the currently active records.

The table below shows 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

ERP 9.0 Naming Conventions

This section provides information about the naming conventions that J.D. Edwards suggests that you use when you set up your configuration. You should use alphanumeric characters for your names. Depending on your 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 AS/400 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 AS/400 allow you to enter different characters when you define the server name. ERP 9.0 also limits the amount of characters that you can use to name a server to 15 characters, 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 NT Server domain, you must use the name that was created for the computer by the network administrator.

  If the workstation name does not have a computer account in the domain, you cannot sign on to the domain or access any domain user accounts.

The jde.ini File

This section provides a listing of the settings within the jde.ini file (on the AS/400, it is known as the INI file).

The jde.ini file is an initialization file that provides runtime settings for ERP 9.0. Specific versions of the file must reside on every ERP 9.0 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 jde.ini file can be accessed three ways:

- Access Windows Explorer, locate the jde.ini file, and double-click on it to open it. Notepad is used to view the file.
- Use the Windows Start button and choose Run from the list of options. Type jde.ini in the Open field.
- Type jde.ini in the Fast Path of ERP 9.0 Explorer.

How to use this section

To enable you to quickly locate descriptions, the sections, such as [CLUSTER], 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 (INI file for AS/400) in various places, depending on your ERP 9.0 platform.

Note

For workstations, see *Setting up the Workstation jde.log* in the *Server & Workstation Administration Guide*.

For enterprise servers, see *Working with the Enterprise Server jde.log* in the *Server & Workstation Administration Guide*.

Understanding Workstation jde.ini Settings

This section describes in detail the settings found in the client-side ERP 9.0 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 various names, depending on the type of operating system being used. If you are using Windows 2000, the default directory might be called Win2000.

[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 jde.ini file with running version of ERP 9.0.
Default User=	JDE	The user account name for the database bootstrap tables.
Default Env=	A9CLA	The default environment on the workstation or the enterprise server.
Default PathCode=	PROD	The name of a subdirectory under \B7 that ERP 9.0 uses to find specifications to display signon information before an environment is selected.
Base Datasource=	Access 32	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 database resides
Database=	Access 32	The name of the database in which the system tables reside.
Load Library=	JDBODBC.DLL (non-Oracle) (default) JDBOCI9.DLL (Oracle only) JDBOCI80.DLL (Oracle only)	The JDE driver that is used to access the database which stores the system tables. This name depends on the database to be used and the type of system running ERP 9.0.
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 S I	A single character denoting the type of database holding the system tables. These characters can be O (Oracle), A (MS Access), S (SQL Server), or I (Client Access, AS/400).

LibraryList=		AS/400 only. The database server that stores the system tables.
Default Pwd=		The default password.
Default Journal=	OW_JRNL	AS/400 only. The name of the default journal. Journaling is required on the AS/400 for rollback recovery. The two components to journaling are : • 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	AS/400 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	AS/400 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	AS/400 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=		AS/400 only.
ThousandsSeparator=	,	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. **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.
DecimalSeparator=	.	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. **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.

[DB SYSTEM SETTINGS - SECONDARY]

This section is used for workstations only. The settings are used for a secondary data source to start ERP 9.0, should the primary data source be unavailable. These settings should be the same as the values in the Data Source Master table (F98611) 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.
Secured=	N (default) Y	A flag to indicate whether or not 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, AS/400).
Library List=		AS/400 only. Database server that stores the system tables
Library=		AS/400 only. Database library that stores the system tables.

[OFFLINE DB SYSTEM SETTINGS]

The settings in this section are used only for running ERP 9.0 in detached mode. If you have not installed your workstation with the detached mode option, this section does not appear in your workstation JDE.INI file. The settings here are the same as in the section [DB SYSTEM SETTINGS] listed earlier in this chapter, although the values are different, as shown below.

Setting	Value	Purpose
Version=	43	A version number to prevent mismatch of the jde.ini file with the running version of ERP 9.0.
Default User=	JDE	The user account name for the database bootstrap tables.
Default Env=	DEMOB9	The default environment on the workstation or the enterprise server.
Default PathCode=	APPL_PGF	The name of a subdirectory under \B7 that ERP 9.0 uses to find specifications to display signon information before an environment is selected.
Base Datasource=	ERP 9.0 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=	ERP 9.0 Local	The name of the database where the system tables reside.
Load Library=	JDBODBC.DLL (non-Oracle) (default) JDBOCI9.DLL (Oracle only) JDBOCI80.DLL (Oracle only)	The JDE driver that is used to access the database which stores the system tables. This name depends on the database to be used and the type of system that is running ERP 9.0.
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	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, AS/400).

S

I

LibraryList=	AS/400 only. Database server that stores the system tables.
Default Pwd=	The default password.

[DEBUG]

The settings in this section determine the location of the jde.log and jdedebug.log. The settings are also used to turn your jdedebug.log on and off.

Setting	Typical Value	Purpose
TAMMultiUserOn=	0	
Output=	None	Controls the status of the jdedebug file. Valid values are: • 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. • EXCFILE. 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 dedebug.log.
ServerLog=	0 (default) 1	Valid values are: • 0. Disables the workstation requesting the business function JDE.LOG and JDEDEBUG.OG entries from the server. • 1. Enables workstation requesting business function JDE.LOG and JDEDEBUG.LOG entries from the server.
LEVEL=	BSFN,EVENTS	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: • 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: • SF_GRID • SF_PARENT_CHILD • SF_GENERAL • SF_MESSAGING • SF_WORKFLOW • SF_WORKFLOW_ADMIN • SF_MEDIA_OBJ • SF_CONTROL

		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.
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]

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 on 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 B9 that contains the ERP 9.0 foundation code and tools.
ClientPath=	ERP 9.0 Client Install	The name of the directory on the deployment server that contains the Workstation Installation program and other files which are used during deployment.
PackagePath=	package	The name of the subdirectory on the deployment server under a path code that contains the packages which 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 AS400 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 *Language Overview* in the *ERP Upgrade Guide* for other 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.
ExplorerShortCut	0 1	If this setting is 0, the ERP 9.0 shortcut and startup are not built into the package, so it does not get delivered and put onto the desktop. If this setting is 1, the ERP 9.0 shortcut and startup are built into the package and installed on the desktop during an installation.
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]

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 ERP 9.0 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 htat 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]

Setting	Typical Value	Purpose
ClientType=	Windows HTML	Defines whether the application shortcut that is attached to an external e-mail message contains a Windows application shortcut or a URL for an HTML application shortcut. The default value is Windows.
mailProfile=	Default Profile	The name of the profile to be used for external mail systems that are accessed through ERP 9.0 Work Center. Examples of external mail servers include Microsoft Exchange Server and Lotus Domino Mail Server.
mailServer=	owsmtp.jdedwards.com	The domain name of the SMTP server to be accessed for sending server mail messages.

[JDENET]

Setting	Typical Value	Purpose
serviceNameListen=	6005	Specifies the communications service port on the TCP/IP network. ERP 9.0 uses this port address to listen for requests on the network.
serviceNameConnect=	6005	Specifies the communications service port on the TCP/IP network. ERP 9.0 uses this port address to connect to the network. OCM determines on which server a business function runs. If you run multiple instances of ERP 9.0 on the same server, each instance runs on a different port. The serviceNameConnect parameter value determines the ERP 9.0 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]

Setting	Typical Value	Purpose
bOneUserOnly=	0	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. Specify the kernel process that the user will have on the server by adding the number of the kernel definition section: [JDENET_KERNEL_DEF6] bOneUserOnly=1 This setting allows a client workstation to have its own CallObject kernel process on the server.

[LOCK MANAGER]

Setting	Typical Value	Purpose
Server=	server name	This setting indicates the lock manager server to be used to process records. The value for this setting is the name of the server that is acting as the lock manager.
RequestedService=	NONE	This setting indicates the type of service that the workstation requests from the server. The service that is currently being provided by the server is time stamping (TS) only.

[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 ERP 9.0.
PrintImmediate=	FALSE (default) TRUE	ERP 9.0 servers hold the UBE spool files submitted from a ERP 9.0 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 AS/400, 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 ERP 9.0 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]

Setting	Value	Purpose
OLTLogMode=	YES (default) NO APPEND	This setting specifies if and how the Object Management Workbench Transaction log (OLT.log) is generated. Valid values are: • 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. 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.
OLTLogContents=	GENERAL (default) DETAIL	Specifies if detail information about specification records will be generated in the OLT.log. Valid values are: • GENERAL. No detail information about specification records will be generated. • DETAIL. Detail information will be generated.

[SECURITY]

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, ERP 9.0 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, ERP 9.0 uses the ERP 9.0 security server.
ShowUnifiedLogon=	0 1 (default)	This setting determines whether the ERP 9.0 environment selection form appears when the unified logon feature is used. Valid values are: • 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 ERP 9.0 source programs to locate files. For instance, if "spec" is changed to "specifications", changing SpecPath would allow this immediately. This value is not updated by any program or process. The only reason to change this 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. J.D. Edwards recommends that you not change the name of this directory.
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. J.D. Edwards recommends 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 htat 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 National Language Support (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 momory 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).
UBEDebugLevel=	0 (default) 1- 6	Used to specify what level of debugging information will be provided when using UBE debug logging. 6 is the highest level of logging information. Valid values are: • 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 hot 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: • 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 ERP 9.0 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: • 0. Disabled • 1. Enabled

[WORKFLOW]

Setting	Value	Purpose
Asynchronous Workflow=	FALSE	Used to turn on and off asynchronous workflow. The default value is FALSE.

[EXPLORER]

Setting	Value	Purpose
ExplorerHomeURL=	variable	Variable value should be the URL of the Solution Explorer Home Page.
ExplorerStart=	variable	Variable value should be either INTERNET (to start the Solution Explorer from the Home Page) or TASK (to start the Solution Explorer from a task view).

[ACTIVE DIRECTORY]

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 ERP 9.0 running on it. Typically, the name is the name of the ERP 9.0 service running on the server, such as: JDEDWARDS_ERP_B9_SP20. JdenetSCP is the connection port parameter.
SecurityServerSCP	variable	Same as above. SecurityServerSCP is the security server parameter.
LockManagerSCP	variable	Same as above. LockManagerSCP is the Lock Manager parameter
UnifiedLogonServerSCP	variable	Same as above. UnifiedLogOnServer SCP is the unified logon server parameter.

Understanding AS/400 Server JDE.INI Settings

This section describes in detail the settings found in the ERP 9.0 AS/400 server INI. Information is organized by section-- for example [DEBUG]. Sections are alphabetized, but settings found within sections are generally listed in the order in which they are found in the software.

[AS400]

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 ERP 9.0 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.
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 ERP 9.0 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 ERP 9.0 at start-up. The SENTINEL job creates them at start-up 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 DBDRVSQL 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 ERP 9.0 always writes the AS/400 JOBLOG for the batch application (UBE) to a spool file.
PrintUBEJoblogOnError=	FALSE (default) TRUE	If true, indicates that ERP 9.0 writes the AS/400 JOBLOG for the batch application (UBE) to a spool file if an error occurs--for example, if a UBE fails.

[BSFN BUILD]

Setting	Value	Purpose
Build Area=	/jdeb9_0/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: • Yes. Turns on inlining on the AS400. • No. Turns inlining off. This entry is blank for non-AS/400 servers.
DefineFlags=	JDENV_AS$))MUTEX PRODUCTION_VERSION JDBDB2400 AS400V3R6	
CompilerFlags=	*EXPMAC *NOSHOWINC	This setting determines whether to compile listings when building a server package. Valid values are: • *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. J.D. Edwards has found that 1024 is adequate to compile the delivered business functions. While values other than the default of 1024 might be valid on various host platforms, this value is the only one validated by J.D. Edwards.

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 NT and AS/400 servers only).
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 ERP 9.0 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 ERP 9.0.
Default User=	JDETL	The user account name for the database bootstrap tables.
Default Pwd=	JDETL	The user account password for the database bootstrap tables.
Default Env=	B9APP	The default data source on the workstation or the enterprise server.
Default PathCode=	B9APP	The subdirectory under \$PKG 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 JDE 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 ERP 9.0.
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 N (default)	A flag to indicate that tables names are to be qualified by owner.
Secured=	Y (default) N	Indicates whether or not this is a secured database requiring a user and password login.
Type=	I	A single character denoting the type of database that stores the system tables. This value can be O (Oracle), A (MS Access), S (SQL Server), or I (Client Access, AS/400).
Library=	database library	AS/400 only. The database library that stores the system tables.
DatabaseProgamMax=	-1 (default)	AS/400 only. The maximum number of database connection programs to allow. The value -1 means no limit.
DatabaseProgramInitial=	10 (default)	AS/400 only. The number of database connection programs to start initially at ERP 9.0 start.
DatabaseProgramThreshold=	3 (default)	AS/400 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)	AS/400 only. The number of new database connection programs to start when the threshold number is reached.
DatabaseProgramCheckIntervalSeconds=	10 (default)	AS/400 only. The length, in seconds, before ERP 9.0 will be idled after the database connection programs are created.
Default Journal=	OW_JRNL	AS/400 only. The name of the default journal. Journaling is required on the AS/400 for rollback

		recovery. The two components to journaling are: • The journal • The journal receiver Both before and after images of a database transaction can be recorded by journaling. This can be set to any character string that is 10 characters or fewer.
Default Journal LIBRARY=	journal library	AS/400 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	AS/400 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	AS/400 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	AS/400 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: • 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. 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. 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.

[DEBUG]

The settings in this section determine the location of the jde.log and jdedebug.log. The settings are also used to turn your jdedebug.log on and off.

Setting	Typical Value	Purpose
Output=	FILE	Controls the status of the jdedebug log file. Valid values are: • 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=	JDEB9/ jdedebug	Location of the jdedebug log. J. D. Edwards ships ERP 9.0 with this value set to jdedebug. No processes update this value. The names of the resulting files are path/jdedebug_######.log, where ###### represents the AS/400 job number that is associated with the job that created the file. **Note** ERP 9.0 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 AS/400. You can use the AS/400 WRKLNK command to see a list of directories and files and navigate between the IFS directories. J.D. Edwards ships a command called DSPSTMF that allows you to view these log files. In addition, you can set up Client Access to more easily view some of the smaller log files. See *Using AS/400 Integrated File System Logging Support* in the *Server & Workstation Administration Guide* for details about how to set up Client Access to view log files.
JobFile=	JDEB9/jde.log	Location of the jde log. J.D. Edwards ships ERP 9.0 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 AS/400 job number that is associated with the job which created the file. See *Using AS/400 Integrated File System Logging Support* in the *System Administration Guide* for details about how to set up Client Access to view log files.
JDETSFile=	/JDEB9/JDETS.LOG	Specifies the location of the lock manager trace file on the AS/400.
ClientLog=	1 (default) 0	Valid values are: • 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: • 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: • 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 allows 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.

[INSTALL]

The settings in this section contain directory paths and general installation information.

Setting	Typical Value	Purpose
DefaultSystem=	B9SYS	The name of the ERP 9.0 System library.
ClientPath=	B9APP	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.
B9=		Should be left blank on the AS/400.
LocalCodeSet=	US_EBCDIC	A setting that is used to determine alternate language usage. See *Language Overview* in the *ERP 9.0 Upgrade Guide* for other 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.

[JDEIPC]

Setting	Typical Value	Purpose
maxNumberOfResources=	1000	The total number of IPC resources that are available to JDE.
startIPCKeyValue	2101	On NT, this value is used just 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 JDE will use on the system. SysAdmins 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	JDE 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: • 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.

[JDEMAIL]

Setting	Typical Value	Purpose
mailServer=	owsmtp.jdedwards.com	The domain name of the SMTP server that is accessed for sending server mail messages.

[JDENET]

Setting	Typical Value	Purpose
serviceNameListen=	jde_server	Specifies the communications service port on the TCP/IP network. ERP 9.0 uses this port address to listen for requests on the network.
serviceNameConnect=	jde_server	Specifies the communications service port on the TCP/IP network. ERP 9.0 uses this port address to connect to the network.

maxNetProcesses=	Depends on the maximum number of concurrent ERP 9.0 users that the system is expected to handle, as well as the processing and memory power of the server.	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=	Dependson the maximum number of concurrent ERP 9.0 users the 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	
maxKernelProcesses=	Depends on several factors: • Total of the individual kernel type maximums. The value should be at least that large, but it can be increased as needed. • 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. • The room that you want to allow for dynamic increase of kernel processes from the Server Administration Workbench.	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 below.

Setting	Value	Purpose
bAllowOneUserOnly=	1	Parameter value of 1 means that one-user-only kernel processes are allowed on client workstations. The default is to allow one-user-only kernel processing. Add the setting only for CallObject kernel processes: [JDENET_KERNEL_DEF6] bAllowOneUserOnly=1 Setting must be added with adding a [JDENET_KERNEL_DEFx] bOneUserOnly=1 section to the client workstation jde.ini file.
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 DEF8: PACKAGE INSTALL KERNEL DEF9: SAW KERNEL DEF10: SCHEDULER KERNEL DEF11: PACKAGE BUILD KERNEL DEF12: UBE SUBSYSTEM KERNEL	• DEF1: Used for internal purposes and testing. • DEF2: Processes ERP 9.0 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. • DEF8: Processes package installation request. • DEF9: Processes SAW application requests

	DEF 13: WORKFLOW 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	application requests. • DEF10: Processes Scheduler application requests. • DEF11: Processes package build requests. • DEF12: Processes UBE subsystem requests. • DEF13: Processes workflow requests. • DEF16: Processes and returns request for data in XML document format. • DEF19: Processes real-time events and XML documents generated by the Interoperability Event Observer, as well as Z file events. Publishes all ERP 9.0 events to subscribers. • DEF20: Processes information from business functions calling real-time APIs and uses that information to create and 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
dispatchDLLName=	DEF1: JDENET DEF2: JDEKRNL DEF3: JDEKRNL DEF4: JDEKRNL DEF5: JDEKRNL DEF6: JDEKRNL DEF7: JDEKRNL	Identifies the name of the JDENET service program.

	DEF8: JDEKRNL	
	DEF9: JDESAW	
	DEF10: JDEKRNL	
	DEF11: JDEKRNL	
	DEF12: JDEKERNL	
	DEF13: JDEKRNL	
	DEF16: XMLLIST	
	DEF19: JDEIE	
	DEF20: JDEIEO	
	DEF22: XMLDISPATCH	
	DEF23: XJSKERNEL	
	DEF24: XMLSERVICE	
dispatchDLLFunction=	DEF1: JDENET_DispatchMessage DEF2: JDEK_DispatchUBEMessage DEF3: DispatchRepMessage DEF4: JDEK_DispatchSecurity DEF5: TM_DispatchTransactionManager DEF6: JDEK_DispatchCallObjectMessage DEF7: JDEK_DispatchJDBNETMessage DEF8: JDEK_DispatchPkgInstallMessage DEF9: JDEK_DispatchSAWMessage DEF10: JDEK_DispatchScheduler DEF11: JDEK_DispatchPkgBuildMessage DEF12: JDEK_DispatchUBESBSMessage	The name of the JDENET function for handling JDENET messages. The dispatchDLLName and dispatchDLLFunction entries are platform-specific.

	DEF13: JDEK_WFServerProcess DEF16: JDEK_XMLListDispatch DEF19: JDEK_DispatchITMessage DEF20: JDEK_DispatchIEOMessage DEF22: XMLDispatch DEF23: JDEK_DISPATCHXTSMessage DEF24: XMLServiceDispatch	
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*	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. 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 ERP 9.0 services start or when the first message for kernel type is received.

[LOCK MANAGER]

Setting	Typical Value	Purpose
AvailableService=	NONE	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: • TS • NONE
RequestedService=	NONE	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: • TS • NONE

[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.

[SECURITY]

Setting	Typical Value	Purpose
DataSource=		
User=	JDESVR	
Password=	JDESVR	

DefaultEnvironment=	P9ASD1	Defines a valid environment in which the path code defines table F98OWSEC.
SecurityServer=	security server name	
ServerPswdFile=	TRUE	The setting of this parameter determines whether ERP 9.0 uses special password handling for batch reports running on the server. Set the value to TRUE to instruct ERP 9.0 to enable special handling of passwords. Set the value to FALSE to disable special handling. When ERP 9.0 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 some operating systems, the status of a job can be queries and the parameters that were used to start the process can be viewed. As a security measure, you can enable special handling by ERP 9.0. When enabled, ERP 9.0 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.” ERP 9.0 instructs the operating system to destroy this file as soon as the batch report reads the password.
History=	0	
SecurityMode=	0 (default) 1 2	This setting controls whether ERP 9.0 uses the standard logon procedure, unified logon, or both. Valid values are: • 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 ERP 9.0. 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 ERP 9.0 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=	/b9APP	

[TCENGINE]

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: • 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 momory 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).
UBEDebugLevel=	0 (default) 1- 6	Used to specify what level of debugging information will be provided when using UBE debug logging. 6 is the highest level of logging information. Valid values are: • 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)	Type 1 to show a box around PDF hot links.

	1	
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: • 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 ERP 9.0 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: • 0. Disabled • 1. Enabled

[WORKFLOW]

Setting	Value	Purpose
Asynchronous Workflow=	FALSE	Used to turn on and off asynchronous workflow. The default value is FALSE.

[WORLD ENVIRONMENT MAP]

Setting	Value	Purpose
OneWorldEnvironmentName= (for example, APPLJDEDC2)	WorldEnvironment Name (for example, QA9COMP)	The string that is used by the special business function code to set up WorldSoftware library lists from within ERP 9.0. The library lists call WorldSoftware from ERP 9.0. As of B73.3; the functions that are associated with these settings might not be used by application developers.

[INTEROPERABILITY]

Setting	Typical Value	Purpose
RegisteredEvents=	RTSOOUT	Names of EventTypes. An event is an ERP 9.0 business transaction running on a ERP 9.0 enterprise server. To enable real-

		time generation of events, you must register each event that you want to generate in real time.
FilteredEvents=	*ALL	The value of this parameter defines the events that you want to create in real time. A value of *ALL generates all registered events. *NONE disables event generation. You can also enter a subset of registered events.

[SAMPLE_EVENT]

Setting	Typical Value	Purpose
DS1= DS2= DS3=	D4202150B D4202150C D34A1050C	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.

[JDEITDRV]

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.

[LREngine]

Setting	Typical Value	Purpose
System=	/B9SYS_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.

Understanding UNIX Server jde.ini Settings (HP9000, RS/6000, or Sun Servers)

This section describes in detail the settings found in the ERP 9.0 UNIX server jde.ini file. 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]

Setting	Value	Purpose
Build Area=	/usr/PeopleSoft/b9/packages	The location on the server where the package will be built.
Optimization Flags=	+02 (default for HP9000) -02 (default for RS/6000 and Sun)	Machine dependent. These compile flags are used when building business functions in Release mode. You should not change these flags.
DebugFlags=	-g -y -D_DEBUG -DJDEDEBUG (default for HP9000) -g -qfulpath -qdbextra -D_DEBUG -DJDEDEBUG (default for RS/6000) -g -D_DEBUG -DJDEDEBUG (default for Sun)	Machine dependent. These compile flags are used when building business functions in Debug mode. You should not change these flags.
InliningFlags=	blank (default)	A value of Yes turns on inlining on the AS400. A value of No turns it off. This entry is blank for non-AS/400 servers.
DefineFlags=	-DKERNEL -DPRODUCTION_VERSION -DNATURAL_ALIGNMENT -D_HPUX_SOURCE (default for HP9000) -DKERNEL -DPRODUCTION_VERSION -DNATURAL_ALIGNMENT (default for RS/6000) -DKERNEL -DPRODUCTION_VERSION -DNATURAL_ALIGNMENT -D_SUN-SOURCE (default for Sun)	
CompilerFlags=	-Aa +w1 +z -c (default for HP9000) -qalign=natural -qflag=I:I -c (default for RS/6000) -qspill=1024 -misalign -KPIC (default for Sun)	Machine dependent. Valid compiler flags. The spill flag sets the stack space when business functions are compiled. J.D. Edwards has found that 1024 is adequate to compile the delivered business functions.
OSReleaseLevel=	+DAportable (for HP-UX only)	The release level to which you are compiling. You should not change these flags.

	-q32 (for AIX)	
LinkFlags=	-b -z -ljdesaw -L/usr/PeopleSoft/BDEV/system/lib (default for HP9000) -b -z -B symbolic -ljdesaw -L/usr/PeopleSoft/BDEV/system/lib (HP9000 only) -B symbolic -ljdesaw -L/usr/PeopleSoft/BDEV/ system/lib (HP9000 only) -bl:/usr/oneworld/BDEV/b9/system/bin32/funclist.imp -bM:SRE -bexpall -brtl -lc -bnoentry -L. -L/usr//PeopleSoft/BDEV/b9/system/lib -lm -ljdelib -lcallobj -lerror -lgentext -ljdb -ljde_erk -ljdecache -ljdecache -ljdeddapi -ljdeknet -ljderepl -ljdeschr -ljdesec -ljdespec -ljdetam -llanguage -lmisc -lpackage -lport -lrdbapi -lruntime -lsrc -ltransmon -lube -lworkflow -ljdenet -bloadmap:loadmap -ljdesaw (default for RS/6000) -bl:/usr//PeopleSoft/BDEV/b9/system/bin32/funclist.imp -bM:SRE -bexpall -brtl -lc -lm -bnoentry -L. -L/usr//PeopleSoft/BDEV/b9/system/lib -lm -ljdelib -lcallobj -lerror -lgentext -ljdb -ljde_erk -ljdecache -ljdecache -ljdeddapi -ljdeknet -ljderepl -ljdeschr -ljdesec -ljdespec -ljdetam -llanguage -lmisc -lpackage -lport -lrdbapi -lruntime -lsrc -ltransmon -lube -lworkflow -ljdenet -lowver -bloadmap:loadmap -ljdesaw (default for AIX) -G -L$ -ljdesaw (ORACLE_HOME)/lib -L/usr/PeopleSoft/ BDEV/system/lib (default for Sun)	Machine dependent. These flags are used when linking business functions, including linking them to the jdesaw system that is shared library. You should not change these flags. The -b -z -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. The -B symbolic setting insures that when a shared library is built, function calls found in it are resolved in the same library, if possible. The settings -ljdesaw and -L/usr/PeopleSoft/BDEV/system/lib settings need to be added before any business function build where a business function links to a function in the system library libjdesaw.sx.
LinkLibraries=	blank (default)	Libraries to which business functions are linked (Windows NT and AS/400 servers only).
SimultaneousBuilds=	0 (unlimited) (default) any integer (number of simultaneous builds)	Indicates the number of DLLs that can be built at a time. A value of 0 means that all DLLs can be built simultaneously.

[CLUSTER]

Setting	Typical Value	Purpose
Primary Node=	server name	When clustering is used with ERP 9.0, this setting specifies either a primary server where ERP 9.0 will run or a floating IP address name. This setting is delivered "commented out."

[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 a mismatch of the jde.ini file with the running version of ERP 9.0.
Default User=	JDESVR	The user account name for the database bootstrap tables.
Default Pwd=		The user account password for the database bootstrap tables.
Default Env=	PDEVHP02 (default for HP9000) PDEVRS02 (default for RS/6000)	The default data source on the workstation or the enterprise server.
Default PathCode=	PROD	The subdirectory under \$PKG under which the business function code is stored.
Base Datasource=	ORACLE SVR	The data source representing the database from which logon information is retrieved.
Object Owner=	JDESVR	The owner of system database tables.
Server=	server name	The server on which the database resides.
Database=	hp9000adevl	The database connect string where the system tables reside.
Load Library=	libora9.sl (default for HP9000) libora80.so (default for RS/6000 and Sun)	The JDE 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 ERP 9.0.
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.
Type=	O (default) A S I	A single character denoting the type of database that stores the system tables. Valid values are: • O (Oracle) • A (MS Access) • S (SQL Server) • I (Client Access, AS/400)
LibraryList=	blank (default)	AS/400 only. The database server that stores the system tables.
TriggerLibrary=	JDBTRIG (default)	AS/400 only. The 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 your jdedebug.log on and off.

Setting	Typical Value	Purpose
Output=	FILE	Controls the status of the jdedebug file. Valid values are: • 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. • EXCFILE. 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.
Trace=	TRUE	Writes additional trace information to the log files to aid in debugging.
ClientLog=	1 (default) 0	Valid values are: • 1. Enables servicing of business functions JDE.LOG and JDEDEBUG.LOG entries from the server to the workstation. • 0. Disables this service.
DebugFile=	jdedebug.log	The location and name of the jdedebug.log file.
JobFile=	jde.log	The location and name of the jde.log file.
LogErrors=	1	

JDETSFile=	JDETS.log	Specifies the location of the lock manager trace file.
RepTrace=	1	Enables replication of log messages.

[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 B9 that contains the ERP 9.0 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 which 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 which is delivered for all packages for that path code.
B9=	/usr//PeopleSoft/b9	Base path of the ERP 9.0 installation.
Double_Byte=	0	
LocalCodeSet=	WE_ISO88591	A setting that is used to determine alternate language usage. See *Language Overview* in the *ERP 9.0 Upgrade Guide* for other values.

[JDEIPC]

Setting	Typical Value	Purpose
ipcTrace=	0	Set to 1 to enable IPC logging messages. **Caution** This setting can cause the log files to grow very fast.
maxNumberOfSemaphores=	200 (default for HP9000 and Sun)	Not delivered for the RS/6000.
startIPCKeyValue	7999	Delivered "commented out." On UNIX, this setting is the value of the IPC ID that JDEIPC uses for its shared memory. This value, plus the

	maxNumberOfResources, defines the range of IPC IDs that JDE 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.

[JDEMAIL]

Setting	Typical Value	Purpose
mailServer=	owsmtp.jdedwards.com	The domain name of the SMTP server to access for sending server mail messages.

[JDENET]

Setting	Typical Value	Purpose
serviceNameListen=	jde_server	The port number or service name that is used by ERP 9.0 to communicate with clients and other servers.
serviceNameConnect=	jde_server	The port number or service name that is used by ERP 9.0 to communicate with clients and other servers.
maxNetProcesses=	1	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=	1250 (default for HP9000) 800 (default for RS/6000)	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.
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
maxLenInlineData=	1024	For internal use only.
maxLenFixedData=	4096	For internal use only.
maxFixedDataPackets=	1024	For internal use only.
netTrace=	1	Enables JDENET log messages.
kernelDelay=	0	For internal use only.

HandleKrnlSignals=	1	Turns on and off the handling of signals that are delivered to the process. Kernel processes read the setting on startup. Parameter value of 1 turns on handling, which means that that the kernel process handles the signal, performs some cleanup tasks, and exits. Parameter value of 0 turns of 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 parameter value of 0 for debugging purposes. Once ERP 9.0 service has started, only processes started after you make a change to this setting are affected.
netCoreDump=	0	For internal use only. Not delivered with the RS/6000.
netTemporaryDir=	temporary file directory	Sets the directory to use for ERP 9.0 temporary files.
newProcessThresholdConnects=	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_DEF12. The settings in these sections should not be changed except where noted below.

Setting	Value	Purpose
bAllowOneUserOnly=	1	Parameter value of 1 means that one-user-only kernel processes are allowed on client workstations. The default is to allow one-user-only kernel processing. Add the setting only for CallObject kernel processes: [JDENET_KERNEL_DEF6] bAllowOneUserOnly=1 Setting must be added with adding a [JDENET_KERNEL_DEFx] bOneUserOnly=1 section to the client workstation jde.ini file.
krnlName	DEF1: JDENET RESERVED KERNEL DEF2: UBE KERNEL DEF3: REPLICATION KERNEL	• DEF1: Used for internal purposes and testing. • DEF2: Processes ERP 9.0 batch process requests. • DEF3: Processes data

	DEF4: SECURITY KERNEL DEF5: LOCK MANAGER KERNEL DEF6: CALL OBJECT KERNEL DEF7: JDBNET KERNEL DEF8: PACKAGE INSTALL KERNEL DEF9: SAW KERNEL DEF10: SCHEDULER KERNEL DEF11: PACKAGE BUILD KERNEL DEF12: UBE SUBSYSTEM KERNEL DEF 13: WORKFLOW 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	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. • DEF8: Processes package installation 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 • 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 ERP 9.0 events to subscribers. • DEF20: Processes information from business functions calling real-time APIs and uses that information to create and 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
dispatchDLLName=	DEF1: libjdenet.sl (default for HP9000) or libjdenet.so (default for	Identifies the name of the JDENET service program.

RS/6000 and Sun)	service program.
DEF2: libjdeknet.sl (default for HP9000) or libjdeknet.so (default for RS/6000 and Sun)	
DEF3: libjderepl.sl (default for HP9000) or libjderepl.so (default for RS/6000 and Sun)	
DEF4: libjdeknet.sl (default for HP9000) or libjdeknet.so (default for RS/6000 and Sun)	
DEF5: libtransmon.sl (default for HP9000) or libtransmon.so (default for RS/6000 and Sun)	
DEF6: libjdeknet.sl (default for HP9000) or libjdeknet.so (default for RS/6000 and Sun)	
DEF7: libjdeknet.sl (default for HP9000) or libjdeknet.so (default for RS/6000 and Sun)	
DEF8: libjdeknet.sl (default for HP9000) or libjdeknet.so (default for RS/6000 and Sun)	
DEF9: libjdesaw.sl (default for HP9000) or libjdesaw.so (default for RS/6000 and Sun)	
DEF10: libjdeschr.sl (default for HP9000) or libjdeschr.so (default for RS/6000 and Sun)	
DEF11: libjdeknet.sl (default for HP9000) or libjdeknet.so (default for RS/6000 and Sun)	
DEF12: jdekern.sl (default for HP9000 and Sun) or libjdeknet.so (default for RS/6000)	
DEF13: libworkflow.so (default for HP9000 and Sun) or libworkflow.sl (default for RS/6000)	
DEF16: libxmllist.so (Sun/AIX); libxmllist.sl (HP9000)	
DEF19: libjdeie.so (Sun/AIX); libjdeie.sl (HP9000)	
DEF20: libjdeieo.so (Sun/AIX); libjdeieo.sl (HP9000)	
DEF22: libxmldispatch.so/sl	
DEF23: libxtskrnl.so/sl	

	DEF24: libxmlservice.so/sl	
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_DispatchWFServer Process 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.
maxNumberOfProcesses=	1	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=	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]

Setting	Typical Value	Purpose
Server=	server name	This setting indicates the lock manager server to use to process records. The value for this setting is the name of the server that is acting as the lock manager.
AvailableService=	TS	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: • TS • NONE
RequestedService=	TS	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: • TS • NONE

[MEMORY DEBUG]

Setting	Typical Value	Purpose
Frequency=	10000	
Full=	1	

[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
UBE Semaphore Key=	3600	
DefaultPrinterOUTQ=	printer name	The default printer to which batch applications will be routed.
OutputDirectory=	directory name	The directory where you want to create the PrintQueue directory.
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.

[SECURITY]

Setting	Typical Value	Purpose
User=	JDESVR	The ERP 9.0 user.
Password=	JDESVR	The ERP 9.0 password.
DefaultEnvironment=	PDEVHP02 (default for HP9000) PDEVRS02 (default for RS/6000)	Defines a valid environment in which the path code defines table F98OWSEC.
DataSource=	ORACLE PVC B9	The name of the ERP 9.0 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 ERP 9.0 uses special password handling for batch reports running on the server. Set the value to TRUE to instruct ERP 9.0 to enable special handling of passwords. Set the value to FALSE to disable special handling. When ERP 9.0 runs a batch report on the server, it runs the report

		using a string of line commands and parameters that include the "user password." Under some operating systems, you can query the status of a job and view the parameters that were used to start the process. As a security measure, you can enable special handling by ERP 9.0. When enabled, ERP 9.0 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". ERP 9.0 instructs the operating system to destroy this file as soon as the batch report reads the password.
History=	0	

[SERVER ENVIRONMENT MAP]

Setting	Typical Value	Purpose
ServerName=	environment name	Each setting in this section lists the environment to which each server is mapped.

[SVR]

The settings in this section contain environment and subdirectory information.

Setting	Typical Value	Purpose
EnvType=	1	Used by JDEKRNL
EnvironmentName=	PDEVHP02 (default for HP9000) PDEVRS02 (default for RS/6000)	
SpecPath=	spec	This line and all of the following in this section specify the path names so that other ERP 9.0 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=	PDEVHP02 (default for HP9000) PDEVRS02 (default for RS/6000)

[TAM]

Setting	Value	Purpose
TAMTraceLevel	0	

[WORKFLOW]

Setting	Value	Purpose
Asynchronous Workflow=	FALSE	Used to turn on and off asynchronous workflow. The default value is FALSE.

[INTEROPERABILITY]

Setting	Typical Value	Purpose
RegisteredEvents=	RTSOOUT	Names of EventTypes. An event is a ERP 9.0 business transaction running on a ERP 9.0 enterprise server. To enable real-time generation of events, you must register each event that you want to generate in real time.
FilteredEvents=	*ALL	The value of this parameter defines the events that you want to create in real time. A value of *ALL generates all registered events. *NONE disables event generation. You can also enter a subset of registered events.

[JDENET_KERNEL_DEFx]

This section defines JDENET internal dedicated server processes.

Setting	Value	Purpose
bAllowOneUserOnly=	1	Parameter value of 1 means that one-user-only kernel processes are allowed on client workstations. The default is to allow one-user-only kernel processing. Add the setting only for CallObject kernel processes: [JDENET_KERNEL_DEF6] bAllowOneUserOnly=1 Setting must be added with adding a [JDENET_KERNEL_DEFx] bOneUserOnly=1 section to the client workstation jde.ini file.
krnlName	DEF1: JDENET RESERVED KERNEL DEF2: UBE KERNEL DEF3: REPLICATION KERNEL DEF4: SECURITY KERNEL DEF5: LOCK MANAGER KERNEL DEF6: CALL OBJECT KERNEL	• DEF1: Used for internal purposes and testing. • DEF2: Processes ERP 9.0 batch process requests. • DEF3: Processes data replication requests. • DEF4: Processes security server requests. • DEF5: Processes

DEF7: JDBNET KERNEL

DEF8: PACKAGE INSTALL KERNEL

DEF9: SAW KERNEL

DEF10: SCHEDULER KERNEL

DEF11: PACKAGE BUILD KERNEL

DEF12: UBE SUBSYSTEM KERNEL

DEF 13: WORKFLOW 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

transaction manager and lock manager requests.

- DEF6: Processes requests for remote master business functions (MBF).
- DEF7: Processes JDBNet server-to-server requests.
- DEF8: Processes package installation 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.
- 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 ERP 9.0 events to subscribers.
- DEF20: Processes information from business functions calling real-time APIs, and uses that information to create an XML file 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

dispatchDLLName=	DEF1: jdenet.dll DEF2: jdekrnl.dll DEF3: jdekrnl.dll DEF4: jdekrnl.dll DEF5: jdekrnl.dll DEF6: jdekrnl.dll DEF7: jdekrnl.dll DEF8: jdekrnl.dll DEF9: jdesaw.dll DEF10: jdekrnl.dll DEF11: jdekrnl.dll DEF12: jdekrnl.dll DEF13: jdekrnl.dll DEF16: xmllist.dll DEF19: jdeie.dll DEF20: jdeieo.dll DEF22: xmldispatch.dlll DEF23: xtskrnl.dll DEF24: xmlservice.dll	Identifies the name of the JDENET service program.
dispatchDLLFunction=	DEF1: JDENET_Dispatch Message@28 DEF2: JDEK_DispatchUBEMessage@28 DEF3: DispatchRepMessage@28 DEF4: JDEK_DispatchSecurity@28 DEF5: JDEK_DispatchTransactionManager@28 DEF6: JDEK_DispatchCallObject Message@28 DEF7: JDEK_DispatchJDBNETMessage@28 DEF8: JDEK_DispatchPkgInstallMessage@28 DEF9: JDEK_DispatchSAWMessage@28 DEF10: JDEK_DispatchScheduler@28 DEF11: JDEK_DispatchPkgBuildMessage@28 DEF12:	The name of the kernel function for handling kernel request messages. On Intel processors running Windows NT, the preceding underscore "_" and following "@28" are required. On Compaq AlphaServer processes running Windows NT, the preceding underscore "_" and following "@28" are omitted.

	JDEK_DispatchUBESBSMessage@28 DEF13: JDEK_DispatchWFServer Process@28 DEF16: JDEK_XMLListDispatch@28 DEF19: JDEK_DispatchITMessage@28 DEF20: JDEK_DispatchIEOMessage@28	
maxNumberOfProcesses=	1	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=	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.

[SAMPLE_EVENT]

Setting	Typical Value	Purpose
DS1= DS2= DS3=	D4202150B D4202150C D34A1050C	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.

[JDEITDRV]

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:libjdetrdrv.so (Sun and AIX) JDENET:libjdetrdrv.sl (HP9000)	The directory location of the JDENET driver.

[LREngine]

Setting	Typical Value	Purpose
System=	/owdisk2/oneworld/b9_bdev/output	The directory location of the List-Retrieval Engine, a database that is used to manage access to XML repository files.

Understanding Windows NT Enterprise Server jde.ini Settings

This section describes in detail the settings found in the ERP 9.0 Windows enterprise server jde.ini file. 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. For cases when defaults for Intel and Compaq AlphaServer processors differ, the two values are labeled.

[BSFN BUILD]

Setting **Value** **Purpose**

DoCompression= 0

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:

- 0. Do not use compression.
- 1. Use compression.

BuildArea=	Z: \OneWorld\b9\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/optimize mode. You should not change these flags.
OSReleaseLevel=	5.0	The Windows NT 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.
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=	jdekrnl.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 J.D. Edwards internal use only.

Setting	Value	Purpose
User=	JDE	ERP 9.0 user ID used to run BSFNBuilder.exe.
Pwd=	JDE	ERP 9.0 user password used to run BSFNBuilder.exe.
PathCode=	appl_pgf	ERP 9.0 pathcode under which BSFNs

		are built.
Build Area=	z: \OneWorld\b9 \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 tha are used to create release builds.
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: • 0. The default setting; do not keep. • 1. Keep.
BFDir=	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 ERP 9.0. 43 is the only valid value.
Default User=		The ERP 9.0 user ID that is used to access the bootstrap tables, F986101 and F98611.

Default Pwd=		The ERP 9.0 user password that is used to access the bootstrap tables.
Default Env=	P9HPO1	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 be read from the spec subdirectory of this pathcode folder.
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: • 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: \OneWorld\b9 \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: \OneWorld\b9 \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: • 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: \OneWorld\b9 \ddp\log\jdets.log	The path and name of the log file that is used to write lock manager tracing information.
KeepLogs=	1	Keeps logs for UBEs in the Print Queue directory. Valid values are: • 1. Keeps the logs created when UBEs are run. • 2. Delete the UBE logs when the UBE is finished

		processing. Regardless of this setting, logs are kept if an error occurs when processing the UBE.
TAMTraceLevel=	0	Controls the amount of TAM information that is logged to the jdedebug.log. Valid values are: • 0-10, with higher numbers increasing the amount of information being logged. • 0. Default setting; no information output.
TAMTrace=	0	Controls TAM file trace information. Valid values are: • 0. Do not write TAM trace information to the debug file. • 1. Write TAM trace information to the debug file.
ClientLog=	0	Sends log information to the client and merges it with the client's jde.log and jdedebug.log files. Valid values are: • 0. Do not send log information to the client. • 1. Send log information to the client.
QKLog=	0	Controls JDE Queue Kernel tracing information. Valid values are: • 0. Do not write Queue Kernel message information to the debug file. • 1. Write Queue Kernel message information to the debug file.
TraceRowSecurityFetch=	FALSE	Controls row level security tracing. Valid values are: • FALSE (default). Turn off tracing. • TRUE. Turn on tracing.
WTSLogs=	FALSE	Creates logs in the User Profile directory for TSE installations. Valid values are: • FALSE (default). Set the log file paths by the JobFile and DebugFile. • TRUE to write the log files to c:\WTSRV\Profiles\%Userid%\Windows.
jdelibFatal=	FALSE	Determines whether message boxes are supported. Valid values are: • 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: • 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: • 0 (default). Do not write fatal error messages to a message box. • 1. Write fatal error messages to a message box.

[INSTALL]

The settings in this section contain directory paths and general installation information.

Setting	Typical Value	Purpose
B9=	\JDEdwards OneWorld\B9\ddp	The path to the ERP 9.0 base installation directory.
LocalCodeSet=	WE_ISO88591	Determines the character code set used by ERP 9.0. Valid values are: • WE_ISO88591 (1252) - English • JA_SJIS (932) - Japanese • TC_BIG5 (950) - Traditional Chinese • SC_GB (936) - Simplified Chinese • KO_KSC (949) - Korean
StartServicePrefix	JDE B9	Uniquely identifies ERP 9.0 services to a single installation. The prefix tags ERP 9.0 services when running parallel releases on a single server. The default value is JDE.
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: • 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: • 0 (default). Do not force. • 1. Force.
	1	Used to retrieve the code page for the current process. Valid values are: • 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.

[JDE_CG]

Setting	Typical Value	Purpose
TARGET=	RELEASE	The type of build that is used to compile objects. Valid values are: • RELEASE (default). Build using release mode. • DEBUG. Build using debug mode.
INCLUDES=	c:\msdev\devstudio\vc\ include	The path to Microsoft Visual C++, ERP 9.0 system, and ERP 9.0 pathcode include (header) files.
LIBS=	c:\msdev\devstudio\vc\lib	The path to Microsoft Visual C++, ERP 9.0 system, and ERP 9.0 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]

Setting	Typical Value	Purpose
ipcTrace=	0	Controls the number of interprocess communications (IPC) written to the jdedebug.log. Valid values are: • 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 ERP 9.0. The values of these keys for each instance of ERP 9.0 must differ by at least the value of maxNumberOfResources. The default value is 5000.
maxNumberOfResources=	1000	The maximum number of IPC resources that the ERP 9.0 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 ERP 9.0 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).

[JDEMAIL]

Setting	Typical Value	Purpose
ClientType=	Windows HTML	Defines whether the application shortcut that is attached to an external e-mail message will contain a Windows application shortcut,or a URL for an HTML application shortcut. The default value is Windows.
mailServer=	owsmtp.jdedwards.com	The domain name of the SMTP server to access for sending server mail messages.
RuleN=	HANDLER: DATA	The SMTP e-mail configuration rules that are taken from the SMTP Transformation Engine Rules & Regs table F90005. Any empty or invalid entry is considered at the end of the list. "N" is a positive integer starting at 1.

[JDENET]

Setting	Typical Value	Purpose
serviceNameListen=	6003 jde_server	The TCP/IP port number that is used for receiving communications packets. If this values is an integer, that number is used as the port. If this value is a character string, it will be translated via 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 values is an integer, that number is used as the port. If this value is a character string, it will be translated via the file c:\winnt\system32\drivers\etc\services into a port number and transport protocol. The default value is jde_server.
maxNetProcesses=	1	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 ok should be greater than all of the ok as added together in

		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.
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 ERP 9.0 net and queue services on Windows NT enterprise servers. The default value is 1.
EnablePredefinedPorts=	0	Allows ERP 9.0 net to use a predefined range of TCP/IP ports. This setting is required to permit the ERP 9.0 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 serviceNameListen = 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]

Setting	Typical Value	Purpose
Server=	server1	The name of the server that is hosting (making available) the record locking services. This setting is a type of kernel. Any ERP 9.0 enterprise server can host record locking services.
RequestedService=	TS	The type of service that the local enterprise server's processes are requesting of the ERP 9.0 enterprise server that is listed in the Server field. Valid value are: • NONE (default). • TS. For time stamping.
AvailableService=	NONE	The type of service that the local enterprise server hosts (makes available). Valid values are: • NONE (default). • TS. Time stamping.
LogServices=	0	Controls lock manager tracing information. Valid values are: • 0 (default) Do not write messages to the file specified in [DEBUG] JDETSFile. • 1. Write messages to this file.

[NETWORK QUEUE SETTINGS]

The settings in this section contain information for starting batch queues.

Setting	Typical Value	Purpose
QEnv=	P733HPO1	The environment for starting batch queues.
QUser=	JDE	The ERP 9.0 user ID for starting batch queues.
QPassword=	JDE	The ERP 9.0 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. *N* 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. *N* ranges from 1 to the value of SpcQueues.
KillImmediate=	1	The action of the shutdown process. Valid values are: • 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:\OneWorld\b9\ddp	The parent directory for the PrintQueue directory where job files (in .pdf format) are located.

[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.
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 J.D. Edwards sales order status.
JDECustomerCode=	JDEAB	Used with create header. Transaction type for J.D. Edwards Customer add and update.
JDEItemPriceCode=	JDEPRICE	Used with create header. Transaction type for J.D. Edwards price update.
JDEItemQtyCode=	JDEIL	Used with create header. Transaction type for J.D. Edwards 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=		ERP 9.0 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 ERP 9.0 is installed.

[SECURITY]

Setting	Typical Value	Purpose
SecurityServer=	server1	The server hosting the security services. Any server running ERP 9.0 services can host security server services.
User=	JDE	The database account that is used to access security table F98OWSEC.
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 - B9	The data source where security table F98OWSEC can be found. The default value is System - B9.

SecurityMode=	0, 1, or 2	Controls whether ERP 9.0 accepts a standard logon, unified logon, or both. Valid values are: • 0 (default). Accept only the standard logon. • 1. Accept only the unified logon. • 2. Accept both.
AllowedUsers=	ERP 9.0_users, Bowens	A comma-delimited list of user accounts, groups of user accounts, or both, that are permitted to sign on to ERP 9.0 using unified logon. This setting allows the users to bypass the ERP 9.0 client sign-on screen.
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]

Setting	Typical Value	Purpose
ENV1=	ENV2	Maps one environment name to another. Wherever ENV1 is to be used on the ERP 9.0 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.
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.

[ACTIVE DIRECTORY]

The setting in this section is used when Active Directory is installed.

Setting	Value	Purpose
SCPToPublish	Variable. Typically use a version of ERP 9.0 running on the server -- for example JD_EDWARDS_ERP_B9_SP12.	Identfies the Service Connection Point (SCP) object in Active Directory. When a user signs on to ERP 9.0, ERP 9.0 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. ERP 9.0 chooses an SCP object with a status of *running* and retrieves the server name and port number, thus enabling the workstation to make a connection to the server. If you move ERP 9.0 service from one server to another or change the service port number, no changes to the workstation jde.ini file are needed, so 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.

[INTEROPERABILITY]

Setting	Typical Value	Purpose
RegisteredEvents=	RTSOOUT	Names of EventTypes. An event is a ERP 9.0 business transaction running on a ERP 9.0 enterprise server. To enable real-time generation of events, you must register each event that you want to generate in real time.
FilteredEvents=	*ALL	The value of this parameter defines the events that you want to create in real time. A value of *ALL generates all registered events. *NONE disables event generation. You can also enter a subset of registered events.

[SAMPLE_EVENT]

Setting	Typical Value	Purpose
DS1= DS2= DS3=	D4202150B D4202150C D34A1050C	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.

[JDEITDRV]

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.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:jdetrdrv.dll	The directory location of the JDENET driver.

[LREngine]

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.

Understanding Server jde.ini Settings for WebSphere

This section details the settings that are found in the ERP 9.0 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.

See Also

- *J.D. Edwards Integrator to Storefronts Installation Guide* for information about setting up a storefront

- *J.D. Edwards Storefront (Powered by IBM WebSphere Commerce Suite) Guide* for information about IBM storefronts

Note

To access Storefront from the Knowledge Garden, navigate the following path: Product - JDE5 – CRM. Then click on the link to Storefronts in the right frame.

[JDENET]

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.
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 J.D. Edwards sales order status.
JDECustomerCode=	JDEAB	Used with create header. Transaction type for J.D. Edwards Customer add and update.
JDEItemPriceCode=	JDEPRICE	Used with create header. Transaction type for J.D. Edwards price update.
JDEItemQtyCode=	JDEIL	Used with create header. Transaction type for J.D. Edwards 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=		ERP 9.0 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 ERP 9.0 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 your enterprise environment. It is also the key to the installation. If any critical settings exist that are incorrect or left blank, 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 using a text editor. The `jas.ini` file is functionally similar to the `jde.ini` file on the J.D. Edwards ERP Enterprise Server.

Note

Starting with ERP 9.0, many of the settings in the `jas.ini` file were moved to a new file called `JDBj.ini`. See *Web Server jdbj.ini Settings* in the *System Administration Guide* for information about this new file.

To configure the `jas.ini` file, your 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 J.D. Edwards recommendations, you should not need extensive modifications to these paths.
- Verify the port numbers for your TCP/IP connections.

Note

A good practice is to add comment line to your .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 ERP 9.0 Java Server:

Setting	Description
[DB SYSTEM SETTINGS]	This optional section is not delivered as part of the standard jas.ini. Contains settings that enable load balancing for multiple JAS instances by using the Redirector functionality.
[SECURITY]	Contains ERP 9.0 security information.
[OWWEB]	ERP 9.0 Web Server-specific settings. Modify for your environment.
[PORTAL CONFIGURATION]	Contains optional settings for the J.D. Edwards Portal. The settings shown in this section are the default settings and are not required to be included as part of the

CONFIGURATION]	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. 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 important.
[CACHE]	HTTP session settings
[DB CONNECTION POOL]	Starting with ERP9, this section was moved to the `JDBj.ini` file and renamed. See *[JDBj-CONNECTION POOL]* in the *System Administration Guide* for information about the new section.
[JDBC URL]	Starting with ERP9, this section was moved to the `JDBj.ini` file and renamed. See *[JDBj-SPEC DATA SOURCE]* in the *System Administration Guide* for information about the new section.
[JDBC DRIVERS]	Starting with ERP9, this section was moved to the `JDBj.ini` file and renamed. See *[JDBj-JDBC DRIVERS]* in the *System Administration Guide* for information about the new section.
[SERVER COMPONENTS]	Loads ERP 9.0 Java Server packages. Do not modify this section.
[JDENET]	Specifies values for the ERP 9.0 Java Server to communicate with the ERP 9.0 Enterprise Server.
[SERVER]	Specifies values for the ERP 9.0 Java Server to retrieve data dictionary error descriptions from the ERP 9.0 Enterprise Server.
[LOGIN]	Contains settings for login and the Local Director.
[LOGS]	Turns on debug logging and specifies the location of log files.
[TRANSACTIONS]	Contains configuration settings to customize transaction processing within JAS
[JAS Instance]	This optional section is not delivered as part of the standard jas.ini. 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.
[JAS Weight]	This optional section is not delivered as part of the standard jas.ini. 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. Specifies the location to which the Redirector will redirect if no Web Server is

available. Typically, 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 customize the Web GUI interface.

[OWWEB]

Parameter	Recommended Setting	Description
PathCodes=	('JD9','DV9','PY9','PD9')	This parameter must be a valid path code for ERP 9.0. 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.
MO QUEUE=	x:\JDEdwards OneWorld\B9\internet\jdeww\ moqueue (For Windows machines)	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 Web browser. This path *must* translate into virtual path `'/jde/moqueue/'` for the Web browser. The Web server process must have write and create authority to this path.
FtpPort=	21	Specifies the default port to be used for FTP. (Unix and iSeries only)
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 ERP 9.0 (internet) users.
UseProxyServer=	FALSE	Defines whether the ERP 9.0 Java Server uses ProxyServer functionality. Valid values are: • FALSE. This value sends JDENET messages directly from the ERP 9.0 JAS Server and does not employ any proxy server functionality. • TRUE. This value sends JDENET messages through the JOWProxy process of the ERP 9.0 Client. This value is not valid for ERP 9.0.

Parameter	Recommended Setting	Description
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: • 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 is 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=	QB9	The batch queue to which UBE jobs are submitted.
VirtualClientTimeOut	30000	The time in milliseconds before a Virtual Client is timed out.
SystemDateFormat=	MDE	Specifies the system data format.
SystemDateSeparator=	/	Specifies the system data separator.

HelpPath=	/jde/owhelp/	This setting specifies the directory path for the help files. The syntax of the setting is:
		http://[machine]/[path]/
		If you do not specify a setting for HelpPath or use the default setting, /jde/owhelp/, the ERP 9.0 Java Server builds a help path that is based on the current instance of the JAS server.
		For example, if the URL for the ERP 9.0 Java Server is:
		`http://machinename:82/`
		then the ERP 9.0 Java Server assumes that the URL for the help path is:
		`http://machinename:82/jde/owhelp`

OWJRNL=	OWJRNL	This setting is only applicable to ERP 9.0 Java Servers running on AS/400 platforms. If you have manual commit turned on to update the AS/400 DB2 database records, this setting allows the ERP 9.0 Java Server to turn on the JOURNAL for the applicable AS/400 tables. The value that you specify for this setting must be the name of the library name on the AS/400 for the STRJOURNAL stored procedure.
AutoPilotIDs=	FALSE	This setting controls whether the Java Server generates IDs that are useful for scripting HTML client actions by using the J.D. Edwards AutoPilot tool. Valid values are:

Parameter	Recommended Setting	Description
		• 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 login. Used with Basic Authentication.
InitialLanguageCode=	EN	ISO language code for initial user language.
LogoutProcessTimeout=	90	Number of seconds after logout that a business function that is activated by the user continues to run.

[CACHE]

The values that are specified for these keys are in milliseconds. For example, 60000ms is equal to one minute.

Note

- Many of the settings that were in this section before ERP9 have been moved. See *[JDBj-CONNECTIONPOOL]* and *[JDBj-RUNTIMEPROPERTIES]* in the *System Administration Guide*.

Parameter	Recommended Setting	Description
UserSession=	2400000	The time in milliseconds before an inactive user session cache is cleaned up. **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). Default value: `12000000` The `UserSession` value must always be greater than the HTTP session timeout `Invalidate Timeout` setting in WebSphere. Effect of Change: When the `HTTP Session timeout` value is reached, JAS receives notification to remove the UserSession from cache. Changing the `UserSession` value does not effect change as long as this value greater than the

Parameter	Recommended Setting	Description
		`HTTP session timeout` value in WebSphere.
CacheCheck=	300000	The time in milliseconds to check the status of all the objects stored in Cache. Default value: 300000 **Note** J.D. Edwards strongly recommends that you use the default value. 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. 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. Relationship: This value does not depend on any other parameters in the `JAS.INI` file. 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 to a very big number, then CacheManager does not check the status of cached objects often, and invalid objects remain in cache even after they expire.

[SERVER COMPONENTS]

The [SERVER COMPONENTS] section of the jas.ini is used by ERP 9.0 Java Server to set environment variables. Do not modify this section unless you are instructed to do so by J.D. Edwards.

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 MAF (Multiple Application Framework) to fuction correctly. If this setting is missing, ERP applications do not launch under MAF.

[JDENET]

Use this section only if you are running business functions and launching UBEs without the JOWProxy service.

Parameter	Recommended Setting	Description
serviceNameConnect=		The TCP port on which the enterprise server is listening. Modify for your 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:\b9\internet (Windows) /tmp (iSeries and UNIX)	A temporary directory for jdenet. This entry must be a valid directory on your system.

[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 ERP 9.0 is listening to provide glossary text information for the ERP 9.0 JAS server modify for your environment.
codePage=	1252	The code page for displaying the glossary text information.

[LOGS]

This section is used to set system-dependent value for various logging functions that are related to the ERP 8.0 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 that is included in the path must exist on your system.
Debuglog=	Site-dependent variable	The name and location of the jasdebug.log file. The directory that is included in the path must exist on your system.
JdbcTrace=	FALSE	TRUE Trace logging of JDBC statements are included in the standard output log file. FALSE No trace logging is performed.
stderr=	Site-dependent variable	Specifies the WebSphere log directory for input errors. 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. Usually the directory under B9. The default path is: iSeries: /PeopleSoft/B9/stderr.log Windows: c:\WebSphere\AppServer\logs\stderr.log Unix: /u01/PeopleSoft/B9/stderr.log
stdout=	Site-dependent variable	Specifies the WebSphere log directory for output errors. 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. Usually the directory under B9. The default path is: iSeries: /PeopleSoft/B9/stdout.log Windows: c:\WebSphere\AppServer\logs\stdout.log Unix: /u01/PeopleSoft/B9/stdout.log

[SECURITY]

Confirm the following settings for the [security] section. These settings are unique to the JAS security server.

Parameter	Recommended Setting	Description
DefaultEnvironment=	JPD9	Specifies the default ERP 9.0 environment.
NumServers=	1	Specifies the total number of ERP 9.0 security servers that are defined as being available to users who sign on to this ERP 9.0 Java Server. If this parameter is missing or has a value of blank, the default value is 1; the sign n is handled by the primary security server that is defined by the `SecurityServer=` parameter in the `[SECURITY]` section of the jas.ini
SecurityServer=	Site-dependent variable	Specifies the name of the security server that is defined for your ERP 9.0 Enterprise Server installation.
SecurityServer*N*=	Site-dependent variable	Specifies the name of the secondary server. You can define multiple security servers if you want sign on to fail over to valid secondary servers if users cannot sign on to the primary server. Valid values for *N* are numeric values from 1 to n where: Defines the first secondary security server Defines the second secondary security server N defines any number of sequentially accessed security server
UserLogonCookie=	FALSE	Defines whether user signon information is saved in an encrypted cookie on the HTML client machine. This information includes user name, password, and environment. Valid values are: • 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. You must use this setting when using the JAS Redirector.
CookieLifeTime unit is	“day”	Specifies the unit of time used by the `CookieLifeTime=` parameter.
CookieLifeTime=	7	Specifies the amount of time before a cookie expires, measured by the value of the `CookieLifeTime unit is` parameter.

[PORTALCONFIGURATION]

This section contains optional settings for the ERP 9.0 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 above 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 public long getLastLoadedTimestamp();. 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

Parameter	Recommended Setting	Description
		portal performance. Use caution when changing this value.
cache_workspace_timeout	300000	The interval in milliseconds 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. Changing this value can drastically affect portal performance. Use caution when changing this value.
cache_workspace_refresh	0	The time in milliseconds before the system deletes all of the workspaces from the cache. Changing this value can drastically affect portal performance. Use caution when changing this value.
cache_component_purge	3600000	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. Changing this value can drastically affect portal performance. Use caution when changing this value.
cache_component_expire	900000	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 public long getLastLoadedTimestamp();. A component does not expire unless a user accesses it. If set to zero, the system never expires components from the cache. Changing this value can drastically affect portal performance. Use caution when changing this value.
cache_component_timeout	300000	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. Changing this value can drastically affect portal performance. Use caution when

Parameter	Recommended Setting	Description
		changing this value.
cache_component_refresh	0	The time in milliseconds before the system deletes all components from the cache. Changing this value can drastically affect portal performance. Use caution when changing this value.
cache_itrust_purge	60000	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. Changing this value can drastically affect portal performance and security. Use caution when changing this value.
cache_itrust_expire	0	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 public long getLastLoadedTimestamp();. An inherited trust session does not expire unless a user accesses it. You should not change this setting unless instructed to do so by J.D. Edwards
cache_itrust_timeout=	30000	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.
cache_itrust_refresh	0	The time in milliseconds before the system deletes all of the inherited trust sessions from the cache.
cache_entbutton_purge	3600000	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. Changing this value can drastically affect portal performance. Use caution when changing this value
cache_entbutton_expire	0	For expirable components, the time in milliseconds in addition to the last loaded

Parameter	Recommended Setting	Description
		timestamp before an Enterprise Navigation Bar button is deleted. To make a component expirable, implement public long getLastLoadedTimestamp();. 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 your Web server is other than 80, you must specify the port. The syntax is: `ip_address:port`, where `ip_address:port` refers to the local ERP 9.0 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	URI 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.
perimg	/jde/owportal/images/ edit2.gif	Default personalize the icon file path and name, such as: /jde/images/edit2.gif. Both relative and fully qualified URLs are valid.

Parameter	Recommended Setting	Description
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; he or she must create and configure it to be included in the JDE 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 hyperlink 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.
corplogolinkurl		The URL of the default corporate logo hyperlink. This link is used when the current workspace does not specify a link. This setting has no default value. Both relative and fully qualified URLs are valid.
DataMigrationHasOccurred	This is a system setting; do not modify this setting or add it the jas.ini	True-- if B9 pristine component and workspace data have been updated.

Parameter	Recommended Setting	Description
	file.	workspace data have been updated.
DefaultWorkspace		The workspace to display when no other workspace is specified or when DefaultWorkspaceOnly is set to TRUE. Use uppercase letters to set this parameter. This setting has no default value.
DefaultWorkspaceOnly	FALSE	Allows access to the default workspace only.
edtimg	/jde/owportal/images/ edit2.gif	The URL of the default edit icon. The edit icon is used for buttons that allow the user to alter an object. Both relative and fully qualified URLs are valid.
jde	`x:\Program Files\JDEdwards\JAS\EA_JAS_80.ear\webclient.war` (Windows) `/JDEdwards/JAS/EA_JAS_80.ear/webclient.war` (UNIXand iSeries)	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	Default|#FFFFFF|#00009C|#0063CE|#080029 |#CECECE|#FFFFFF|#636363|#FFFFFF |background.jpg| /jde/owportal/owportal.css	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	Springtime|#FFFFFF|#218C7B|#84BDB5 |#006B63|#CECECE|#FFFFFF|#FF6B29 |#FFFFFF |springtimebkgd.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.
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|#FFF	Delimited String for color schemes. String consists of name, background color, toolbar color, tool bar tools color, fixed area color,

Parameter	Recommended Setting	Description
	FFF |technobkgd.gif| /jde/owportal/portal.css	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.

See Also

- *J.D. Edwards Web Server Installation Guide* on the Update Center of the Knowledge Garden for the most up-to-date jas.ini and jdbj.ini file settings (these settings can change with each service pack release)
- *Interoperability Overview* and other topics in the *Interoperability Guide* for information about configuring Interoperability
- *Enterprise XPI Foundation Installation and Configuration Guide* for more information about configuring XPIe on a J.D. Edwards ERP system
- *Creating a Workflow Process* and other topics in the *J.D. Edwards Workflow Tools Guide* for information about configuring workflow

[JAS PREFERENCE]

Setting	Typical Value
JasServer=	ownts1
Port=	80
Servlet=	/jde/servlet/html.login

Web Server jdbj.ini Settings

The `jdbj.ini` file contains configuration information for JDBj, which allows the J.D. Edwards Web Server to access ERP databases. The parameters in this file are only used for accessing J.D. Edwards ERP 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`.ini file is functionally similar to the `jde.ini` file on the J.D. Edwards ERP Enterprise Server.

Hint

It is generally good practice to add comment line to your .ini files to include such information as:

- The current JAS package version (as labeled on the CD)
- The date 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:

- J.D. Edwards ERP Data-Specific Sections
- General Sections

J.D. Edwards ERP Data-Specific Sections

The following `jdbj.ini` sections apply only when accessing J.D. Edwards ERP data. These sections are ignored for standalone database access.

Setting	Description
[JDBj-BOOTSTRAP SESSION]	Contains signon 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 on for access to system tables. JDBj signs this user on via the security server during the bootstrap process. if the signon information is not valid, then no access to the OneWorld/ERP database is possible.

Note

The information in this section should match the corresponding information that is specified in the [DB SYSTEM SETTINGS] section of the `JDE.INI` file of your previous installation (before ERP 9).

Parameter	Recommended Setting	Description
user=	Site-dependent variable	User name for logging in to the OneWorld/ERP security server.
password=	Site-dependent variable	Password for logging in to the OneWorld/ERP security server.
environment=	Site-dependent variable	The OneWorld/ERP environment that

Parameter	Recommended Setting	Description
		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 later, to look up OCM entries on demand. If it is not valid, then no OneWorld/ERP database access is possible.

Note

The information in this section should match the corresponding information that is specified in the [DB SYSTEM SETTINGS] section of the `JDE.INI` file of your previous installation (before ERP 9).

[JDBj-BOOTSTRAP DATA SOURCE]		
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	Select the type of database that is used by the OneWorld/ERP system. (All servers)
server=	Site-dependent variable	Name of the server. (AS/400, 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 AS/400) (AS/400, SQL Server)
owner	Site-dependent variable	The database owner. (Oracle, SQL Server, UDB)
lob=	True	Supports lobs.

[JDBj-BOOTSTRAP DATA SOURCE]		
Parameter	**Recommended Setting**	**Description**
	False	(Oracle and AS/400)
unicode=	True False	Performs unicode conversion. (SQL Server)

[JDBj-SPEC DATA SOURCE]

This optional section defines the data source where the serialized spec tables reside. JDBj uses these parameters at bootstrap time and after to look up serialized spec objects on demand. If this section is not specified, then JDBj uses the OCM to find the serialized spec table. If it is not valid, no J.D. Edwards ERP database access is possible.

[JDBj-SPEC DATA SOURCE]		
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	Select the type of database that is used by the OneWorld/ERP system. (All servers)
server=	Site dependent variable	Name of the server. (AS/400, 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 AS/400) (AS/400, SQL Server)
owner=	Site-dependent variable	The database owner. (Oracle, SQL Server, UDB)
lob=	True False	Supports lobs. (Oracle and AS/400)
unicode=	True False	Performs unicode conversion. (SQL Server)

[JDBj-SPEC DATA SOURCE]		
Parameter	**Recommended Setting**	**Description**
user=	Site-dependent variable	User name for logging in to the OneWorld/ERP server.
password=	Site-dependent variable	Password for logging in to the OneWorld/ERP server.

See Also

- *[JDBj-BOOTSTRAP DATA SOURCE]* in the *System Administration Guide* for information about which fields must be filled in for a given database platform

General Sections

The rest of the sections apply when accessing both ERP 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.

[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 releases of J.D. Edwards ERP, setting Oracle and iSeries drivers was not necessary because they were defaults for the Web Server. However, J.D. Edwards ERP does not assume any default drivers to avoid JAS classpath exceptions. The Web Server only loads the drivers that you specify in this section.

[JDBC DRIVERS]		
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 AS/400.
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	Specifies the location of your 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. The default value is: D:\Oracle\Ora9\ network\ADMIN\tnsnames.ora The value "Ora9" identifies the version of Oracle that you are using. This value changes if you install a different version of Oracle.

[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 environement has a negative impact on perfomance.

[JDBj-CONNECTION POOL]

These settings are used for pooling JDBC connections.

Parameter	Recommended Setting	Description
jdbcPooling=	False	Currently, JDBC pooling is not 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	The time (in milliseconds) before an inactive connection cache is removed from the pool. Before ERP 9, this setting was the *Connection* parameter in the [cache] section.
CleanPoolInterval=	300000	Specifies how often the pool cleaner is set to clean data sources that have a validation string. **Note** The values that are specified for these keys are in milliseconds. For example, 60000ms is equal to one minute. The validation string is in the form: `ValidationString_x=<statement>` where `x` is I, 4, or R for DB2/400, S for SQL Server, O for Oracle and `statement` is a SQL statement that any user can execute. For example: ValidationString_I=Select * from QSYS2.SYSCOLUMNS WHERE 1=2 ValidationString_S=Select @@connections ValidationString_O=Select sysdate from dual
maxSize	50	Maximum number of JDBC prepared statements cached on

		each JDBC connection.
cachePurgeSize	5	Number of JDBC statements that are 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 values that are listed are the defaults. The template default entries are commented out. Remove the pound sign (#) when changing these values.

Parameter	Recommended Setting	Description
dataCacheEntrySizeThreshold=	500	Sets the maximum size (in rows) 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. Valid values are -1 or greater.
dataCacheEntryThreshold=	100	Sets the maximum size (in entries) 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.
forceSingleDataSource=	False	Indicates whether JDBj should force operations involving multiple database objects to run against a single data source. If this is value is true, JDBj only resolves the physical data source for the first database object that is involved in an operation. If this value is false, JDBj 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: • True • False

resultSetTimeout=	60000	Time (in milliseconds) before a result set timeouts if it has not had any operations. J.D. Edwards recommends using the default setting. Valid values are -1 or greater. Before ERP 9, this setting was the `ResultSet` parameter in the [cache] section.
retryInterval=	0	Retry interval property. Sets the interval (in milliseconds) to wait before retrying idempotent database operations. -1 means not to retry; 0 means retry immediately. Valid values are -1 or greater.
retryMaximum=	5	Sets the number of times to retry idempotent database operations. -1 means to retry indefinitely. Valid values are -1 or greater.
ocmCachePurge=	3600000	Sets the number of milliseconds after which inactive OCM cache entries are purged. 0 means to never purge OCM cache entries.
personalSpecVersions=	False	Indicates if a user's personal version can be read. This information is only enforced during a read and not during a spec generation. If it set to a true, the personal version is returned if it exists; otherwise, the public version is returned. If the property is set to a false, then the personal version is not read and defaults to the public version. Valid values are: • True • False
securityCachePurge=	3600000	Time (in milliseconds) before an inactive service cache entries are purged. 0 means to never purge service cache entries. J.D. Edwards recommends using the default values.

		Valid values are 0 or greater Before ERP 9, this setting was the `Security` parameter in the [cache] section.
serviceCachePurge=	3600000	Time (in milliseconds) before inactive service cache entries are purged. 0 means to never purge service cache entries. Valid values are 0 or greater Before ERP 9, this setting was the `UDCInfo` parameter in the [cache] section.
specCachePurge=	3600000	Time (in milliseconds) before inactive spec cache entries are purged. 0 means to never purge spec cache entries. Valid values are 0 or greater Before ERP 9, this setting was the `ViewTable` parameter in the [cache] section.
specConsistencyCheck=	minimal	The level of spec consistency checking. Set this property to a higher level to improve exception messages relating to spec inconsistency problems. Set this property to a lower level when it is not needed since it can degrade performance. Valid values are: • Full • Minimal • None
transactionIsolation=	default	Sets the isolation level for transactions. Valid values are: • Default • None • Read uncommitted • Read committed • Repeatable read • Serializable
transactionTimeout=	120000	Time (in milliseconds) before a transaction timeoust. A transaction timeouts if it has not had any operations for the specified period of time. If this timeout is set to a -1, then the transaction timeout feature is disabled. (This action

		currently only happens when JDBj is run as part of a JAS transaction.) Valid values are -1 or greater.
triggerAutoFetch=	none	Indicates whether JDBj should automatically fetch rows to be changed to pass them to OneWorld triggers. This action is needed for certain triggers to work properly. Valid values are: • None • Single • All
updatableResultSetTimeout=	-1	Time (in milliseconds) before an updatable result set timeouts if it has not had any operations. -1 indicates that updatable result sets should have the same value as RESULT_SET_TIMEOUT. Valid values are -1 or greater.
usageExecutionThreshold=	20000	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. Valid values are 0 or greater.
usageFetchSizeThreshold=	500	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. -1 indicates that any fetch size is valid. Valid values are -1 or greater.
usageResultSetOpenThreshold=	60000	Maximum time (in milliseconds) for a result set to remain open. If a result set is left 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. A usage result set open threshold value of -1 indicates that no such usage tracking will occur.

		Valid values are -1 or greater.
usageTracking=	false	Enables or disables usage tracking. This setting provides additional tracking and logging to use during testing. Usage tracking does incur a performance penalty, so it should be disabled for production code. Valid values: • True • False
usageTrackingOutput=	log	Specifies the destination of usage tracking output. Valid values are: • 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`	Use to build fully qualified URLs for a browser request for a resource.
DisplayEnvironment=	Administrator preference	Environment display rule if a default environment has been set with DefaultEnvironment. Show: User can override the default environment at login. Hidden: The user cannot see the environment box at login. ReadOnly: The user cannot tamper with the environment setting at login. UseDefault: The user can select different environments at login, but the system overrides any other user choice and logs in to the default environment anyway.
DisablePasswordAboutToExpire	TRUE	Override that suppresses *password about to expire* notification.

[TRANSACTIONS]

This section is used to set configuration settings to customize transaction processing within JAS.

[TRANSACTIONS]		
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 five minutes.
MaxAge=	10	Maximum age in minutes of a transaction. Transactions older than this number are rolled back by the TransactionReaper. Valid value is an integer from 1 to n. Default is ten minutes.

[ERPINTERACTIVITY]

This section is used to activate and configure the Interactive HTML settings. These setting are new for Service Pack 22.

Parameter	Recommended Setting	Description
InteractivityLevel=	LOW or HIGH	Indicates the level of interactivity for the entire instance of JAS. Valid values are: • LOW (default) • MEDIUM • HIGH In Low Interactivity mode, whenever a critical or non-critical posting event happens, the whole page is sent to the Web server; the user has to wait for the page to come back. When it does, the whole page is repainted, which usually causes a flash on the browser. This action is equivalent to the functionality in SP21 and below. An example of Critical Events that force a post are: Form. Row ,View ,Tools Exit, or Toolbar button clicks; clicking on Visual Assist; switching Tab pages; expanding or collapsing tree nodes; parent and child tree drag-and-drops; and clicking on clickable static text control. Certain other events can be marked in FDA to force a post. In Medium Interactivity mode, the data transfer and event execution occurs at the same points that Low Interactivity causes a full page refresh. However, unlike Low interactivity mode, Medium interactivity does not send the whole page when these events happen; it sends only the queued

		events and data to the server. Furthermore, it does not do a whole page refresh. It uses JavaScript and DHTML to repaint only the changed controls. The page flash does not happen in this mode. In High interactivity, events and data are transferred far more frequently. It posts when critical events happen. It also 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. Furthermore, it does not do a whole page refresh. It uses JavaScript and DHTML to repaint only the changed controls. The page flash does not happen in this mode. **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.
MultipleBrowserEnabled=	FALSE	This setting determines whether to launch multiple applications in seperate browsers from Task Explorer and portal links. Valid values are: • TRUE • FALSE (default)
MaxOpenBrowsers=	10	[1-n] The default value is 10. 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 *not* 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. Maximum number of records that is 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 warning. After you click OK, the Web Server displays a second warning for the second set of 500 records.

[WEB GUI]

This section is used to customize the web GUI interface and is new for Service Pack 22.

Parameter	Recommended Setting	Description
bandwidth=	narrow wide (default)	The bandwidth setting is used to customize the GUI interface to account for networks with low bandwidth. By default, the J.D. Edwards Web Server uses tab decoration on all o the OneWorld/ERP forms that are displayed in HTML. Tab decoration shows tabs with rounded corners but requires more bandwidth to display in 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 simple 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.