ORACLE
JD EDWARDS ENTERPRISEONE

JD Edwards EnterpriseOne Tools 8.97 Security Administration Guide

October 2007

ORACLE

JD Edwards EnterpriseOne Tools 8.97 Security Administration Guide
SKU E1_TOOLSTSC-B1007

Contents

About This Documentation Preface

JD Edwards EnterpriseOne implementation guides provide you with the information that you need to implement and use JD Edwards EnterpriseOne applications from Oracle.

This preface discusses:

- JD Edwards EnterpriseOne application prerequisites.
- Application fundamentals.
- Documentation updates and printed documentation.
- Additional resources.
- Typographical conventions and visual cues.
- Comments and suggestions.
- Common fields in implementation guides.

Note. Implementation guides document only elements, such as fields and check boxes, that require additional explanation. If an element is not documented with the process or task in which it is used, then either it requires no additional explanation or it is documented with common fields for the section, chapter, implementation guide, or product line. Fields that are common to all JD Edwards EnterpriseOne applications are defined in this preface.

JD Edwards EnterpriseOne Application Prerequisites

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

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

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

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

Application Fundamentals

Each application implementation guide provides implementation and processing information for your JD Edwards EnterpriseOne applications.

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

The application fundamentals implementation guide consists of important topics that apply to many or all JD Edwards EnterpriseOne applications. Whether you are implementing a single application, some combination of applications within the product line, or the entire product line, you should be familiar with the contents of the appropriate application fundamentals implementation guides. They provide the starting points for fundamental implementation tasks.

Documentation Updates and Printed Documentation

This section discusses how to:

- Obtain documentation updates.
- Download documentation.

Obtaining Documentation Updates

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

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

See Also

Oracle's PeopleSoft Customer Connection, http://www.oracle.com/support/support_peoplesoft.html

Downloading Documentation

In addition to the complete line of documentation that is delivered on your implementation guide CD-ROM, Oracle makes JD Edwards EnterpriseOne documentation available to you via Oracle's website. You can download PDF versions of JD Edwards EnterpriseOne documentation online via the Oracle Technology Network. Oracle makes these PDF files available online for each major release shortly after the software is shipped.

See Oracle Technology Network, http://www.oracle.com/technology/documentation/psftent.html.

Additional Resources

The following resources are located on Oracle's PeopleSoft Customer Connection website:

Resource	Navigation
Application maintenance information	Updates + Fixes
Business process diagrams	Support, Documentation, Business Process Maps

Resource	Navigation
Interactive Services Repository	Support, Documentation, Interactive Services Repository
Hardware and software requirements	Implement, Optimize + Upgrade; Implementation Guide; Implementation Documentation and Software; Hardware and Software Requirements
Installation guides	Implement, Optimize + Upgrade; Implementation Guide; Implementation Documentation and Software; Installation Guides and Notes
Integration information	Implement, Optimize + Upgrade; Implementation Guide; Implementation Documentation and Software; Pre-Built Integrations for PeopleSoft Enterprise and JD Edwards EnterpriseOne Applications
Minimum technical requirements (MTRs)	Implement, Optimize + Upgrade; Implementation Guide; Supported Platforms
Documentation updates	Support, Documentation, Documentation Updates
Implementation guides support policy	Support, Support Policy
Prerelease notes	Support, Documentation, Documentation Updates, Category, Release Notes
Product release roadmap	Support, Roadmaps + Schedules
Release notes	Support, Documentation, Documentation Updates, Category, Release Notes
Release value proposition	Support, Documentation, Documentation Updates, Category, Release Value Proposition
Statement of direction	Support, Documentation, Documentation Updates, Category, Statement of Direction
Troubleshooting information	Support, Troubleshooting
Upgrade documentation	Support, Documentation, Upgrade Documentation and Scripts

Typographical Conventions and Visual Cues

This section discusses:

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

Typographical Conventions

This table contains the typographical conventions that are used in implementation guides:

Typographical Convention or Visual Cue	Description
Bold	Indicates PeopleCode function names, business function names, event names, system function names, method names, language constructs, and PeopleCode reserved words that must be included literally in the function call.
Italics	Indicates field values, emphasis, and JD Edwards EnterpriseOne or other book-length publication titles. In PeopleCode syntax, italic items are placeholders for arguments that your program must supply. We also use italics when we refer to words as words or letters as letters, as in the following: Enter the letter *O*.
KEY+KEY	Indicates a key combination action. For example, a plus sign (+) between keys means that you must hold down the first key while you press the second key. For ALT+W, hold down the ALT key while you press the W key.
`Monospace font`	Indicates a PeopleCode program or other code example.
" " (quotation marks)	Indicate chapter titles in cross-references and words that are used differently from their intended meanings.
. . . (ellipses)	Indicate that the preceding item or series can be repeated any number of times in PeopleCode syntax.
{ } (curly braces)	Indicate a choice between two options in PeopleCode syntax. Options are separated by a pipe (|).
[ ] (square brackets)	Indicate optional items in PeopleCode syntax.
& (ampersand)	When placed before a parameter in PeopleCode syntax, an ampersand indicates that the parameter is an already instantiated object. Ampersands also precede all PeopleCode variables.

Visual Cues

Implementation guides contain the following visual cues.

Notes

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

Note. Example of a note.

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

Important! Example of an important note.

Warnings

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

Warning! Example of a warning.

Cross-References

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

Country, Region, and Industry Identifiers

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

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

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

Country Identifiers

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

Region Identifiers

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

- Asia Pacific
- Europe
- Latin America
- North America

Industry Identifiers

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

- USF (U.S. Federal)

- E&G (Education and Government)

Currency Codes

Monetary amounts are identified by the ISO currency code.

Comments and Suggestions

Your comments and suggestions are important to us. We encourage you to send us your feedback about our PeopleBooks and other reference and training materials. Please include the release numbers for the PeopleTools and applications that you are currently using. Email your comments to PSOFT-INFODEV_US@ORACLE.COM.

Common Fields Used in Implementation Guides

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

As If Currency Code Enter the three-character code to specify the currency that you want to use to view transaction amounts. This code enables you to view the transaction amounts as if they were entered in the specified currency rather than the foreign or domestic currency that was used when the transaction was originally entered.

Batch Number Displays a number that identifies a group of transactions to be processed by the system. On entry forms, you can assign the batch number or the system can assign it through the Next Numbers program (P0002).

Batch Date Enter the date in which a batch is created. If you leave this field blank, the system supplies the system date as the batch date.

Batch Status Displays a code from user-defined code (UDC) table 98/IC that indicates the posting status of a batch. Values are:

Blank: Batch is unposted and pending approval.

A: The batch is approved for posting, has no errors and is in balance, but has not yet been posted.

D: The batch posted successfully.

E: The batch is in error. You must correct the batch before it can post.

P: The system is in the process of posting the batch. The batch is unavailable until the posting process is complete. If errors occur during the post, the batch status changes to *E*.

U: The batch is temporarily unavailable because someone is working with it, or the batch appears to be in use because a power failure occurred while the batch was open.

Branch/Plant Enter a code that identifies a separate entity as a warehouse location, job, project, work center, branch, or plant in which distribution and manufacturing activities occur. In some systems, this is called a business unit.

Business Unit Enter the alphanumeric code that identifies a separate entity within a business for which you want to track costs. In some systems, this is called a branch/plant.

Category Code Enter the code that represents a specific category code. Category codes are user-defined codes that you customize to handle the tracking and reporting requirements of your organization.

Company Enter a code that identifies a specific organization, fund, or other reporting entity. The company code must already exist in the F0010 table and must identify a reporting entity that has a complete balance sheet.

Currency Code Enter the three-character code that represents the currency of the transaction. JD Edwards EnterpriseOne provides currency codes that are recognized by the International Organization for Standardization (ISO). The system stores currency codes in the F0013 table.

Document Company Enter the company number associated with the document. This number, used in conjunction with the document number, document type, and general ledger date, uniquely identifies an original document.

If you assign next numbers by company and fiscal year, the system uses the document company to retrieve the correct next number for that company.

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

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

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

P: Accounts payable documents.

R: Accounts receivable documents.

T: Time and pay documents.

I: Inventory documents.

O: Purchase order documents.

S: Sales order documents.

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

	• The date on which a change of address becomes effective. • The date on which a lease becomes effective. • The date on which a price becomes effective. • The date on which the currency exchange rate becomes effective. • The date on which a tax rate becomes effective.
Fiscal Period and **Fiscal Year**	Enter a number that identifies the general ledger period and year. For many programs, you can leave these fields blank to use the current fiscal period and year defined in the Company Names & Number program (P0010).
G/L Date (general ledger date)	Enter the date that identifies the financial period to which a transaction will be posted. The system compares the date that you enter on the transaction to the fiscal date pattern assigned to the company to retrieve the appropriate fiscal period number and year, as well as to perform date validations.

JD Edwards EnterpriseOne Tools Security Administration Preface

This preface discusses Oracle's JD Edwards EnterpriseOne Tools 8.97 Security Administration guide.

JD Edwards EnterpriseOne Tools

This guide refers to this Oracle product line: JD Edwards EnterpriseOne Tools. In addition to the security topics discussed in this guide, essential information describing the setup and design of the system resides in companion documentation. The companion documentation consists of important topics that apply to many or all JD Edwards EnterpriseOne Tools. You should be familiar with the contents of these guides as well.

This guide contains references to server configuration settings that JD Edwards EnterpriseOne stores in configuration files (such as jde.ini, jas.ini, jdbj.ini, jdelog.properties, and so on). Beginning with the JD Edwards EnterpriseOne Tools Release 8.97, it is highly recommended that you only access and manage these settings for the supported server types using the Server Manager program. See the *Server Manager Guide* on Customer Connection.

The following companion guides contain information that applies to JD Edwards EnterpriseOne configuration and administration:

- System Administration
- Server and Workstation Administration
- Configurable Network Computing Implementation
- Package Management

See Also

JD Edwards EnterpriseOne Tools 8.97 System Administration Guide, "Getting Started with JD Edwards EnterpriseOne Tools System Administration"

JD Edwards EnterpriseOne Tools 8.97 Server and Workstation Administration Guide, "Getting Started with JD Edwards EnterpriseOne Tools Server and Workstation Administration"

JD Edwards EnterpriseOne Tools 8.97 Configurable Network Computing Implementation Guide, "Getting Started with JD Edwards EnterpriseOne Tools Configurable Network Computing Implementation"

JD Edwards EnterpriseOne Tools 8.97 Package Management Guide, "Getting Started with JD Edwards EnterpriseOne Package Management"

CHAPTER 1

Getting Started with JD Edwards EnterpriseOne Tools Security Administration

This chapter discusses:

- Security Administration Overview
- Security Administration Implementation

Security Administration Overview

Oracle's JD Edwards EnterpriseOne Tools provides security features, including components and JD Edwards EnterpriseOne security applications, to ensure that your company's sensitive application data is protected.

Security Administration Implementation

In the planning phase of your implementation, take advantage of all Oracle sources of information for JD Edwards EnterpriseOne, including the installation guides and troubleshooting information. A complete list of these resources appears in the preface in *About This Documentation* with information about where to find the most current version of each.

CHAPTER 2

Understanding JD Edwards EnterpriseOne Security

This chapter provides an overview of JD Edwards EnterpriseOne security and discusses:

- Object-level security.
- Users, roles, and *PUBLIC.
- How JD Edwards EnterpriseOne checks security.
- Cached security information.

JD Edwards EnterpriseOne Security Overview

JD Edwards EnterpriseOne security enables a security administrator to control security for individual users and for groups of users. 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. The User Security application (P98OWSEC) uses the F98OWSEC table to manage the JD Edwards EnterpriseOne user IDs and system (database) user IDs. Use P98OWSEC to create, test, and change user security for JD Edwards EnterpriseOne and the logically attached database management systems.

See Chapter 5, "Setting Up User Security," page 43.

The Security Workbench application (P00950) enables you to secure JD Edwards EnterpriseOne objects, such as applications, forms, rows, tabs, and so on. It stores all objects security records in the F00950 table.

See Chapter 7, "Using Security Workbench," page 65.

Object-Level Security

JD Edwards EnterpriseOne security is at the object level. This level means that you can secure specific objects within JD Edwards EnterpriseOne, which provides flexibility and integrity for your security. For example, you can secure a user from a specific form and then, no matter how the user tries to access the form (using a menu or any application that calls that form), the software prevents access to the form. The software simplifies the process of setting up security by enabling you to set security for hundreds of objects at one time by securing all objects on a specific menu or by securing all objects under a specific system code.

Note. Only the objects are secured; the software does not support menu or system code security. Object security provides a higher level of integrity.

For example, if you secured a specific menu to prevent users from accessing the applications on that menu, the users might still be able to access those applications through another menu or another application that accesses the applications that you wanted to secure.

Object Level Security Types

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

Level of Security	Description
Application security	Secures users from running or installing, or both, a particular application, an application version, or a form within an application or application version.
Action security	Secures users from performing a particular action, such as adding, deleting, revising, inquiring, or copying a record.
Row security	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 in an application or application version. This item can be a database or non-database field that is defined in the data dictionary, such as the work/calculated fields. For example, if you secure a user from viewing the Salary field on the Employee Master application, the Salary field does not appear on the form when the user accesses that application.
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 or application versions. 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 select 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 JD Edwards EnterpriseOne forms. These exits call applications and allow users to manipulate data. Exit security also restricts use of the same menu options.
Exclusive application security	Overrides row security that is set for an application. When you set exclusive application security for a user, the system overrides row security for every table that is accessed by the application that is specified. All other security still applies.

Level of Security	Description
External calls security	Secures users from accessing standalone executables that exist external to JD Edwards EnterpriseOne. These external executables, which might include design tools, system monitors, and debugging tools, are specific to JD Edwards EnterpriseOne.
Data Browser security	Controls access to the Data Browser program.
Published business service security	Controls access to published business services. For published business services, JD Edwards EnterpriseOne uses a "secure by default" security model which means that users cannot access a published business service unless a security record exists that authorizes access. For all other objects in JD Edwards EnterpriseOne, access is granted unless otherwise secured or restricted.
Push button, image, and link security	Controls whether users can user or view push button, link, and image controls.
Media object security	Controls whether users can add, change, delete, or view media objects within interactive applications, forms, or application versions.

Users, Roles, and *PUBLIC

The JD Edwards EnterpriseOne security administrator can set up security for:

- A particular user

  This option controls security by specific JD Edwards EnterpriseOne user ID.

- A user role

  This option controls security by role, which enables you to group users based on similar job requirements. An example is putting all of the accounts payable clerks in one role, such as Accounts Payable (AP).

- All users

  This option controls security for all users who are designated by ID type **PUBLIC* in the User or Role field. The designation **PUBLIC* is a special ID within JD Edwards EnterpriseOne that automatically includes all of the users within it. You can use this ID to apply security even if you do not have a specific record set up for it in user profiles.

How JD Edwards EnterpriseOne Checks Security

When a user attempts to access an application or perform an action, JD Edwards EnterpriseOne checks security for that particular user ID. If security exists for that user ID, the software displays a message indicating that the user cannot proceed.

If the user ID has no security, the software checks role profiles (if that user is part of a specific role), and then *PUBLIC for security. If no security is established at any of these levels, the software allows the user to continue.

JD Edwards EnterpriseOne also provides software license security through protection codes, and it requires user validation at sign-in and when accessing new data sources.

Cached Security Information

JD Edwards EnterpriseOne caches security information from the F00950 table in the workstation's memory cache for JD Edwards EnterpriseOne. If system administrators make changes to this table, those changes are not immediately realized on workstations that are logged on to the system while security revisions are being made. The workstations must sign off and sign back on before the security changes are enabled.

CHAPTER 3

Working with User and Role Profiles

This chapter provides overviews of user profiles, how role profiles make profiling easier, tables used by the User Profile Revisions application (P0092), and discusses how to:

- Set up user profiles.
- Set up role profiles.

Understanding User and Role Profiles

You use the P0092 application to add users and to set up user profiles. For every user, you must create a user profile, which defines such information as the a list of environments that a user can select when signing in to JD Edwards EnterpriseOne and the language preference of the user. You can also assign roles to users. A role defines the tasks that an end user sees in JD Edwards EnterpriseOne.

You can use P0092 to define specific users or roles. This definition includes:

- The role to which a user belongs.

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

How to Assign and Delete Environments for User and Role Profiles

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

How to Assign Business Preferences to User and Role Profiles

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

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

User and Role Profile Copying

You can copy all or part of a user or role profile. When you copy an entire user or role profile (display and environment preferences), you are creating a new user or role 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.

Understanding How Role Profiles Make Profiling Easier

Roles eliminate the need to set up preferences for each individual user profile. By assigning individual users to a role, you can assign preferences to the role and have those settings available to all of the individual users who have that role. We recommend creating all profiles that are needed for the enterprise first. This method makes creating user profiles easier; instead of defining specific environments, packages, and machine configurations for each user, administrators can define them for the role. If an individual in a role needs a different setup, you can assign different setups at the user profile level, which overrides the role settings.

JD Edwards EnterpriseOne uses roles for these purposes:

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

Tables Used by the User Profile Revisions Application

The P0092 application uses these tables:

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

See Also

JD Edwards EnterpriseOne Tools 8.97 Package Management Guide, "Deploying Packages," Defining Machines

Chapter 3, "Working with User and Role Profiles," Setting Up User Profiles, page 9

Chapter 3, "Working with User and Role Profiles," Creating and Modifying User Profiles, page 12

Chapter 3, "Working with User and Role Profiles," Creating Profiles by Using a Batch Process, page 15

Setting Up User Profiles

This section provides overviews of setting up user profiles, how to add users, lists prerequisites, and discusses how to:

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

Understanding User Profile Setup

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

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

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

   See Chapter 3, "Working with User and Role Profiles," Setting Up Roles, page 16.

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

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

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

User Profile Creation and Modification

The user profile defines certain setup and display features, such as access to Fast Path, language, date format, or country code. If you select a country code for a user, the menu filtering process displays for that user any special menu selections unique to that country code. For example, if you enter *CA* (Canada), that user would see the Canadian Tax Information application on the appropriate menu, which users without that country code would not see.

Batch Process for Creating User Profiles

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

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

Report Used for Reviewing User Profiles

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

Understanding How to Add Users

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

Note. This section is a checklist for all the steps needed to add a new user. These steps do not address third-party setup issues such as assigning network user IDs.

How to Add an Individual User

If you need to add only a few users, use the User Profile Revisions program. The following list details the steps for adding user profiles one at a time.

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

How to Add Multiple Users

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

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

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

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

The following list details the steps that you need to perform when you add multiple user profiles simultaneously.

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

   If you are migrating data from a non- JD Edwards EnterpriseOne system, you can populate the data tables with a table conversion. Otherwise, you can manually add data to the Address Book tables.
4. Run the Populate User Profiles (R0092) batch process to create user profile records from existing Address Book records.

   Normally, this report is based on address book records with a search type for employees (*E*). You have the option of picking one default role for everyone or running the report more than once for different roles.
5. Adjust each user's role assignments.

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

   These settings are dictated by role:

   - Environments
   - User Overrides
   - Application Security
6. Run the Summary of Environments, Packages and Profiles batch process (R00921) to view the new user profiles.
7. Use Security Workbench (P00950) to apply application, action, and processing option security for roles and any individual overrides to those roles.
8. Create sign-in security records using the User Security application (P98OWSEC).

   You can create sign-in security records for all individuals within a role by entering one record for the role.
9. Manually populate the F00960 table.

   This table is automatically populated each time a machine signs in to JD Edwards EnterpriseOne. However, if you intend to use schedule packages, you must manually populate this table.
10. Create user overrides for roles.

    Normally, you will not create any overrides for individuals because they can easily create their own as they use the software.

Prerequisites

Before you complete the tasks in this section:

- Create all of the role profile information by using the User Profile Revisions application.

- Define:
  - Role profiles.
  - Environments that each role can access.

Forms Used to Set Up User Profiles

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

Setting Processing Options for User Profile Revisions (P0092)

Access the Processing Options form. Select the A/B Validation tab.

1. Enter 1 to enable Address Book validation.

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

2. Enter 0 (or leave blank) to disable Address Book validation.

   When disabled, this processing option allows you to create user profiles for Address Book entries that do not yet exist in the F0101 table.

Creating and Modifying User Profiles

Access the User Profiles Revision form.

User ID The code that identifies a user profile.

WhosWhoLineID A value that references the Who's Who Line ID in Address Book.

Menu Identification The menu name, which can include up to nine characters. JD Edwards EnterpriseOne standards are:

- Menu numbers are preceded with a *G* prefix.
- The two characters following the prefix are the system code.
- The next characters further identify the menu.
- The fourth character specifies a skill level.
- The fifth character distinguishes two menus of the same system with the same skill level.

For example, the menu identification G0911 specifies:

- 09 is the system code.
- 1 is the display level or skill level.
- 1 indicates that this is the first menu.

Default Icon File The path field contains the path used for client based menus. The path describes where the application is located on the computer or network. A path includes the drive, folders, and subfolders that contain the application to be executed.

Language A user defined code (01/LP) that specifies the language to use on forms and printed reports. Before you specify a language, a code for that language must exist at either the system level or in the user preferences.

Date Format The format of a date as it is stored in the database.

These date formats are valid: YMD, MDY, DMY, EMD. If you leave this field blank, the system displays dates based on the settings of the operating system on the workstation. With NT, the Regional Settings in the Control Panel control the settings for the operating system of the workstation.

Date Separator Character The character to use when separating the month, day, and year of a given date. If you enter an asterisk, the system uses a blank for the date separator. If you leave the field blank, the system uses the system value for the date separator.

Decimal Format Character The number of positions to the right of the decimal that you want to use. If you leave this field blank, the system value is used as the default.

Localization Country Code A code that identifies a localization country. It is possible to attach specific county functionality that is triggered baed on this code using the country server methodology in the base product.

Universal Time A code that you use to associate a time zone with a user's profile. This code represent the user's preferred time zone, and it must be a value from the UDC table (H91/TZ).

Time Format A code that determines the user's preferred format for time-of-day. The user can choose from a 12- or 24-hour clock.

Daylight Savings Rule A code that specifies the daylight savings rule for a region or country.

See Creating Daylight Savings Rules in the *JD Edwards EnterpriseOne Security Administration Guide* for information on how to create a daylight savings rule.

Copying User Profiles

Access the Work With User/Role Profiles form.

1. Select a user profile, and do one of these:
   - To copy an entire profile (the display, environment, and deployment preferences), click Copy.

     The User Profile Revisions form appears. Because this action creates a new profile, the user profile that you create cannot already exist in JD Edwards EnterpriseOne.
   - To copy environment preferences, from the Row menu, select Copy Environment.

     The User Environment Revisions form appears. This action copies environment preferences from one user profile to another. The user profile that you copy to must already exist.
2. In the User/Role field, enter a user ID to copy the profile into and change any other information.
3. Click OK.

Assigning or Deleting Environments for User Profiles

Access the Work With User/Role Profiles form.

1. Click Find, and then select a user profile.
2. From the Row menu, select Environments.

   The User Environment Revisions form appears. This form displays the list of environments available for a particular user or role.
3. To add a new environment, in the last row, enter a number that specifies the order in which the environment is displayed in the Display Seq. field.
4. In the Environment field, click the search button to select an environment.
5. To delete an environment from the list, select the environment and click Delete.

Assigning Business Preferences to User Profiles

Access the Work With User/Role Profiles form.

1. Click Find.
2. Select a user profile, and then click Select.
3. On the User Profile Revisions form, from the Form menu, select Bus Preferences.
4. On the Business Preferences form, complete any of these fields and click OK:
   - Industry Code

     This field associates the user profile with a specific industry, such as manufacturing.
   - Business Partner Code

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

- Customer Code

  This field associates the user profile with a specific customer.

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

Creating Profiles by Using a Batch Process

Access the Work With Batch Versions - Available Versions form.

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

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

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

   After you complete the Data Selection form, the Processing Options form appears.
5. On the Processing Options form, enter:
   - One of these values for option 1:

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

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

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

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

     Complete these user profile fields for option 2:

     Fast Path

     Language

     Date Format

     Data Separator Character

     Data Format Character

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

Reviewing User and Profile Definitions

Access the Work With Batch Versions - Available Versions form.

1. Select a version and click Select.

   Default version XJDE0001 creates a report for all role profiles in the enterprise. 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 Roles

This section provides overviews of user roles, role-to-role relationships, the sign-in Role Chooser, the menu filtering Role Chooser, workstation initialization file parameters, and discusses how to:

- Create and modify roles.
- Migrate roles.
- Sequence roles.
- Add an environment to a role.
- Assign business preferences to a role.
- Set up a role relationship.
- Enable the Role Chooser.
- Create role-to-role relationships.
- Revise role relationships.
- Delegate roles.
- Add roles to a user.
- Add users to a role.
- Copy user roles.
- Add a language translation to a role.

Understanding User Roles

As part of the system setup, you must define the roles for users in the organization. Roles define the tasks that users see when they work in the JD Edwards EnterpriseOne Menu and determine what authority the users have in JD Edwards EnterpriseOne.

After you have defined a role, you can associate users with it and apply security to it to provide the appropriate level of access to JD Edwards EnterpriseOne functions. You can assign more than one user to a role, or you can assign more than one role to a user. To establish a role relationship, you use the Role Relationships application (P95921), which enables you to add, remove, or revise a role relationship for a user. Role relationships are revised by removing an assigned role or by changing the expiration date for an assigned role.

Assigning roles accomplishes these purposes:

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

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

- Users can have multiple roles.

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

- Administrators can set up security based on user roles.

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

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

This table summarizes the steps an administrator must perform to set up roles for users:

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

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

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

After you have created one or more role relationships for a user, you can revise the relationships. 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.

In addition, you might want to delegate one or more of the roles to another user if a particular user will be unavailable. When you delegate the role relationship records, you can copy existing records to another user. You cannot add role relationships to another user unless those roles are already assigned to you.

See Also

JD Edwards EnterpriseOne Tools 8.97 Solution Explorer Guide, "Using the Menu Design Mode," Applying Roles to a Task

Chapter 7, "Using Security Workbench," page 65

Understanding Role-to-Role Relationships

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

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

Understanding the Sign-In Role Chooser

When signing into JD Edwards EnterpriseOne, if enabled, users can use the Role Chooser to select a particular role from a list of valid roles. In the Role Chooser, users can either select a particular role or *ALL. You can limit the freedom that a user has to select roles by disabling the Role Chooser. With the Role Chooser disabled, the user must enter JD Edwards EnterpriseOne with *ALL.

At the JD Edwards EnterpriseOne sign-in form, the user enters a user ID and password. The user must then enter a valid environment and role before entering JD Edwards EnterpriseOne. User roles and assigned environments are dependent on each other. The user can select an environment, which then determines what roles appear in the Role Chooser; or the user can select a role, which determines the environments that appear in the Environment Chooser.

The option for enabling the Role Chooser is a global setting. When enabled, it applies to all users in the system.

This table summarizes the scenarios that can occur when the user encounters the Environment and Role fields at sign-in on the Microsoft Windows client, and the behavior of JD Edwards EnterpriseOne in each scenario:

Sign-in Scenario	JD Edwards EnterpriseOne Behavior
User enters values in both the Environment and Role fields.	The software validates the role against the environment. If the role is not valid for the chosen environment, the Environment Chooser appears and the user must choose a valid environment for the role.
User enters a value only in the Role field.	The Environment Chooser displays only the valid environments for the chosen role.

Sign-in Scenario	JD Edwards EnterpriseOne Behavior
User enters a value only the Environment field.	The Role Chooser displays only the valid roles for the user and the chosen environment.
User does not enter a value in either the Environment field or the Role field.	The Role Chooser appears, containing 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, which is defined in the jde.ini file.

Understanding the Menu Filtering Role Chooser

In P95921, you can select the "Choose role on Menu filtering page" option to give users the ability to filter menus by role in the EnterpriseOne Menu. When enabled, the JD Edwards EnterpriseOne web client displays the Role drop-down menu above the EnterpriseOne Menu. From the Role drop-down menu, users can select *ALL (All My Roles) to view a concatenated list of all the tasks enabled for every role that is included in the *ALL role. Alternatively, users can select a particular role from the Role drop-down menu and the system displays only the tasks enabled for that role in the EnterpriseOne Menu.

The "Choose role on Menu filtering page" option is a global setting. When enabled, it applies to all users in the system.

In order for users to filter menus by role:

- The system administrator must enable the "Choose role on Menu filtering page" option in P95921.
- Users must sign in using *ALL.

Note. If a user signs in to JD Edwards EnterpriseOne using a particular role instead of *ALL, then the system only displays the tasks in the EnterpriseOne Menu for that role; the user cannot select a different role in the EnterpriseOne Menu.

See Also

Chapter 3, "Working with User and Role Profiles," Enabling the Role Chooser, page 27

Chapter 3, "Working with User and Role Profiles," Understanding User Roles, page 16

Understanding Workstation Initialization File Parameters

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

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

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

Forms Used to Set Up Roles

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

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

Creating and Modifying Roles

Access the Work With User/Role Profiles form.

1. Perform one of these operations:
   - To create a new role, select Add Role from the Form menu.
   - To modify an existing profile, click the Roles Only option; click Find and select a role in the detail area; and then click Select.

   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, enter the name of the role, such as ACCOUNTING, and a description in the Role field.

   When you modify a role profile, this field displays the name of the role.

3. In the Sequence Number field, 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.

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

Migrating Roles

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

Run the TC R89959211

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

This TC has no processing options.

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

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

Run the TC R8995921

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

The recommended processing option values are:

- Final/Proof Modes

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

- Effective Date

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

- Expiration Date

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

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

- Included In All

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

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

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

Sequence the Roles

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

Add Environments

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

Set up the JDE.INI/JAS.INI file

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

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

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

Server Executables

Run a PortTest.

Set Up Security

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

Run the UBE R98OWPU

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

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

This UBE has no processing options.

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

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

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

Run the UBE R98OWUP (Optional)

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

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

Set these procession options:

- Proof or Final

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

- Password Change Frequency

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

- Allowed Attempts

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

- Enable/Disable User

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

- Daily Password Change Limit

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

- Force Immediate Password Change

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

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

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

Sequencing Roles

The Work With Role Sequences form contains all of the roles that you defined and enables you to assign a sequence to the roles. The sequence defines a hierarchy of roles and determines which role is used when a security conflict exists among roles when a user signs in as *ALL.

The Windows client and Web client differ as to how they use the role sequence to determine which security record is applied. The Web client only checks the first role in the role sequence to determine the security for an application, form, column, row, and so forth. The Windows client checks all the roles in *ALL for security, but uses the role sequence to determine which role to use when there are duplicate security records.

This is an example of duplicate security records in which the JD Edwards EnterpriseOne Windows client is forced to use the role hierarchy to determine which security record to apply:

A user signs in as *ALL. The *ALL has two roles associated with it—Role 1 and Role 2.

- Role 1 = Form A is secured; no access allowed.
- Role 2 = Form A is not secured; access allowed.

Because of the conflict in security between these two roles, JD Edwards EnterpriseOne uses the information in the role sequence to determine which role to use for security. If Role 1 was higher in the sequence, then the security for that role is applied.

In this same example, if each of these roles had different security records for the same security type, the system would apply the security as defined by both records. For example, if Role 1 does not allow users to view column A and Role 2 does not allow users to view column B, the user would not be able to view either column on the form.

You can configure the JD Edwards EnterpriseOne Web client to use the same role sequencing functionality as the Windows client. This is recommended if you are migrating from the Windows client to the Web client. To enable this functionality in the Web client, use Server Manager to configure the following setting in the [OWWEB] section of the JAS.INI:

Setting	Value
useRoleHierarchy=	true

Access the Work With Role Sequences form.

1. Select a role from the tree structure and drag it to the point in the sequence that you want.

   Note. The system checks the sequence of roles in descending order.

2. After you have set the order that you want, select Set Sequences from the Form menu and click Close.

3. If you decide you do not want to change the sequence, select Close Without Set from the Form menu and click Close.

Adding an Environment to a Role

Use the Work With User/Role Profiles form to assign one or more environments to a role or to change an existing environment for a role. When a user signs in to JD Edwards EnterpriseOne, the Environment Chooser and Role Chooser present each user with a list of valid roles and environments.

Access the Work With User/Role Profiles form.

1. Select the Roles Only option and click Find.

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

2. Select a role from the detail area of the grid, and select Environments from the Row menu.
3. On the User Environment Revisions form, in the Display Seq. (display sequence) column, specify the order in which the environments will be presented in the Environment Chooser at JD Edwards EnterpriseOne sign-in.
4. In the Environment column, click the search button to select an environment, and then click OK:

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

Assigning Business Preferences to a Role

Access the Work With User/Role Profiles form.

1. Click Find.
2. Select a role, and then click Select.
3. On the Role Revisions form, from the Form menu, select Bus Preferences.
4. On the Business Preferences form, click the search button in the Industry Code field to associate the role with a specific industry, such as manufacturing.
5. In the Business Partner Code field, click the search button to associate the role with a specific business partner.
6. In the Customer Code field, click the search button to associate the role with a specific customer.

Setting Up a Role Relationship

Access the Work With Role Relationships form.

1. Complete the User field and click Find.

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

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

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

4. Enter an expiration date in the Expiration Date field, if one is needed.

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

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

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

Enabling the Role Chooser

Access the Work With Role Relationships form.

1. From the Form menu, select Enable Role Chooser.
2. To enable users to select a role from a list of assigned roles at sign-in, on the Enable/Disable Role Chooser form, select the "Choose role on Login page" option.

   If you do not select this option, users must enter JD Edwards EnterpriseOne using *ALL.

3. To enable users to filter menus by role in the EnterpriseOne Menu, select the "Choose role on Menu Filtering page" option.

Note. Both the Role Chooser and Menu Filtering Role Chooser options are global settings. When enabled, they apply to all users in the system.

Creating Role-to-Role Relationships

Access the Work With Role Relationships form.

1. From the Form menu, select Distribution Lists.
2. On the Work With Distribution Lists form, complete the Role field and click Find.
3. To add a role to the distribution list, select a role from the Available Roles tree control and click the left-arrow button.
4. On Role Revisions, complete these fields and click OK:
   - Effective date

     Enter an effective date if you want the delegation to occur at a date other than the current date.
   - Expiration date
   - Include in *All

     Select this option if you want the role to be one that the user can use if the user enters JD Edwards EnterpriseOne playing all roles.
5. Select the *ALL option if you want the role to be one that the user can play if the user enters JD Edwards EnterpriseOne playing all roles.

   JD Edwards EnterpriseOne adds the role to the Assigned Roles tree control.
6. To remove a role from the distribution list, select a role from the Assigned Roles tree control and click the right-arrow button.

Note. JD Edwards EnterpriseOne does not currently support multilevel roles.

Delegating Roles

Access the Work With Role Relationships form.

1. From the Form menu, select Roles Delegation.
2. On the Work With Delegation Relationships form, complete the Delegate field by entering the user ID of the user being delegated to and click Find.

   The roles of the user who is delegating appear in the Available Roles tree control. The roles of the user who is being delegated to appear in the Assigned Roles tree control.
3. To delegate a role, select the role from the Available Roles tree control and click the left-arrow button.
4. Complete these fields and click OK:
   - Effective date

     Enter an effective date if you want the delegation to occur at a date other than the current date.
   - Expiration date
5. Select the *ALL option if you want the role to be one that the user can play if the user enters JD Edwards EnterpriseOne playing all roles.

   JD Edwards EnterpriseOne adds the delegated role to the Assigned Roles tree control on the Work With Delegation Relationships form.

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

Adding Roles to a User

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

Access the Work With Role Relationships form.

1. From the Form menu, select Add Roles to User.
2. Complete the User ID field and click Find.
3. Select the roles that you want to add to the user and click Select.

   Hold down the Control key to select more than one role to add.
4. On the Role Revisions form, complete these fields:
   - Effective Date

     Enter a date if you want the effective date to be different from the current date.
   - Expiration Date
   - Include in *All
5. Select the *ALL option if you want the role to be one that the user can play if the user enters JD Edwards EnterpriseOne playing all roles.

6. Click OK.
7. If you are adding more than one role relationship record, complete the Role Revisions form for each record that you are adding.

Adding Users to a Role

Access the Work With Role Relationships form.

1. Select Add Users to Roles from the Form menu.
2. Complete the Role field and click Find.
3. Select the users that you want to add to a role and click Select.

   Hold down the Control key to select more than one user to add.
4. In the Role Revisions form, complete these fields:
   - Effective Date

     Enter a date if you want the effective date to be different from the current date.
   - Expiration Date
   - Include in *All
5. Select the *ALL option if you want the role to be one that the user can play if the user enters JD Edwards EnterpriseOne playing all roles.
6. Click OK.
7. If you are adding more than user record, complete the Role Revisions form for each record you are adding.

Copying User Roles

You can copy the role relationship records of one user to another from Role Relationships (P95921). You can either copy and add the records, which means that JD Edwards EnterpriseOne adds the copied records to the user's existing records; or you can copy and replace the records, which means that the copied records replace the user's existing records.

Access the Work With Role Relationships form.

1. Complete the User field and click Find.

   The user's roles appear in the Assigned Roles tree control.
2. Click Copy.
3. On the Copy User Roles form, select one of these options:
   - Copy and Add
   - Copy and Replace
4. Complete the To User field to specify the user to whom you want the records copied.
5. Click OK.

Adding a Language Translation to a Role

Using the Language Role Description Revisions form, you can either set up the translation of any role that you have defined, or you can change role descriptions for any language.

If you want to view the descriptions of any role in all the languages into which it is being translated, use the Work With Language Role Description form.

Access the Work With User/Role Profiles form.

1. Select the Roles Only option.

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

2. Select a role from the detail area of the grid and select Role Description from the Row menu.
3. To add a language to a role, click Add.
4. On the Language Role Description Revisions form, in the Role field, enter the name of the role to which you want to add a language.
5. In the Language field, click the search button to select a language from the list of supported languages.
6. Enter a description of the role in the Role Description field, and then click OK.

CHAPTER 4

Employing Sign-in Security

This chapter provides an overview of sign-in security and discusses how to set up processing options for the User Security program (P98OWSEC):

- Security table access.
- Password encryption.
- Security setup.
- Process flow for sign-in security.
- Sign-in security for web users.

Understanding Sign-in Security

This section discusses:

- Sign-in security overview.
- Security table access.
- Password encryption.
- Sign-in security setup.
- Process flow for sign-in security.
- Sign-in security for web users.

Sign-In Security Overview

JD Edwards EnterpriseOne security runs on a logic server in a dedicated internal process. You create a security table on the data server that stores information, such as:

Value	Description
EnterpriseOne User	The user ID used to sign in to JD Edwards EnterpriseOne.
EnterpriseOne Password	The user's password, which the software validates when the user signs in to JD Edwards EnterpriseOne.
System User and System Password	The actual user and password used to connect to all database management systems (DBMS). If the JD Edwards EnterpriseOne environment includes more than one DBMS, you can create different system users and passwords for each data source.

Value	Description
Change Frequency	The frequency of password changes required by the software.
Last Change	The date that the password was last changed.

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

You can also set up unified logon with JD Edwards EnterpriseOne to simplify sign-in security. When you set up unified logon, JD Edwards EnterpriseOne uses Windows Authentication to verify security. This verification enables sign-in security to use the network logon information that a user supplies when logging on to Windows; JD Edwards EnterpriseOne does not require the user to enter another user ID and password when signing in.

See Chapter 5, "Setting Up User Security," Managing Unified Logon, page 58.

Security Table Access

If you keep the system user and password secure, no users have direct access to the Security table (F98OWSEC). The exception to this situation is for system administrators who maintain the security information. The JD Edwards EnterpriseOne security server has access to the F980WSEC table through JDENet.

You must perform all of the validation and changes of JD Edwards EnterpriseOne passwords through a JDENet message to the enterprise server that has the F980WSEC table. Upon validating a JD Edwards EnterpriseOne password, the JDENet message returns the system user and password that you enter. These words are encrypted across the network. Internally, this system password is used for all connections to databases.

Using the database management system, you should place database security on the F980WSEC table. You should also assign JD Edwards EnterpriseOne object security to the F980WSEC table so that users cannot access the object except to enter User Password Revisions.

See Also

Chapter 5, "Setting Up User Security," page 43

Password Encryption

You can enter the initial sign-in password for each user in these ways:

- Type it manually.
- Use a default password established through the sign-in security processing options.
- Have JD Edwards EnterpriseOne enter it automatically because the user has an existing security record.

When typing a password manually or when using the processing option default password, you cannot see the password for a new user because you are typing it in. When you revise this record, however, the system encrypts the password so that all you see are asterisks. The number of asterisks does not represent the number of characters in the password. The user security application does not know what the password is. The application is given a flag that indicates that a password was entered. The system stores the actual password on the security server within a binary object in the F980WSEC table. The system accesses the binary object when the user security application requests a change or inquiry.

Sign-In Security Setup

This checklist is an overview of the steps that are required to set up sign-in security:

Determine location of the F98OWSEC table.	Ensure that the F98OWSEC table is located in the system data source on the enterprise server, and ensure that the table is mapped to the correct data source through the Object Configuration Manager. If your system data source resides on the enterprise server, the F980WSEC table should reside in the system data source. However, if the system data source is located on the deployment server (or other servers), the F980WSEC table should be moved to the server map data source for the enterprise server. If you have more than one logic server, you should use only one as the security server.
Set database security on the F98OWSEC table.	From within the DBMS, place database security on this table to prevent a user from accessing the object, except to enter passwords through User Password Revisions.
Place security on the logic server's jde.ini file.	The DBMS user ID and password to the Sign On Security table are stored in this file. ***Warning!*** Implementing jde.ini file security will prevent Server Manager from modifying configuration settings.
Create security records for individual users.	Assign these: • Data source • System user • System password • EnterpriseOne 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 JD Edwards EnterpriseOne security database requires a unique user ID.
Verify and modify the jde.ini file on the JD Edwards EnterpriseOne logic server for the platform environment.	If you use a unified logon, you need to change the settings for a unified logon in the [SECURITY] section as well as in the JD Edwards EnterpriseOne [SECURITY] settings.

Set up a unified logon server.	If you use a unified logon with the JD Edwards EnterpriseOne security, set up a unified logon server for each instance of JD Edwards EnterpriseOne on each server. For example, if you have an NT server with multiple releases of JD Edwards EnterpriseOne, you need a unified logon server for each release on the server. The unified logon server differentiates instances of JD Edwards EnterpriseOne based on the port numbers for these instances. For example, if the port number for JD Edwards EnterpriseOne is 6104, the port number for the associated unified logon server is 6104. Other instances and unified logon servers use different port numbers.
Verify and modify jde.ini file.	Verify and modify the jde.ini file that will be deployed to the server's workstation installations.
Set up sign-in security.	Require sign-in security for all machines.

Process Flow for Sign-in Security

JD Edwards EnterpriseOne provides sign-in security with an architecture that is designed to provide user security for JD Edwards EnterpriseOne and the logically attached database management systems. The security architecture prevents you from viewing the database or system password and from bypassing JD Edwards EnterpriseOne applications to view and change data.

This text explains the process flow for standard sign-in security:

- Workstations sign in to JD Edwards EnterpriseOne by using their user ID and password.

  These workstations can be networked or standalone workstations, laptop computers, or other JD Edwards EnterpriseOne hosts.

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

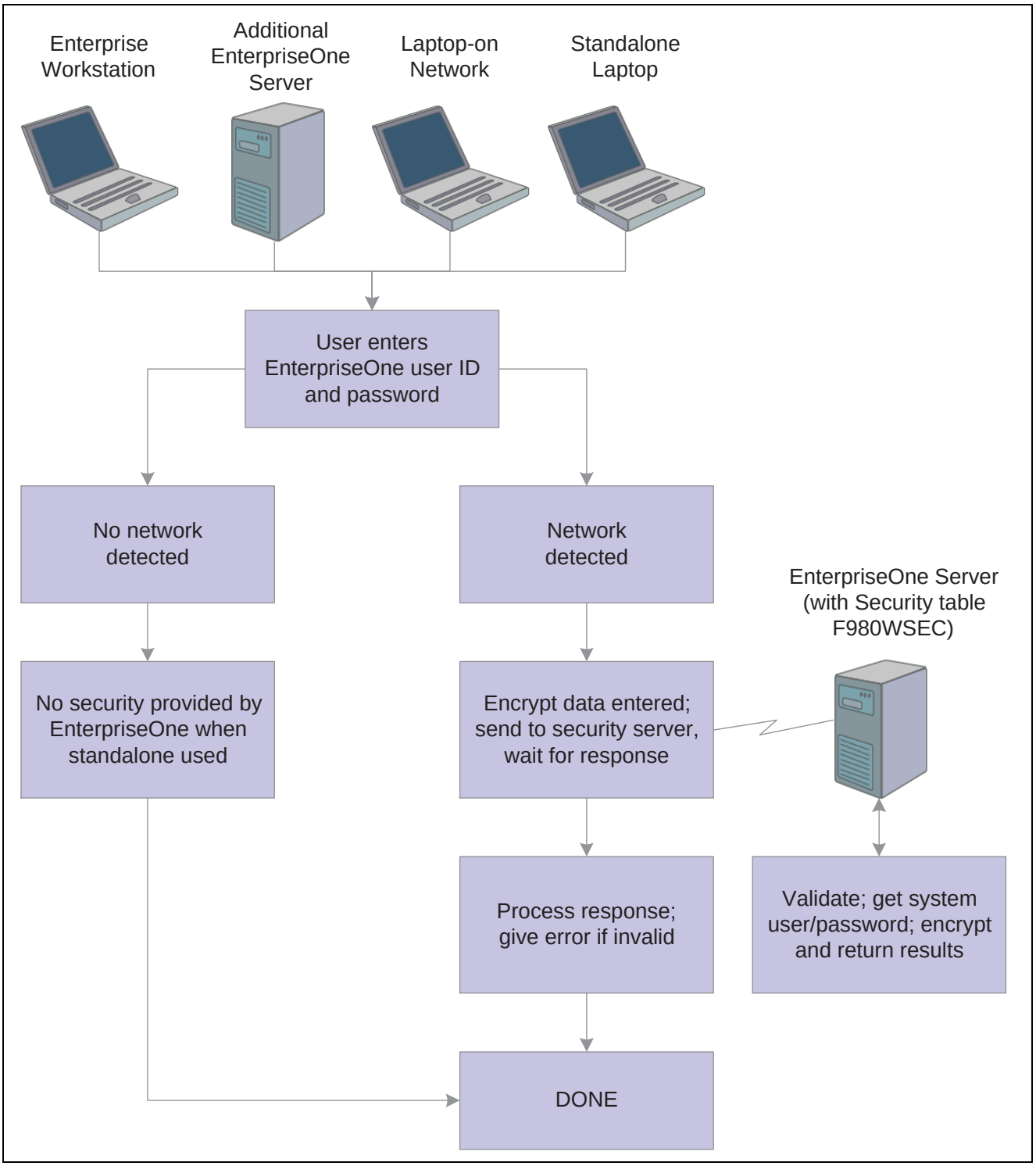
- As the software starts, it tries to detect an operational network environment.

  If a network is not detected, the software allows local operation in a store-and-forward mode. Because the workstation or laptop computer is not connected to a network or an enterprise server, no validation can be performed against the F980WSEC table. Therefore, security is limited to that provided by the local workstation or laptop installation.

  If a network is detected, the software encrypts the password information and sends it over the network to the JD Edwards EnterpriseOne enterprise server.

  The enterprise server checks the incoming validation request against a table of valid users and passwords. If the user ID and password information are valid, the software accepts the sign-in values and returns the system ID and password to the logically attached database servers. This information is also encrypted on the enterprise server prior to broadcast on the network.

This graphic displays a process flow model for standard sign-in security:



Process flow model for standard JD Edwards EnterpriseOne sign-in security

The process flow for sign-in security with a unified logon is as follows:

- A user starts up JD Edwards EnterpriseOne on a workstation.
- JD Edwards EnterpriseOne verifies that the unified logon is active and then sends an authentication request to the unified logon server, based on the domain user ID.

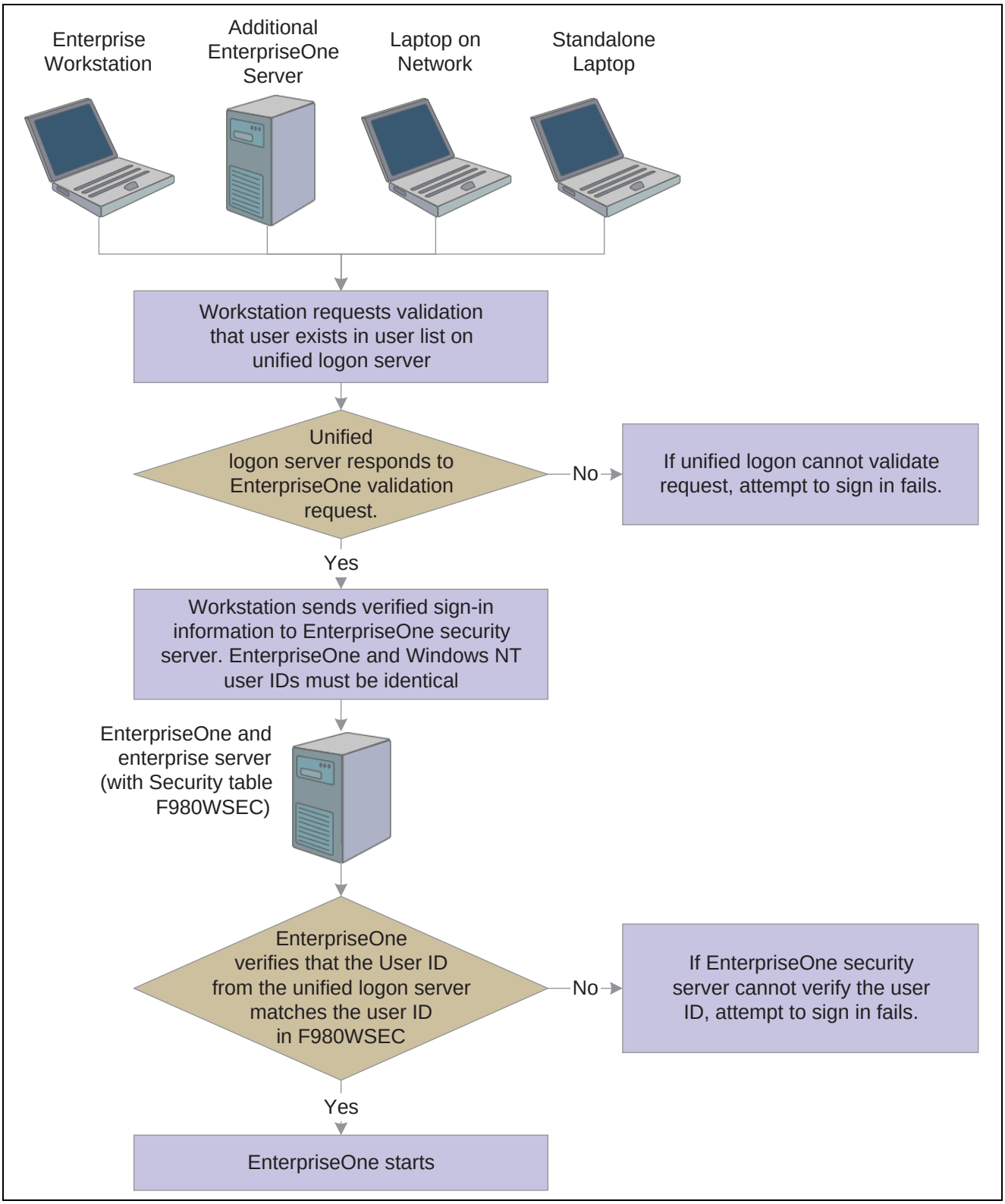
Note. The unified logon server is not a physical server. It is a device that verifies sign-in security against the domain sign-in security maintained by Microsoft Windows.

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

- The unified logon server searches its user list for an entry that matches the domain user ID. When the server finds a match, the server sends a validation request to the enterprise server.
- The enterprise server verifies that the response from the unified logon server matches the security information in the F980WSEC table.
- If the security information from the user list on the unified logon server matches the security information in the F98OWSEC table on the enterprise server, the start-up process continues.
- The first time that a user signs in to JD Edwards EnterpriseOne with the unified logon, the Environment Selection appears.

  The user must enter an environment in the Environment field. Select the option to set the environment as the default, and avoid the Environment Selection form on subsequent sign-in attempts.

This illustration displays the process flow for unified logon:



Unified logon process flow

ShowUnifiedLogon Setting

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

Value	Description
0	A value of 0 for ShowUnifiedLogon disables the Environment Selection form. When you click the option on the Environment Selection form to set a default environment, you set this value to 0.
1	A value of 1 for ShowUnifiedLogon enables the Environment Selection form. When a user signs in to JD Edwards EnterpriseOne, the Environment Selection form appears and allows the user to choose an environment. This setting is the default for ShowUnifiedLogon.

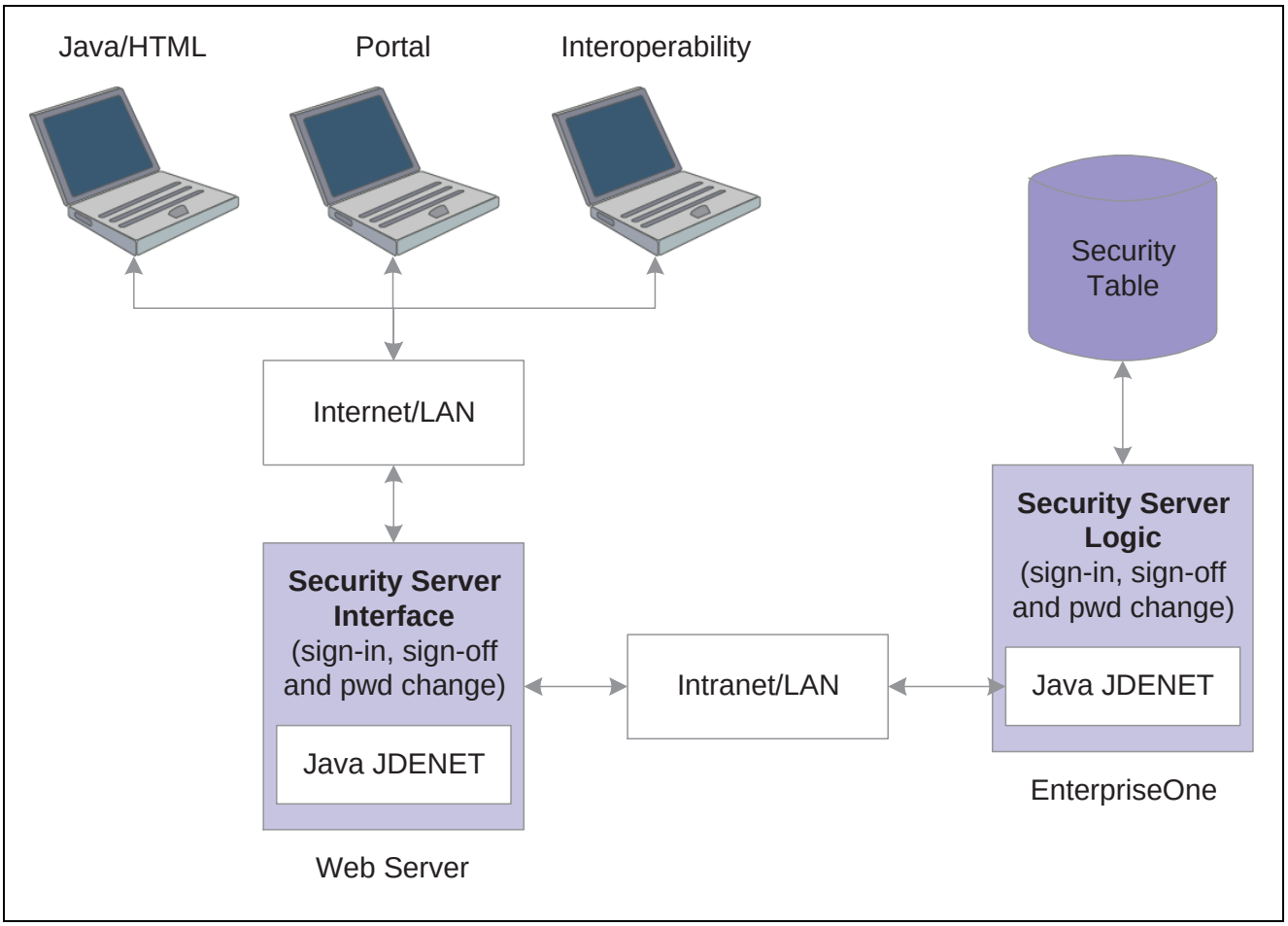
Sign-in Security for Web Users

The JD Edwards EnterpriseOne security server and the F98OWSEC table authenticate Java/HTML, Portal, and Interoperability users who sign in to JD Edwards EnterpriseOne across the internet to the JAS security server. The JAS security server acts as an interface between the web user's client workstation and the security server.

When web users sign in, disconnect, or make a password change, the JAS server sends the request using a JDENET message to the security server, which, in turn, accesses the F98OWSEC table. The security server then returns the authentication through a JDENET message to the JAS security server. If the user is authenticated, the security info is cached to the JAS security server.

The JAS security server acts as an intermediary between the Java/HTML, Portal, and Interoperability client and the security server.

This graphic displays a process flow for sign-in security with unified logon for web users:



Sign-in security with unified logon for web users

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

- Connecting to the JD Edwards EnterpriseOne security server for user security authentication and password when a web user signs in.
- Switching to a secondary JD Edwards EnterpriseOne security server when the primary server is down, provided the correct jas.ini settings are defined.
- Notifying Java/HTML, Portal, and Interoperability client workstations when a user password has expired.

  If an Interoperability user's password has expired, sign-in fails without notification of the cause.
- Sending error message to user log after the web user has attempted unsuccessfully to sign in *x* number of times to JD Edwards EnterpriseOne, where *x* is the number of sign-in attempts defined in the F98OWSEC table.
- Allowing Java/HTML and Portal users to change name and password.
- Encrypting JDENET messages sent between the JAS security server and the JD Edwards EnterpriseOne security server.
- Keeping a valid user session open until the user signs off or the session expires.

To the web user, sign-in and sign-out function the same as they do to a user on Windows, UNIX, or iSeries platforms.

To set up security for web users through the JD Edwards EnterpriseOne security server, add these parameters to those that already exist in the jas.ini file:

[SECURITY] Parameter in jas.ini File	Parameter Value
NumServers	Total number of JD Edwards EnterpriseOne security servers that are available to web users signing on to the system. If this parameter is missing, the default value is 1 and the primary security server handles the sign-in.
SecurityServer	Name of the primary security server.
SecurityServerN	Name of the secondary security server. The value of N is 1 for the first secondary server, 2 for the second, and so on. Assign values to this parameter if you want sign-in to switch to a secondary server if users cannot sign in to the primary server.
UserLogonCookie=	If the value is TRUE, the user can save signon information (username, password, and environment) in an encrypted cookie on the workstation and does not have to type the information in for subsequent sign-ins. If the value is FALSE, the feature is disabled.
#CookieLifeTime unit	Unit of time used to measure a cookie's lifetime. For example, the parameter value day means that the cookie's lifetime is measured in days.
Cookie LifeTime	Amount of time before a cookie expires. The unit of measure is defined by the #CookieLifeTime unit parameter value. If that value is day and the value of the Cookie LifeTime parameter is 7, the cookie expires in seven days.

If you define one primary server and two secondary servers, the jas.ini file [SECURITY] settings look like this example:

```
NumServers=3
SecurityServer=JDED
SecurityServer1=JDEC
SecurityServer2=corowhp2
UserLogonCookie=TRUE
#CookieLifeTime unit is day
CookieLifeTime=7
```

If you define one or more secondary servers, sign-in fails over to the secondary server if the primary server is down. If both the primary JD Edwards EnterpriseOne security server and a secondary server as defined in the jas.ini file fail, the JAS server fails the user sign-in.

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

```
[SECURITY]
SecurityServer=JDED
UseLogonCookie=TRUE
CookieLifeTime unit is day
CookieLifeTime=7
```


Setting Processing Options for P98OWSEC

The User Security program (P98OWSEC) has processing options that you can use to set a default password when creating user security for users or roles, and to set a default change frequency for the password:

Default

Although processing options are set up during JD Edwards EnterpriseOne implementation, you can change processing options each time that you run a program.

1. Enter a '1' to default the User ID into the password field.

2. Enter in the default Change Frequency.

3. Enter the number of sign-on attempts a user is given prior to being disabled.

4. Enter if a new user is to default to as enabled or disabled.

5. Enter a '1' to force immediate password change of new users.

Password

Although processing options are set up during JD Edwards EnterpriseOne implementation, you can change processing options each time you run a program.

1. Enter the daily password change limit that will be applied to all users when attempting to change a password.	If this field is 0 or is left blank, there will be no limit on daily password changes.
2. Enter the minimum password length that is to be used when users attempt to change a password.	If this field is 0 or is left blank, the password will not be checked for a minimum length.
3. Enter the minimum number of character that must be used within a password.	If this field is 0 or is left blank, the password will not be checked for characters.
4. Enter the minimum number of numerics that must be used within a password.	If this field is 0 or is left blank, the password will not be checked for numerics.

5. Enter the maximum number of consecutive characters that can be used in a password.	If this field is 0 or is left blank, the password will not be checked for consecutive characters.
6. Enter the minimum number of special characters that must be within a password.	If this field is 0 or is left blank, the password will not be checked for special characters.

CHAPTER 5

Setting Up User Security

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

- Create and revise user security.
- Review security history.
- Manage data sources for user security.
- Enable and synchronize security settings.
- Run a Security Analyzer report.
- Manage unified logon.

Understanding User Security

Use the User Security application (P98OWSEC) to create, test, and change user security for JD Edwards EnterpriseOne and the logically attached database management systems. The security architecture prevents you from viewing the database or system password and from bypassing JD Edwards EnterpriseOne applications to view and change data. JD Edwards EnterpriseOne uses an encryption algorithm to ensure that applications other than JD Edwards EnterpriseOne security cannot access passwords transmitted across the network.

You can also set up a unified logon server for a JD Edwards EnterpriseOne server. The unified logon server enables JD Edwards EnterpriseOne to use the domain logon information to determine user security. In a JD Edwards EnterpriseOne unified logon scenario, a user needs to enter a user ID and a password only at network logon.

Creating and Revising User Security

This section provides an overview of user security, lists prerequisites, and discusses how to:

- Create user security.
- Copy user security.
- Revise user and role security.
- Revise all user security.
- Change a sign-in password.
- Require sign-in security.

Understanding How to Create and Revise User Security

A user profile must already exist for a user before you can create user security records for that user. You can create security records one at a time for each of the users, you can set security for a role, or you can set security for all users.

The P98OWSEC application provides a copy function to simplify the creation of security records for individual users. Typically, users within a specific role use similar security information. We recommend that you create a model user with security information that you can copy to create other users because

---

Note. When you copy security records to a user, security records must not already exist for that user. If you try to copy user security to a user with existing user security records, you will receive an error message.

You should keep user security simple. Managing JD Edwards EnterpriseOne user IDs and system (database) user IDs can become complicated quickly. The simplest way to set up user security is to have all data sources share the same system user ID and password by leaving the data source field blank when you initially create user security records for users or roles on the Security Revisions form.

When you leave the data source field blank, the P98OWSEC application automatically enters *DEFAULT* in the field. The DEFAULT data source enables you to create one security record for all users. Each time a user accesses a table through a JD Edwards EnterpriseOne application, the software searches for a security record for that user and the specific data source where the table resides. If the software does not find a specific record, then it uses the default data source, which is the security record that you created with the DEFAULT data source field.

You use system user IDs to manage user access to databases. Although you should try to maintain as few system user IDs as you can, occasions arise that require you to set up database security in addition to the JD Edwards EnterpriseOne object and user security for specific users and specific tables. For example, you might need to create system users with additional authority to what the typical system user needs.

See Also

JD Edwards EnterpriseOne Tools 8.97 Configurable Network Computing Implementation Guide, "Setting Up Data Sources"

Prerequisites

Before you complete the tasks in this section:

- Set up all user records in the Address Book application (P01012).
- Create user profiles using the User Profile application (P0092).

  See Chapter 3, "Working with User and Role Profiles," page 7.
- Attach the proper Address Book record to the user or role profile.
- Review and set the appropriate processing options before using the P98OWSEC application for the first time.

  See Chapter 3, "Working with User and Role Profiles," Setting Processing Options for User Profile Revisions (P0092), page 12.

Forms Used to Create and Revise User Security

Form Name	FormID	Navigation	Usage
Work With User Security	W98OWSECE	Security Maintenance (GH9052), User Security (P98OWSEC)	Access forms to work with user security.
Security Revisions	W98OWSECB	On the Work With User Security form, click Add.	Create user security.
Copy User Records	W98OWSECN	On the Work With User Security form, select the user or role and click Copy to copy all security records. To copy a single user security record, select the security record from the detail area, and select Copy Record from the Row menu.	Copy user security.
Security Detail Revisions	W98OWSECI	On the Work With User Security form, select the appropriate record, and then select Revise Security from the Row menu.	Revise user and role security.
Administration Password Revisions	W98OWSECF	Security Maintenance menu (GH9052), Administrative Password Revisions (P98OWSEC)	Change a sign-in password.
Sign On Security - Required/Not Required	W98OWSECG	On the Work With User Security form, select Req / Not Req from the Form menu.	Require all machines to use JD Edwards EnterpriseOne sign-in security.

Creating User Security

Access the Work with User Security form.

1. Click Add.

   Note. Do not use the GlobalPasswordPolic option in the Form menu. This form contains password settings that only apply to users who are using the User Profile Self-Service application (P0092SS).

2. On the Security Revisions form, complete one of these fields:

   - User ID

     If you enter a user ID that already exists, you can modify data source information for the user. The system disables all other fields and options for the user ID.

- Role

  If you enter a role that already exists, you will overwrite the security record for role when you enter information on the form.

Note. When you type information in one of these fields, the system disables the other field. For example, if you type *ROLE1* in the User Class/Role field, the User ID field becomes unavailable for data entry.

---

3. Complete these fields:

   - Data Source

     If you leave this field blank, you will set security for all data sources. *DEFAULT* appears in the Data Source field when you tab out of the field.

   - System User
   - Password

     We recommend you complete at least the System User field.

     If you create records by role or for all users at one time, the Password field is populated according to the processing option that you select.

4. In the User Status area, select one of these options:

   - Enabled

     With User Status enabled, security allows the user to sign in. This option is the default setting when you create user security.

   - Disabled

     With User Status disabled, security prohibits the user from signing in to the software.

Note. If a user commits a security violation, such as exceeding the maximum number of allowed password attempts, the software automatically sets the value for User Status to *Disabled.* The system administrator must access the user security record for the user and set User Status to *Enabled* before the user can sign in. In addition, the system administrator can access Administrative Password Revisions to reset the password of the user, which also restores a user profile to the status of enabled.

---

5. If you want to set limits on the passwords for users, complete these fields:

   - Allowed Password Attempts

     Enter the number of invalid password attempts allowed before the system disables access for the user.

   - Password Change Frequency

     Enter the number of days until the system requires the user to change the password.

   - Daily Password Change Limit

     Enter the allowed number of times a user can change a password in a day.

   - Force Immediate Password Change

     Click this option to require the user to change the password on the next sign-in.

6. Click OK to save the current user security information.

Copying User Security

A user profile must already exist for a user before you can create user security records for that user. In addition, when you copy security records to a user, security records must not already exist for that user. If you try to copy user security to a user with existing user security records, you will receive an error message.

Note. You should create a model user with security information that you can copy to create other users. Typically, users within a specific role use similar security information.

Access the Work With User Security form.

To copy user security:

1. On the Work With User Security form, find the user, and then perform one of these actions:
   - To copy all user security records for a user or role, select the user or role in the tree structure, and click Copy.
   - To copy a single user security record for a user or role, select the security record row in the detail area, and select Copy Record from the Row menu.
2. On the Copy User Records form, enter a valid user ID in the To User / Role field and click OK.

Revising User and Role Security

Access the Work With User Security form.

1. On the Work With User Security form, complete the User ID / Role field.
2. Click Find.
3. Select the appropriate record in the tree structure, and then select Revise Security from the Row menu.
4. On the Security Detail Revisions form, complete these fields, as necessary:
   - User Status

     Under User Status, you can enable or disable a user profile.
   - Password Change Frequency
   - Allowed Password Attempts

   Note. For a role, select the appropriate option from the Change box to enable each field.
5. Click OK.

Revising All User Security

Access the Work With User Security form.

1. From the Form menu, select Revise All.
2. On the Security Detail Revisions form, in the Change box, select any of these options to enable the related field:
   - User Status
   - Frequency
   - Attempts

- Change Limit

3. Complete any of these fields, and then click OK:
   - User Status

     This field enables you to enable or disable user profiles.
   - Password Change Frequency
   - Allowed Password Attempts
   - Force Immediate Password Change

     This field requires the user to change the password on the next sign-in.

Changing a Sign-in Password

Access the Administration Password Revisions form.

Note. You can also access Administrative Password Revisions from the User Security application. On the Work with User Security form, find the user, select the user in the tree structure, and then select Password Revisions from the Row menu.

User ID	Enter the user ID that you want to force a password change during sign-in. The user ID is the default value in this field when the user record is highlighted and Password Revision is activated.
New Password	Enter a new password. On this form, the system does not restrict the password choices. Any password is valid.
New Password - Verify	Enter the password again to verify it.
Force Immediate Password Change	Select this option to force the user to change the password during the next sign-in.

Requiring Sign-in Security

Use this feature to require all machines to use JD Edwards EnterpriseOne sign-in security. This procedure enables mandatory security only for the environment that you are signed into when you make this change.

Access the Work With User Security form.

1. Select Req / Not Req from the Form menu.
2. On the Sign On Security - Required/Not Required form, click the lock icon to change the Security Server to *Required* or *Not Required.*

   Note. If you set up the security as *Not Required* and have security turned on through the jde.ini file on the enterprise server, users that comment out signon security in their jde.ini files will still not be able to access any data sources without knowing the system user ID and password.

   When attempting to access a table in a secured data source, users will receive a database password entry form. If system user IDs and passwords are confidential, no one will be able to access the secured tables.

Reviewing Security History

This section lists the prerequisite and the forms used to review security history.

If you know the specific user or role, you can review the user's or role's security history by using the JD Edwards EnterpriseOne Security application. You can also search for specific information for all users. For example, to see the users who were deleted on a given day, you can search on event type 06 *(Delete User)* and a specific event date.

Prerequisite

The [SECURITY] section in the server jde.ini must include the`History=1` setting for the system to record security history.

Forms Used to Review Security History

Form Name	FormID	Navigation	Usage
Work With User Security	W98OWSECE	Security Maintenance (GH9052), User Security (P98OWSEC)	Access forms to review security history.
Work With Security History	W98OWSECC	On the Work With User Security form, from the Form menu, select Security History.	Click Find to review the security history records.

Managing Data Sources for User Security

This section provides an overview of data source management for user security and discusses how to:

- Add a data source to a user, a role, or all users.
- Revise a data source for a user, a role, or all users.
- Remove a data source from a user, a role, or all users.
- Change the system user password for multiple users.

Understanding Data Source Management for User Security

You add data sources to user and role records in user security to authorize users and roles to access JD Edwards EnterpriseOne databases. You can also revise the system user and password for existing data sources.

Forms Used to Manage Data Sources for User Security

Form Name	FormID	Navigation	Usage
Work With User Security	W98OWSECE	Security Maintenance (GH9052), User Security (P98OWSEC)	Access forms to set up user security.
Add Data Source	W98OWSECS	On the Work With User Security form, from the Form menu, select Add Data Source.	Add a data source to a user, role, or all users.
Data Source Revisions	W98OWSECH	On the Work With User Security form, select a data source, and then select Revise Data Source from the Row menu.	Change the system user for a data source.
Remove Data Source	W98OWSECK	On the Work With Security form, select the appropriate record in the tree structure, and then click Delete.	Remove a data source. If you chose a data source for a specific user or role, this form displays the user ID or the role name with the data source name. If you chose only the data source, this form displays only the data source name.
Work With System Users	W980001A	In Solution Explorer, enter *P980001* in the Fast Path.	Locate a system user.
System User Revisions	W980001C	On the Work With System Users form, select a system user and then click the Select button.	Change the system user password.

Adding a Data Source to a User, a Role, or All Users

Access the Add Data Source form.

1. Complete one of these fields or options:
   - User ID

     Complete this field to add a data source to a specific user.
   - Role

     Complete this field to add a data source to a specific role.
   - All Users

     Select this option to add a data source to all users.
2. Complete these additional fields and click OK:
   - Data Source

     Leave this field blank to set the data source information for all data sources. When you leave this field blank, the system automatically enters *DEFAULT* in the field.
   - System User

Revising a Data Source for a User, a Role, or All Users

Access the Work With User Security form.

1. Complete theData Source field, and then click Find.

   Note. You can also enter both a data source and user ID/role. If you select just a data source, the change will affect all users.

2. Select the data source in the tree structure and then, from the Row menu, select Revise Data Source.

   The Data Source Revisions form appears. If you chose a specific user or role, this form displays the user ID or the role name and the data source information. If you chose only the data source, this form automatically selects the All Users option with the data source information.

3. Complete the System User field and click OK:

   This field is necessary to access databases within the software. Depending on what you selected from the tree on the Work With User Security form, this information will apply to a specific user, a specific role, or all users.

Removing a Data Source for a User, Role, or All Users

Access the Work With User Security form.

1. Complete the Data Source field, and then click Find.
2. Select the appropriate record in the tree structure, and then click Delete.

   Note. For a user, you can also select a row in the detail area for the user, and then click Delete.

   The Remove Data Source form appears. If you chose a data source for a specific user or role, this form displays the user ID or the role name with the data source name. If you chose only the data source, this form displays only the data source name.

   Important! If you performed the search by data source without including a specific user or role, when you click OK on Remove Data Source, you remove the data source for *all* users.

3. Click OK to remove the data source.

Changing the System User Password

Access the Work With System User form.

1. Locate a system user and then click Select.
2. On the System Users Revision form, complete these fields and then click OK:
   - Password

     Enter a new password for the system user/data source combination.
   - Password Verify

     Enter the password again for verification purposes.

Enabling and Synchronizing Security Settings

This section provides an overview of enabling and synchronizing security settings and discusses how to:

- Change the workstation jde.ini file for user security.
- Set auxiliary security servers in the workstation jde.ini.
- Change the timeout value due to security server communication error.
- Change the enterprise server jde.ini file for security.
- Set auxiliary security servers in the server jde.ini.
- Verify security processes in the server jde.ini.

Understanding Security Setting Synchronization

You must modify the enterprise server and the workstation jde.ini files to enable and synchronize security settings between the enterprise server and the workstation.

Note. For the JD Edwards EnterpriseOne workstations, enable security by changing settings in the workstation jde.ini file. You should make these changes on the deployment server-resident jde.ini file that is delivered to the workstation through a package installation.

Changing the Workstation jde.ini File for User Security

Access the jde.ini file.

1. Locate the jde.ini file that will be sent to the workstation as part of a package installation.

   This file is located on the deployment server in the release share path:

   ```
   \\xxx\CLIENT\MISC\jde.ini
   ```

   Where *xxx* is the installed release level of the software (for example, 810).

2. Using a text editor such as Notepad, view the jde.ini file to verify this setting:

   ```
   [SECURITY]
   SecurityServer=Enterprise Server
   NameDefaultEnvironment=Default Environment
   ```

   This table explains the variable values:

Setting	Value
Security Server	The name of the enterprise server. For workstations to sign on and run batch reports on the enterprise server, this value must be the same for both the workstation and the enterprise server.
DefaultEnvironment	A name that identifies any valid environment. If no value is specified, security is not enabled for that workstation.

Setting Auxiliary Security Servers in the Workstation jde.ini

Within the [SECURITY] section of the workstation jde.ini file, you can set as many as 10 auxiliary security servers. This example shows how the jde.ini file might look:

```
[SECURITY]
NumServers=Numeric Value
SecurityServer=Enterprise Server Name (primary)
SecurityServer1=Enterprise Server Name (auxiliary)
SecurityServer2=Enterprise Server Name (auxiliary)
```

This table explains the variable values:

Setting	Value
NumServers	The total number of security servers (primary and auxiliary) that you set under the [SECURITY] section of the jde.ini file. For example, if you set one primary and four auxiliary servers, the NumServers value is 5. You can set NumServers to any value between 1 and 10. If you do not include the NumServers setting, the system assumes that you have only one server.
SecurityServer*n*	The name of a JD Edwards EnterpriseOne enterprise server. The primary and auxiliary security server names must all correspond to valid enterprise servers. The values for both the workstation and the enterprise servers must be the same for workstations to sign on to and run batch reports from the enterprise server. The variable value *n* can be a number between 1 and 10. This number defines the auxiliary security server.

Changing the Timeout Value Due to Security Server Communication Error

You might need to change a setting in the workstation jde.ini file if you receive an error such as:

```
Failure to Communicate with Security Server.
```

Change this section:

```
[JDENET]
connectTimeout=30
```

Changing the Enterprise Server jde.ini File for Security

To change the enterprise server jde.ini file for security, you should verify the server jde.ini file settings as shown in this task. Use these settings to specify the internal security parameters, valid users and passwords, environments, and data sources.

Locate the enterprise server's jde.ini file.

Using an ASCII editor, such as Notepad, view the jde.ini file to verify these settings:

```
[JDENET_KERNEL_DEF4]
dispatchDLLName=name of host dll
dispatchDLLFunction=JDEK_DispatchSecurity
maxNumberOfProcesses=1
beginningMsgTypeRange=551
```

```
endingMsgTypeRange=580
newProcessThresholdRequests=0
[SECURITY]
Security Server=Enterprise Server Name
User=user ID
Password=user password
ServerPswdFile=TRUE/FALSE
DefaultEnvironment=default environment
```

This table explains the variable values:

Setting	Value
dispatchDLLName	Values for enterprise server host platforms are: • HP9000, libjdeknet.sl • RS/6000, libjdekrnl.so • Windows (Intel), jdekrnl.dll • Windows (Compaq AlphaServer), jdekrnl.dll • iSeries, JDEKRNL For UNIX platforms, values are case-sensitive.
SecurityServer	The name of the enterprise server. This value must be the same for both the workstation and the enterprise server for workstations to run batch reports on the enterprise server.
User	The ID of a user with access to the F98OWSEC. This is the ID used to connect to the DBMS; therefore, this value must match that of the target DBMS.
Password	The password for the user ID with access to theF98OWSEC. 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 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 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, PD810).

Setting Auxiliary Security Servers in the Server jde.ini

Within the [SECURITY] section of the server jde.ini file, you can set one to 10 auxiliary security servers. You set multiple auxiliary security servers to establish levels of default servers. For example, if a machine cannot access a given security server, the machine tries the next security server that is defined in the [SECURITY] section. The settings for the auxiliary security servers might look like this example:

```
[SECURITY]
NumServers=Numeric Value
SecurityServer=Enterprise Server Name (primary)
SecurityServer1=Enterprise Server Name (auxiliary)
SecurityServer2=Enterprise Server Name (auxiliary)
```

This table explains the variable values:

Setting	Value
NumServers	The total number of security servers (primary and auxiliary) that you set under the [SECURITY] section of the jde.ini file. For example, if you set one primary and four auxiliary servers, the NumServers value is 5. You can set NumServers to any value between 1 and 10. If you do not include the NumServers setting, the system assumes that you have only one server.
SecurityServer*x*	The name of an enterprise server. The primary and auxiliary security server names must all be valid enterprise servers. The values must be the same for both the workstation and enterprise servers for workstations to log onto and run batch reports from the enterprise server. The variable value *x* can be any number between 1 and 10. This number defines the auxiliary security server.

Verifying Security Processes in the Server jde.ini

You should define only one process for the security network. You can set multiple processes, but they are probably not necessary. Under the [JDENET_KERNEL_DEF4] section of the server jde.ini file, verify that this parameter is set:

```
[JDENET_KERNEL_DEF4]
maxNumberOfProcesses=1
```

Running a Security Analyzer Report

This section provides an overview of the Security Analyzer Report and discusses how to:

- Run the Security Analyzer by Data Source Report (R98OWSECA).
- Run the Security Analyzer by User or Group Report (R98OWSECB).

Understanding the Security Analyzer Report

This process generates two separate reports that provide you with an analysis of JD Edwards EnterpriseOne security. The first report is the Security Analyzer by Data Source (R98OWSECA); it is organized and sorted by data source. A blank data source means that security for the System User ID is applicable to all data sources. The Security Analyzer by Data Source report is based on data that it reads from the F98OWSEC table.

The second report is the Security Analyzer by User or Group (R98OWSECB); it is organized by user or role. The Security Analyzer by User or Role report is also based on data that it reads from the F98OWSEC table.

Form Used to Run a Security Analyzer Report

Form Name	FormID	Navigation	Usage
Work With Batch Versions - Available Versions	W98305A	Report Management (GH9111), Batch Versions (P98305)	Run the Security Analyzer by Data Source (R98OWSECA) and Security Analyzer by User or Group (R98OWSECB) reports.

Running the Security Analyzer by Data Source Report (R98OWSECA)

This report presents security analysis information for each data source, each user ID, and each role. The report is sorted by data source and then by user ID. This columnar data appears in the report:

- Data Source

  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

  The actual user that JD Edwards EnterpriseOne uses to connect to the DBMS that you specified as the data source. This system user must match the user value that is defined in the DBMS.

- Change Frequency

  The number of days before the system requires that a user change their password. This data can be set by individual user ID or by role.

- Source Password Changed

  The date when a user's password was last changed.

- Invalid Signons

  The number of invalid sign-in attempts by a user. If the retry count value exceeds the number of allowed attempts, the user profile is disabled.

- Allowed Attempts

  The number of sign-in attempts that a user can make before that user profile is disabled.

- User Status

A value that indicates whether the user can sign in to JD Edwards EnterpriseOne. Values are *01* (enabled) and *02* (disabled).

- Status

  The display status of the User Status field.

Access the Work With Batch Versions - Available Versions form to run the Security Analyzer by Data Source Report (R98OWSECA).

1. Select a version and then click Select.

   The default version is XJDE0001. It creates a report for all user IDs for all data sources.
2. On the Version Prompting form, click Submit.
3. On the Report Output Destination form, select any of these options:
   - On Screen
   - To Printer
   - Export to CSV
4. If desired, select the OSA Interface Name option and enter a name in the box that appears.

Running the Security Analyzer by User or Group Report (R98OWSECB)

The Security Analyzer by User or Group Report (R98OWSECB) report presents security analysis information for each user ID, each group, and each data source. The report is sorted either by user ID or user group, depending on which processing option you select. This columnar data appears in the report:

- User ID
- Role
- Password Change Frequency

  The number of days before a user must change their password. This data can be set by individual user ID or by group.
- Data Source

  The data source to which the user is secured. A blank indicates all data sources.
- System User

  The actual user that the software uses to connect to the DBMS that you specified as the data source. The system user that is defined here must match the user value that is defined in the DBMS.

Access the Work With Batch Versions - Available Versions form to run the Security Analyzer by User or Group Report (R98OWSECB).

1. Select a version and click Select.

   The default version is XJDE0001. It creates a report for all user IDs for all data sources.

   By default, the XJDE0001 version has the processing option for this report set to *1*. This option generates a report by user ID.

   To generate a report by role, you can prompt for processing options and then, on the User Setup tab, change the value to *2*.
2. On the Version Prompting form, click Submit.

3. Complete the processing options as necessary, and then click OK.
4. On Report Output Destination, select any of these options:
   - On Screen
   - To Printer
   - Export to CSV
5. If desired, select the OSE Interface Name option and type a name in the field that appears.

Managing Unified Logon

This section provides an overview of unified logon and discusses how to:

- Modify the jde.ini setting to enable or disable unified logon.
- Set up a service for unified logon.
- Remove a service for unified logon.

Understanding Unified Logon

For configurations that use a Windows enterprise server, to set up unified logon, you need to modify only the [SECURITY] section of the jde.ini file. When a user signs on, these settings alert the software to use unified logon.

When the enterprise server is on a non-Windows platform, you need to set up a Windows service for unified logon. This service identifies the unified logon server for JD Edwards EnterpriseOne. You also need to set the unified logon settings in the [SECURITY] section of the jde.ini file.

Important! When you use unified logon, you need to use the same user ID for the Windows domain and JD Edwards EnterpriseOne so that the records for each are synchronized. For example, if the user ID for a user in the Windows domain is USER1, the user ID for JD Edwards EnterpriseOne must also be USER1. If the user IDs are different, unified logon does not work for the user.

Modifying the jde.ini Setting to Enable or Disable Unified Logon

Locate the jde.ini files on the server and on the workstation.

To modify the jde.ini setting to enable or disable unified logon:

1. In the server jde.ini file, add these settings in the [SECURITY] section:

```
[SECURITY]
SecurityMode=0, 1 or 2
```

Value	Description
0	Accepts only users set up for standard sign-in security.

Value	Description
1	Accepts only users set up for unified logon.
2	Accepts users set up for both unified logon and standard sign-in security.

2. In the workstation jde.ini file, add these settings in the [SECURITY] section:

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

Value	Description
0	Disables unified logon for the workstation. This setting is the default value.
1	Sets unified logon for the workstation.
server_name	Enter the name of the server on which the unified logon server data resides.

Setting Up a Service for Unified Logon

If the enterprise server is not a Windows server, you should set up services for unified logon on the deployment server. The deployment server is always a Windows server.

To set up a service for unified logon:

1. On the deployment server, in Windows Explorer, access the \Unified Logon directory and run the file UniLogonSetup.exe.

   The Unified Logon Server Setup form appears. On this form, you define the Windows service for unified logon servers. You can also remove these services on this form.

2. Complete these fields:

   - Unified Logon Service Name

     Enter the name for the unified logon server.

   - EnterpriseOne Port Number

     The port number for the unified logon server should match the JD Edwards EnterpriseOne port number of the server for which you want to set up unified logon.

   - Service Executable Filename

     Enter the directory path for the unified logon service program.

   - Log Filename

     Enter the name of the unified logon log file, including the full directory path.

     The default user list contains all authenticated network users.

3. To create a custom user list, enter the users or the groups in the Users or User Groups box to add the user information to the unified logon user list.

Note. Generally, the default Windows list of authenticated network users lists users by group.

4. Click the Install Service button to save the service information for the unified logon server.

Removing a Service for Unified Logon

To remove a service for unified logon:

1. Run UniLogonSetup.exe.

   The Unified Logon Server Setup form appears.

2. From the Unified Logon Service Name menu, select a unified logon server, and then click the Uninstall Service button.

CHAPTER 6

Setting Up JD Edwards Solution Explorer Security

This chapter provides an overview of JD Edwards Solution Explorer security and discusses how to configure JD Edwards Solution Explorer security.

Understanding JD Edwards Solution Explorer Security

Use the Security Workbench application (P00950) to set up security for these JD Edwards Solution Explorer features:

- Menu Design
- Menu Filtering
- Fast Path
- Documentation
- OMW Logging

This table describes the three general security settings for JD Edwards Solution Explorer features:

Security Setting	Description
Secured	Restricts the user from accessing the feature.
View	Allows read-only access to the feature but no modification capability.
Change	Gives the user full access to the feature with no restrictions on changing, adding, or deleting data.

In JD Edwards Solution Explorer, you can check the permissions for each feature for any user in the system. You view the settings by signing onto JD Edwards EnterpriseOne as the user whose settings you want to view, and then clicking the security button in the status bar of the JD Edwards Solution Explorer, which launches the Solution Explorer Security form. You cannot change the security settings from this form.

Note. You can also view existing Solution Explorer security records in P00950.

Fast Path Security Settings

Besides preventing or allowing access to Fast Path, you can also set up Fast Path access in a restricted view. The restricted view prevents web client users from entering an application ID in the Fast Path to launch an application. Instead, users can enter menu IDs to access menus in the EnterpriseOne Menu. The menu ID must be associated to a menu in the Task Master table (F9000).

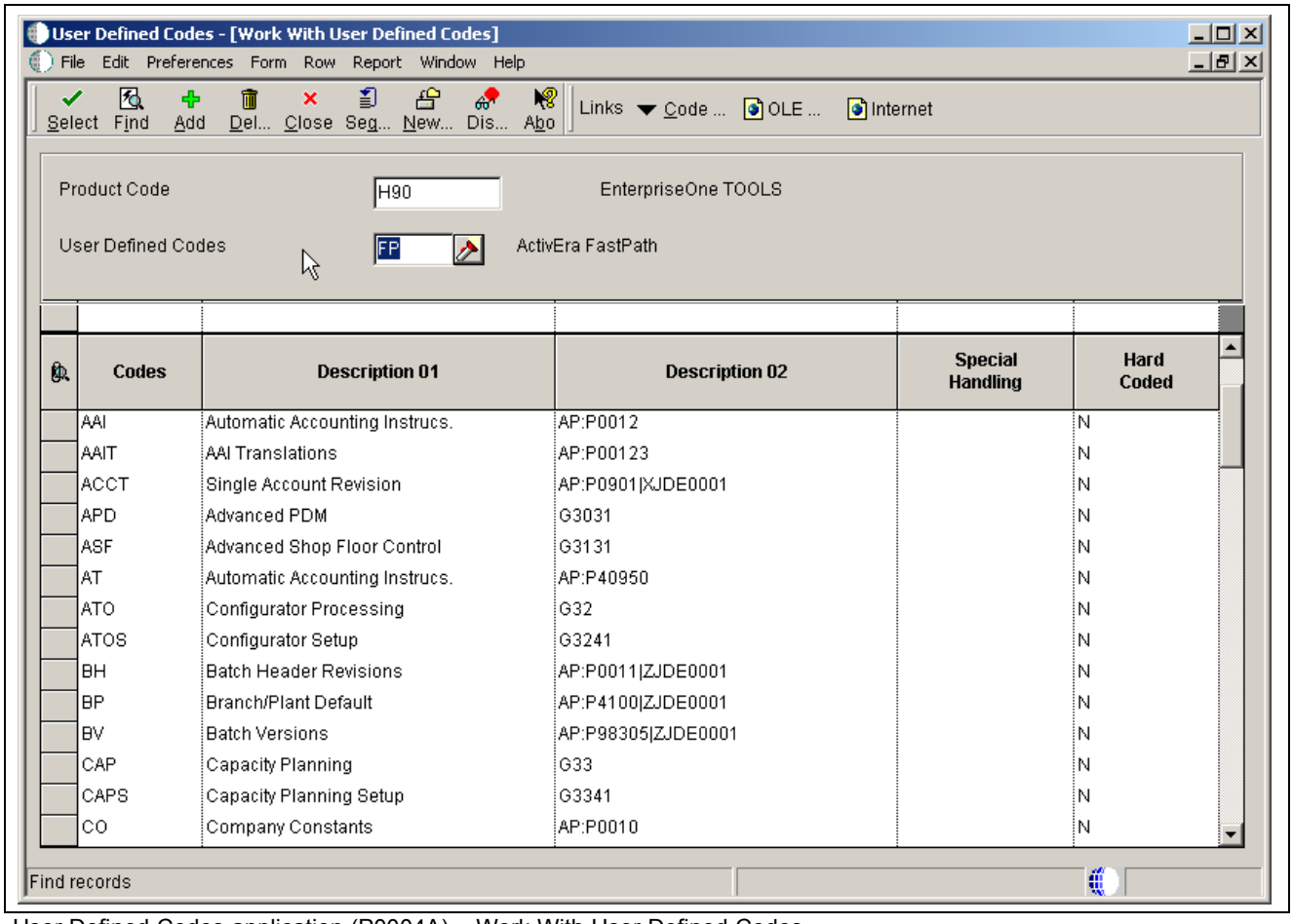
The restricted view also allows users to enter a mnemonic code, defined in the User Defined Code Values table (F0005), to launch an application or access a menu.

You can add UDCs for mnemonic codes using the User Defined Codes application (P0004A). Use these parameters when adding UDCs for mnemonic codes in P0004A:

- Product Code: H90 (EnterpriseOne Tools)
- UDC Type: FP

Note. After you add UDCs for mnemonic codes, you must clear the cache in order for the UDCs to take affect in the system. See "Clearing Cache" in the JD Edwards EnterpriseOne Solution Explorer guide.

This example shows some of the mnemonic codes already defined in JD Edwards EnterpriseOne:



User Defined Codes application (P0004A) – Work With User Defined Codes

To set up UDCs for mnemonic codes, refer to the instructions on how to customize and add UDCs.

See *JD Edwards EnterpriseOne Tools 8.97 System Administration Guide*, "Working with User Defined Codes," Customizing User Defined Codes.

Solution Explorer Security Presets

Security Workbench (P00950) contains security presets that determine default security settings for different types of users. These security presets correspond to novice (Preset One), intermediate (Preset Two), and expert (Preset Three) 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 task of manually choosing security setting options for each individual in the system because you can apply the settings to groups as well as to individual users.

Prerequisite

Fast Path Restricted View security is part of the JD Edwards EnterpriseOne Tools 8.97 release. However, to use this functionality, you must download a JD Edwards EnterpriseOne Tools ESU form the Update Center on Customer Connection. See SAR 8517645 for more information.

Configuring JD Edwards Solution Explorer Security

Access the Work With User/Role Security form. In Solution Explorer, enter *P00950* in the Fast Path.

1. Select the Form menu, Setup Security, Solution Explorer.
2. On the Work with Solution Explorer Security Revisions form, enter a user ID or role in the User/Role field.
3. Select the security options for Menu Design, Menu Filtering, and Documentation, as appropriate:
   - Secured
   - View
   - Change
4. For Fast Path, select one of these options:
   - Secured
   - View
   - Restricted View (menu navigation and mnemonics only)
5. Select one of these options to enable or disable OMW Logging:
   - Off
   - On
6. Alternatively, you can select any of these options from the Preset drop-down menu to specify default Solution Explorer security settings:
   - Preset One
   - Preset Two
   - Preset Three

CHAPTER 7

Using Security Workbench

This chapter provides an overview of Security Workbench (P00950) and discusses how to:

- Create security overrides.
- Manage application security.
- Manage action security.
- Manage row security.
- Manage column security.
- Manage processing option security.
- Manage tab security.
- Manage hyper exit security.
- Manage exclusive application security.
- Manage external calls security.
- Manage miscellaneous security.
- Manage push button, link, and image security.
- Manage text block control and chart control security.
- Manage media object security.
- Manage Data Browser security.
- Manage published business services security.
- Copy security from one user or role to another.
- Review and delete security records on the Work With User/Role Security form.
- Run the Security Workbench Records reports.

Understanding Security Workbench

Use Security Workbench to apply security to JD Edwards EnterpriseOne applications, application versions, forms, and other objects within JD Edwards EnterpriseOne that are described in this chapter. You can apply security for these objects to users, roles, or *PUBLIC. JD Edwards EnterpriseOne stores security information in the F00950 table and caches the security information in the web server's memory for the web clients and each workstation's memory on Microsoft Windows clients. Changes that you make to security are applied after the user exits JD Edwards EnterpriseOne and signs back in. For the security changes to take affect on web clients, you must restart the web server or clear the web server's cache using the Server Administration Workbench (SAW) application.

When applying object level security, you need to consider how JD Edwards EnterpriseOne checks for security. When a user signs in, the system first checks the user ID for security. If no object security is assigned to the user ID, then it checks the role (if the user is part of a specific role), and then finally it checks *PUBLIC.

Note. You can access Security Workbench on the JD Edwards EnterpriseOne web client, as well as the Microsoft Windows client.

Creating Security Overrides

This section provides an overview of security overrides, provides a prerequisite, and discusses how to add security overrides.

Understanding Security Overrides

Security overrides operate as exceptions to existing security records. They specify that users are *unsecured* from a JD Edwards EnterpriseOne object. In other words, security overrides allow users access to a particular object, even if another security record in the system specifies that access is not allowed.

Security overrides enable you to create object security more efficiently, with fewer security records to manage. For example, you might have a scenario that requires securing four out of five versions of an application from a group of users. Instead of creating four security records to prevent users from accessing each of the four versions, you can create two security records to achieve the same result. First, you would create a security override for the application version that you want users to access. This security override would specify that this version is not secured. These are the high level steps to create security overrides in Security Workbench:

1. Create a security record for the version, making sure that the security options are cleared.
2. Create a security record that secures users from accessing the application, including all versions of the application. In Security Workbench, you would select the application and then select the Run security option, which secures users from running the application.

As a result, when users try to access the application version, the security override for the version operates as an exception to the second application security record, allowing users access to the version of the application. All other versions of the application are secured.

You can create security overrides for these JD Edwards EnterpriseOne objects:

- Applications
- Actions
- Processing options
- Tabs
- Hyper exits
- External calls
- Push buttons, links, and images
- Media objects

Creating security overrides simplifies the process of applying security to various JD Edwards EnterpriseOne items. The following table provides some scenarios in which you could use security overrides to set up your security:

Scenario	Method
Allow a user or group of users access to a single form in an application. These users are otherwise restricted from using the application.	To set up: 1. Create a security override for the form. 2. Create a security record to prevent users from accessing the application.
Secure users from using all but one push button on a form in an application. This security shall apply to all versions of the application as well.	To set up: 1. Create a security override for the push button. 2. Create a security record to prevent users from using all push buttons on the form.
Allow only one user in a role access to an external application.	To set up: 1. Create a security override for the user that gives the user access to the external application. 2. Create a security record that prevents the role from accessing the external application.
Secure users from all action buttons except Add and Copy on a form in a particular version of an application.	To set up: 1. Create a security override to specify that Add and Copy action buttons are not secured on a form in a particular version of an application. 2. Create a security record to secure all actions on the form.

Prerequisite

Before you can create a security override for a JD Edwards EnterpriseOne object, you must first understand how a standard security record for the object is created in Security Workbench. See the appropriate sections in this chapter for instructions on how to apply security to JD Edwards EnterpriseOne objects such as applications, processing options, tabs, and media objects.

Adding Security Overrides

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, and then select the menu for the type of object for which you want to create a security override.
2. On the security form, enter the user or role ID in the User / Role field.

   Enter a complete user or role, which includes **PUBLIC*.
3. In the Display UnSecured Items region, complete the appropriate fields, and then click Find.

   This step provides a list of unsecured items for the user, role, or *PUBLIC in the UnSecured node.
4. Expand the UnSecured node to view the individual applications or versions, and the forms associated with each, that do not already have security set for them.

   After you expand the node, each item that you select appears in the grid.
5. Select the item in the node that you want to create a security override for.
6. In the Create with region, make sure that the security options are cleared or not selected.
7. Drag the item from the UnSecured node to the Secured node.

This action creates a security override for the user or role that can operate as an exception to a another security record for the user or role.

Managing Application Security

This section provides an overview of application security and discusses how to:

- Review the current application security settings for a user or role.
- Add security to an application.
- Secure a user or role from all JD Edwards EnterpriseOne objects.
- Remove security from an application.

Understanding Application Security

Application security enables you to secure these types of items from users:

- Applications

  When you secure an application, you secure all versions and forms associated with the application.

- Versions

  You can secure access to a version of an application while leaving other versions available to the user.

- Forms

  You can secure access to a single form in an application or application version.

You can secure users from running or installing (or both) a particular application, version, or form within an application.

This section also explains how to add a *ALL object and change all of the applications for a particular user or role from unsecured to secured.

Reviewing the Current Application Security Settings for a User or Role

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Application.
2. On the Application Security form, enter the user or role ID in the User / Role field.

   Enter a complete user or role, which includes **PUBLIC* but not wildcards.
3. In the Display UnSecured Items region, complete the appropriate fields to determine which items have already been secured for the user or role, and then click Find:

   - Application

     Enter an application name, such as *P01012.* You can also enter **ALL* to display all applications.

   - Version

     Enter a version name, such as *ZJDEC0001,* if you want to check only a specific version of an application. You can also use an asterisk to display all versions.

- Form Name

  Enter a form name, such as *W01012A*. You can also enter an asterisk to display all forms.

4. Expand the Secured node to view the security settings for the user or role in the detail area.

Adding Security to an Application

Enter *P00950* in the Fast Path.

Note. You cannot secure the Data Browser program using the Application Security form. Security Workbench provides a separate option for securing this program.

See Chapter 7, "Using Security Workbench," Managing Data Browser Security, page 94.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Application.
2. On the Application Security form, enter the user or role ID in the User / Role field.

   Enter a complete user or role, which includes **PUBLIC* but not wildcards.
3. In the Display UnSecured Items region, complete the appropriate fields, and then click Find.
   - Application
   - Version

     Enter a particular version of the application that you entered in the Application field. If you leave this field blank, the system displays all versions associated with the application in the UnSecured node.
   - Product Code

     Enter a product code to display all applications, versions, and forms associated with a particular product code. This field does not work in conjunction with the Application or Version fields.

     The search results appear under the UnSecured node.
4. Expand the UnSecured node to view the individual applications or versions, and the forms associated with each, that do not already have security set for them.

   After you expand the node, the individual items also appear in the grid.
5. In the Create with region, select one or both of these security options:
   - Run Security

     Select this option to secure users from running the application.
   - Install Security

     Select this option to prevent the just-in-time installation (JITI) of anything necessary to run the application.
6. Complete one of these steps:
   - Drag applications, versions, or forms from the UnSecured node to the Secured node.
   - From the Row menu, select All Objects to move all applications to the Secured node.
   - From the Row menu, select Secure to All to move all objects that are under the UnSecured node to the Secured node.

     If you secured an individual form, only the form appears under the Secured node. If you secured an application or version, the application or version and the forms associated with each appear under the Secured node.

7. To change the security on an item, select the item under the Secured node, select the appropriate security option, and then, from the Row menu, select Revise Security.

   In the grid, the values under the Run and Install fields change accordingly.

Securing a User or Role from All JD Edwards EnterpriseOne Objects

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Application.
2. On the Application Security form, enter the user or role ID in the User / Role field.

   Enter a complete user or role, which includes **PUBLIC* but not wildcards.
3. In the Display UnSecured Items area, enter **ALL* in the Application field to select *all* JD Edwards EnterpriseOne objects, and then click Find.
4. Expand the UnSecured node and then click *ALL in the detail area.
5. In the Create with region, select one or both of these options:
   - Run Security

     Use this option to secure users from running all applications.
   - Install Security

     Use this option for JITI only.
6. Complete one of these steps:
   - Drag **ALL* from the UnSecured node to the Secured node.
   - From the Row menu, select All Objects to move **ALL* to the Secured node.
   - From the Row menu, select Secure to All to move **ALL* from UnSecured node to the Secured node.

Removing Security from an Application

Access the Application Security form.

On the Application Security form, perform one of these steps:

- Under the Secured node, select an application, version, or form and click Delete.
- Drag an application, version, or form from the Secured node to the UnSecured node.
- Select Remove All from the Row menu to move *all* items from the Secured node to the UnSecured node.

Managing Action Security

This section provides an overview of action security and discusses how to:

- Review the current action security settings for a user or role.
- Add action security.
- Remove action security.

Understanding Action Security

Action security enables you to secure the buttons that enable users to perform particular actions, such as adding, deleting, inquiring, revising, or copying a record. These buttons typically reside on the toolbar in a form. Do not confuse these buttons with buttons that are located on other parts of a form.

See Also

Chapter 7, "Using Security Workbench," Managing Push Button, Link, and Image Security, page 86

Reviewing the Current Action Security Settings

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Action.
2. On the Action Security form, enter the user or role ID in the User / Role field and click Find.

   You can enter **PUBLIC* but not wildcards.

   Current action security settings for the user or role appear under the Secured node in the tree.
3. To see if an action security is applied to a particular application, version, or form, complete a combination of these fields in the Display Secured Item region, and then click Find:
   - Application

     Enter an application name, such as *P01012*.
   - Version

     Enter a version of the application entered in the Application field to see if action security is applied to the version.
   - Form Name

     Enter a form name, such as *W01012A*.
4. Expand the Secured node and click a secured item to view the current security settings for the user or role in the detail area.

Adding Action Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Action.
2. On the Action Security form, enter the user or role ID in the User / Role field and click Find.

   You can enter **PUBLIC* but not wildcards.

   Current action security settings for the user or role appear under the Secured node in the tree.
3. To find the applications, versions, or forms to which you want to apply action security, complete any of these fields under the Display UnSecured Items heading, and then click Find:
   - Application

     Enter an application name, such as *P01012*. Enter **ALL* to display all applications.
   - Version

     Enter a version of the application you entered in the Application field. If you leave this field blank, all versions associated with the application will appear in the UnSecured node.

- Product Code

4. Expand the Unsecured node to view individual applications, versions, and forms in the detail area.
5. In the Create with region, select any of these options:
   - Change
   - Add
   - Delete
   - OK/Select
   - Copy
   - Scroll To End
6. To secure the actions on an application, version, or form, perform one of these steps:
   - Drag the application, version, or form from the UnSecured node to the Secured node.
   - From the Row menu, select All Objects to move all items to the Secured node.
   - From the Row menu, select Secure to All to move all objects under the UnSecured node to the Secured node.

     For example, to set delete security on an application, select the Delete option. Next, drag the application from the UnSecured node to the Secured node. The detail area will reflect the delete security that you set for this application, which means that the user you entered cannot perform the delete action on this application.

     The applications or forms now appear under the Secured node and they have the appropriate action security.
7. To change the security on an item, select the item under the Secured node, select the appropriate security option, and then, from the Row menu, select Revise Security.

   In the grid, the values for the security options change accordingly.

Removing Action Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Action.
2. On the Action Security form, enter the user or role for which you want to change action security in the User / Role field, and then click Find.
3. To delete action security from an application, version, or form, do one of these:
   - Under the Secured node, select an application, version, or form and click Delete.
   - Under the Secured node, drag an application, version, or form from the Secured node to the UnSecured node.
   - Select Remove All from the Row menu to move *all* applications and forms from the Secured node to the UnSecured node.

Managing Row Security

This section provides an overview of row security and discusses how to:

- Add row security
- Remove row security

Understanding Row Security

Row security enables you to secure users from accessing a particular range or list of data in any table. Use row security sparingly because it can adversely affect system 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

JD Edwards EnterpriseOne first looks for row security at the user level, then at the group level, and then at the *PUBLIC level. If you set any of the security at a higher level, such as at the user level, the software ignores lower-level security settings, such as the group or *PUBLIC levels.

Before you set up row security for an item in a table, you should verify that the item is actually in that table. For example, the F0101 table contains the data item AN8. Therefore, you can set up row security for that item. However, the same table does not contain data item PORTNUM. Setting row security on this item for the F0101 table has no effect.

You set up row security on a table, not on a business view. You should verify that the object that you want to secure uses a business view over a table containing the object. For example, the Work With Environments application (P0094) uses business view V00941 over the F00941 table. You could secure the data item RLS (Release) because it is in the F00941 table. On the other hand, the same item is not in the F0094 table. If you attempt to secure the item on the F0094 table, data item RLS is not secured.

Note. You can find the tables, applications, forms, business views, and so on that use a data item by launching the Cross Reference application (P980011) after you build cross-reference tables (F980011and F980021).

Prerequisite

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

See *JD Edwards EnterpriseOne Tools 8.97 Development Tools: Data Dictionary Guide*, "Defining a Data Dictionary Item," Creating a Data Dictionary Item.

Adding Row Security

Enter *P92001* in the Fast Path.

1. On the Work With Data Items form, click Find.

   Note. You can enter search criteria in the Search Description field and the query by example (QBE) row to narrow your search.

2. Select the data item that you want to secure, and click Select.

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

   This option must be selected for row security to work.
4. Click OK.
5. Exit the data dictionary application.
6. In Solution Explorer, enter *P00950* in the Fast Path and press ENTER.
7. On the Work With User/Role Security form, select the Form menu, Set Up Security, Row.
8. On the Row Security form, complete the User / Role field and then click Find to display current row security.
9. Complete these fields, either in the first open detail area row (to add security) or in a pre-existing detail area row (to change security):
   - Table

     You can enter **ALL* in this field.
   - Data Item

     This field is required.
   - From Value

     This field is required.
   - Thru Value
   - Add
   - Change
   - Delete
   - View
10. Click OK to save the security information.

Removing Row Security

Enter *P00950* in Fast Path.

1. On the Work With User/Role Security form, select an object.
2. From the Form menu, select Set Up Security, Row.
3. On the Row Security form, complete the User / Role field and click Find.

   Note. If you accessed the Row Security form from the Work With User/Role Security form for a specific record, the user or role associated with the security record appears in the User / Role field by default.
4. Select the security record or records in the detail area, and then click Delete.
5. On Confirm Delete, click OK.
6. Click OK when you finish deleting row security.

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

Managing Column Security

This section provides an overview of column security and discusses how to:

- Add column security
- Remove column security

Understanding Column Security

This section explains how to add and revise column security. You can secure users from viewing a particular field or changing the value for a particular field. This item can be a database field, or a field that is defined in the data dictionary but is not in the database.

Note. You can find the tables, applications, forms, business views, and so on, that use a data item by launching the Cross Reference application (P980011) after you build the cross-reference tables (F980011and F980021).

You can set up column security on a table, an application, an application version, or a form. Even if an application uses a business view that does not contain the data item that you want to secure, you can still secure it, as long as the item appears on a form in the application.

Column Security on a Table

Before you set up column security on a table, do these:

- Verify that the object that you want to secure is in the table.
- Verify that the object that you want to secure is part of an application that uses a business view over a table containing the object.
- Verify that the object that you want to secure uses a business view that includes the column containing the object.

For example, if you want to apply column security to data item RLS (Release Number) in the F00941 table, RLS must be an item in that table, and it must also be part of an application using a business view over that table. Finally, the business view over the F00941 table must include a column containing the data item RLS.

If all of these conditions are met, you can successfully apply column security to the data item. Setting column security on a table also means that you set security on the data item for any other applications that use the F00941 table.

Column Security on an Application

Before you set up column security on an application, do these:

- Verify that the object that you want to secure is in the application.
- Verify that you are securing the correct data item in an application (data item descriptions can be similar, if not identical).

For example, if you want to apply column security to data item UGRP (UserRole) in the Object Configuration Manager application (P986110), you first verify that the item is in the application. Because it is in the application, you can apply security to the data item. However, note that data items UGRP, MUSE, USER, and USR0 all contain the identical data description of *User ID*. Verify the item by its alias, not by its data description.

Column Security on an Application Version

You can secure users from using columns (or fields) in a version of an application. When you secure a column in a version, the system secures the column in all forms associated with that application version.

Before you set up column security on an application version, do these:

- Verify that the object that you want to secure is in the version of the application.
- Verify that you secure the correct data item in an application (data item descriptions can be very similar, if not identical). Verify the item by its alias, not by its data description.

Column Security on a Form

Security Workbench enables you to secure the column in one particular form, either in an application or in a version of an application.

Before you set up column security on a form, do these:

- Verify that the object that you want to secure is in the form.
- Verify that you secure the correct data item in the form (data item descriptions can be very similar for different data items).

Adding Column Security

Enter *P00950* in Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Column.
2. On the Column Security form, complete the User / Role field, and then click Find to display current column security for the user or role.
3. To add new security, go to the last row of the detail area and enter information into any of these fields:
   - Table
   - Application
   - Version

     If you want to add column security to a particular version, enter a version of the application that you entered in the Application field.
   - Form Name

     You can enter **ALL* in any of these fields; however, after **ALL* is entered for a table, application, or form for a specific data item, you cannot enter **ALL* again for that data item.
4. Complete these fields:
   - Data Item
   - View
   - Add
   - Change
5. To change security, change the row values in the detail area.
6. Click OK to save the security information.

Removing Column Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Column.
2. On the Column Security form, complete the User / Role field, and then click Find.

   Note. If you accessed the Column Security form from the Work With User/Role Security for a specific record, the user or role associated with the security record appears in the User/Role field by default.

3. Highlight the security record or records in the detail area and click Delete,and then click OK on Confirm Delete.
4. Click OK when you finish deleting column security.

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

Managing Processing Option Security

This section provides an overview of processing option security and discusses how to:

- Review the current processing option security settings.
- Add security to processing options.
- Remove security from processing options.

Understanding Processing Option Security

You can secure users from changing, prompting for values, and prompting for versions of specific processing options. By itself, setting security that prohibits users from prompting for versions does not prevent them from changing values in the processing option. If you do not want users to use processing option values, you might want to set security so that users are secured from the "prompt for" value and "prompt for" versions.

For example, to set prompt-for-values security, which also automatically sets change security, select the Prompt for Values option. Next, drag one application at a time from the UnSecured node to the Secured node. The detail area reflects the prompt-for-values and change security that you set for these applications. This procedure means that the user 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.

Reviewing the Current Processing Option Security Settings

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select Set Up Security, Processing Option.
2. On the Processing Option Security form, enter a user or role ID in the User / Role field.

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

3. In the Display Secured Item region, complete these fields and then click Find:

- Application

  Enter an application name, such as *P01012*. Enter **ALL* to display all applications.

- Version

  Enter a version of the application you entered in the Application field.

  Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.

Adding Security to Processing Options

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Processing Option.
2. On the Processing Option Security form, enter the user or role ID in the User / Role field and then click Find.

   Enter a complete user or role, which includes **PUBLIC* but not wildcards.
3. In the Display UnSecured Items region, complete the appropriate fields and then click Find:
   - Application

     Enter an application name, such as *P01012*. Enter **ALL* to display all applications.

   - Version

     You can enter a particular version of the application that you entered in the Application field. If you leave this field blank, all versions associated with the application will appear in the UnSecured node.

   - Product Code

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

     The search results appear under the UnSecured node. Expand the node to view applications (interactive and batch) and menus with interactive or batch applications. After you expand the node, the applications appear in the detail area.

     For example, to set security on applications within the 00 product code, you 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. In the Create with region, select one or more of these options and drag applications from the UnSecured node to the Secured node:
   - Change
   - Prompt for Values

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

   - Prompt for Versions
   - Prompt for Data Selection
5. Perform one of these actions:
   - Drag applications from the UnSecured node to the Secured node.
   - From the Row menu, select All Objects to move all applications to the Secured node.

- From the Row menu, select Secure to All to move all objects under the UnSecured node to the Secured node.

  The applications now appear under the Secured node and have the appropriate security.

6. To change the security on an item, select the item under the Secured node, select the appropriate security option, and then, from the Row menu, select Revise Security.

   In the grid, the values for the security options change accordingly.

Removing Security from Processing Options

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Processing Option.
2. On the Processing Option Security form, enter a user or role ID to which you want to remove processing option security in the User / Role field.

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

   Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.
4. Perform one of these steps:
   - Under the Secured node, select an application or application version and click Delete.
   - Under the Secured node, drag an application or application version from the Secured node to the UnSecured node.
   - On the Row menu, select Remove All to move *all* items from the Secured node to the UnSecured node.

Managing Tab Security

This section provides an overview of tab security and discusses how to:

- Add tab security
- Remove tab security

Understanding Tab Security

You can secure users from changing the name of the tab and viewing the form that you call by using the tab. For example, to set up change security, select the Change option. Next, drag tabs one at a time from the UnSecured node to the Secured node. The detail area reflects the changed security that you set for the tabs. This security means that the user 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.

Adding Tab Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Tab Security.
2. On the Tab Exit Security form, complete these fields and click Find:
   - User / Role

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

     You can view security for a specific application or enter **ALL* to display all applications.

     Current security settings for the user or role appear under the Secured node in the tree. Expand the nodes to view the secured tabs. After you expand the node, the secured tabs also appear in the grid.
3. Complete *only one* of these fields in the Display UnSecured Items region and click Find:
   - Application

     Enter **ALL* in this field to select *all* JD Edwards EnterpriseOne objects.

     In the detail area, this special object appears as *ALL and displays the security that you defined for the object, such as Run Security or Install Security. The *ALL object acts as any other object, and you can use the Revise Security and Remove All options from the Row menu.
   - Product Code

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

     The search (application or product code) appears under the UnSecured node. Expand the node to view applications (interactive and batch) and the associated tabs. After you expand the node, the applications or tabs also appear in the detail area.

     For example, to set security for tabs in applications within the 00 product code, you 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. In the Create with region, select one or more of these options:
   - Change

     Select this option to prohibit a user or role from changing information on the tab page.
   - View

     Select this option to hide the tab from the user or the role.
5. Drag tabs from the UnSecured node to the Secured node.

   These tabs now appear under the Secured node.
6. To change the security on an item, select the item under the Secured node, select the appropriate security option, and then, from the Row menu, select Revise Security.

   In the grid, the values for the security options change accordingly.

Removing Tab Security

Access the Work With User/Role Security form.

1. From the Form menu, select Set Up Security, Tab Security.

2. On the Tab Exit Security form, complete these fields and click Find:
   - User / Role

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

     You can view security for a specific application or enter **ALL* to display all applications.

     Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the secured tabs. After you expand the node, the secured tabs also appear in the grid.
3. Perform one of these steps:
   - Under the Secured node, select a tab and then click Delete.
   - Under the Secured node, drag a tab from the Secured node to the UnSecured node.
   - On the Row menu, select Remove All to move all tabs from the Secured node to the UnSecured node.

Managing Hyper Exit Security

Menu bar exits, also referred to as hyper exits, call applications and allow users to manipulate data. You can secure users from using these exits. Hyper exit security also provides restrictions for menu options. This section discusses how to:

- Add hyper exit security
- Remove hyper exit security.

Adding Hyper Exit Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Hyper Exit Security.
2. On the Hyper Exit Security form, complete these fields and click Find:
   - User / Role

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

     View security for a specific application. Enter **ALL* to display all applications.

     Current security settings for the user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as interactive and batch. After you expand the node, the secured hyper-button exits also appear in the detail area.
3. In the Display Unsecured Items region, complete only one of these fields to locate the applications to which you want to apply exit security, and click Find:
   - Application

     You can enter **ALL* in this field.

- Product Code

  You can search for all of the applications within a product code. For example, to set security on hyper-buttons in applications within the 00 product code, you 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.

  The search (application, product code, or menu) appears under the UnSecured node. Expand the node to view applications (interactive and batch) and hyper-button exits. After you expand the node, the hyper-button exits also appear in the detail area.

4. Expand the UnSecured node to view and select applications (interactive and batch) and hyper-button exits.

   After you expand the node, the hyper-button exits also appear in the detail area.

5. In the Create with region, select the Run Security option.
6. Drag exits one at a time from the UnSecured node to the Secured node.

   The exits that you dragged now appear under the Secured node. The grid reflects the security that you set for these exits. This security prevents the user that you entered from using the exit.

Removing Hyper Exit Security

Enter *P00950* in the Fast Path..

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Hyper Exit Security.
2. Complete these fields and click Find:
   - User / Role

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

   - Application

     View security for a specific application. Enter **ALL* to display *all* applications.

     Current security settings for the user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as interactive and batch. After you expand the node, the secured hyper-button exits also appear in the detail area.

3. Perform one of these steps:
   - Under the Secured node, select a hyper exit and click Delete.
   - Under the Secured node, drag a hyper exit from the Secured node to the UnSecured node.
   - On the Row menu, select Remove All to move all hyper exits from the Secured node to the UnSecured node.

Managing Exclusive Application Security

This section provides an overview of exclusive application security and discusses how to:

- Add exclusive application security.
- Remove exclusive application access.

Understanding Exclusive Application Security

Exclusive application security enables you to grant access to otherwise secured information through one exclusive application. For example, assume that you use row security to secure a user from seeing a range of salary information; however, the user needs to run a report for payroll that includes that salary information. You can grant access to the report, including the salary information, using exclusive application security. JD Edwards EnterpriseOne continues to secure the user from all other applications in which that salary information might appear.

Adding Exclusive Application Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Exclusive Application.
2. On the Exclusive Application Security form, complete the User / Role field.

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

     Enter the name of the exclusive application for which you want to allow access (the security). For example, to change the security for a user of the Vocabulary Overrides application, enter *P9220* in this field.
   - Run Application
4. Click OK to save the information.

Removing Exclusive Application Access

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Exclusive Application.
2. On the Exclusive Application Security form, complete the User / Role field and click Find.

   Note. If you accessed the Exclusive Application Security form from a specific record in the Work With User/Role Security form, the user or role associated with the security record appears in the User/Role field by default.
3. Highlight the security records in the grid and click Delete.
4. On the Confirm Delete message form, click OK.
5. Click OK when you finish deleting exclusive application security.

   If you do not click OK after you delete the security records, JD Edwards EnterpriseOne does not save the deletion.

Managing External Calls Security

This section provides an overview of external call security and discusses how to:

- Add external call security.
- Remove external call security.

Understanding External Call Security

In JD Edwards EnterpriseOne, certain applications exist that are not internal to JD Edwards EnterpriseOne; they are standalone executables. For example, the Report Design Aid, which resides on the Cross Application Development Tools menu (GH902), is a standalone application. You can also call this application externally using the RDA.exe. By default, this file resides in the `\E810\SYSTEM\Bin32` directory.

Adding External Call Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, External Calls.
2. On the External Calls Security form, complete these fields and click Find:
   - User / Role

     Enter a complete user or group ID, which includes **PUBLIC* but not wildcards.
   - Executable

     Enter the name of the external application, such as *debugger.exe.* When you enter information into this field, the software searches only for the indicated application.

     Current security settings for that user or group appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as debugger.exe.
3. In the Create with region, select the Run Security option.
4. Complete one of these steps:
   - Drag applications from the UnSecured node to the Secured node.
   - To move all applications to the Secured node, select All Objects from the Row menu.

     The external call applications now appear under the Secured node and have the appropriate security.

     For example, to set run security on the Business Function Design application, select the Run Security option and then drag the Business Function Design node from the UnSecured node to the Secured node. The detail area reflects the run security that you set for this application, which means that the user you entered could *not* run the Business Function Design application.
5. To change the security on an item, select the item under the Secured node, select the Run Security option, and then, from the Row menu, select Revise Security.

   In the grid, the value in the Run field changes accordingly.

Removing External Call Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, External Calls.

2. On the External Calls Security form, complete these fields and click Find:
   - User / Role

     Enter a complete user or group ID, which includes **PUBLIC* but not wildcards.
   - Executable

     Enter the name of the external application, such as *debugger.exe*. When you enter information into this field, the software searches only for the indicated application.

     Current security settings for that user or group appear under the Secured node in the tree. Expand the node to view the individual secured applications, such as debugger.exe.
3. Perform one of these steps:
   - Under the Secured node, select an application and click Delete.
   - Under the Secured node, drag an application from the Secured node to the UnSecured node.
   - On the Row menu, select Remove All to move *all* applications from the Secured node to the UnSecured node.

Managing Miscellaneous Security

This section provides an overview of miscellaneous security and discusses how to manage miscellaneous security features.

Understanding Miscellaneous Security

JD Edwards EnterpriseOne security enables you to secure users and roles from:

- Read/write reports
- Workflow status monitoring

Read/Write Reports Security

JD Edwards EnterpriseOne enables administrators to prevent specific users and roles from running reports that update JD Edwards EnterpriseOne database tables (read/write reports). Administrators can assign users to a user profile called No Update Report Creation User (NUR), which restricts users to running only read-only reports. When an NUR user runs a report, JD Edwards EnterpriseOne prevents the report from making table input/output (I/O) calls to databases that can affect business data. Users assigned to this profile can create and run read-only reports, but are restricted from creating or running existing UR reports. NUR users can copy existing UR reports and run the copied report, although the software disables the report's ability to change business data and displays a warning that the copied report cannot be updated. NUR users can edit NUR reports in Report Design Aid, but are prevented from even opening existing UR reports in RDA.

Workflow Status Monitoring Security

Users can access Workflow Modeler, (a scaled-down version of Process Modeler) to design JD Edwards EnterpriseOne workflow models. Process Modeler Server includes a JD Edwards EnterpriseOne Portal-based component called Model Viewer, which enables users with appropriate access to monitor the status of a workflow and perform workflow administration tasks directly from the Viewer.

Miscellaneous security includes these Workflow Status Monitoring settings, which determine the operations a user can perform from the Model Viewer:

- Secured

  Restricts users from accessing any Model Viewer tasks using the Portal.

- Partial

  Allows users to view workflow models and to monitor their status, but restricts these users from performing any administrative tasks.

- Full

  Allows users to access all Model Viewer tasks using the JD Edwards Collaborative Portal. Users can view workflow statuses and perform administrative tasks.

Managing Miscellaneous Security Features

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Misc Security.
2. On the Miscellaneous Security form, complete the User / Role field and click Find.

   Enter a complete user or role, which includes **PUBLIC* but not wildcards.
3. To change Read-Only Report security, select one of these options:
   - Read / Write
   - Read Only
4. To change Workflow Status Monitoring security, select one of these options:
   - Secured

     Prevents users from viewing or administering workflow.
   - View

     Allows users to view workflow but prevents them from making changes.
   - Full

     Allows users to view and administer workflow.
5. Click OK to accept the changes.

Managing Push Button, Link, and Image Security

This section provides an overview of push button, link, and image security and discusses how to:

- Add push button, link, and image security.
- Remove push button, link, and image security.

Note. Push button, link, and image security is enforced only for interactive applications in the JD Edwards EnterpriseOne HTML client and the Portal. It is not supported on the Microsoft Windows client.

Understanding Push Button, Link, and Image Security

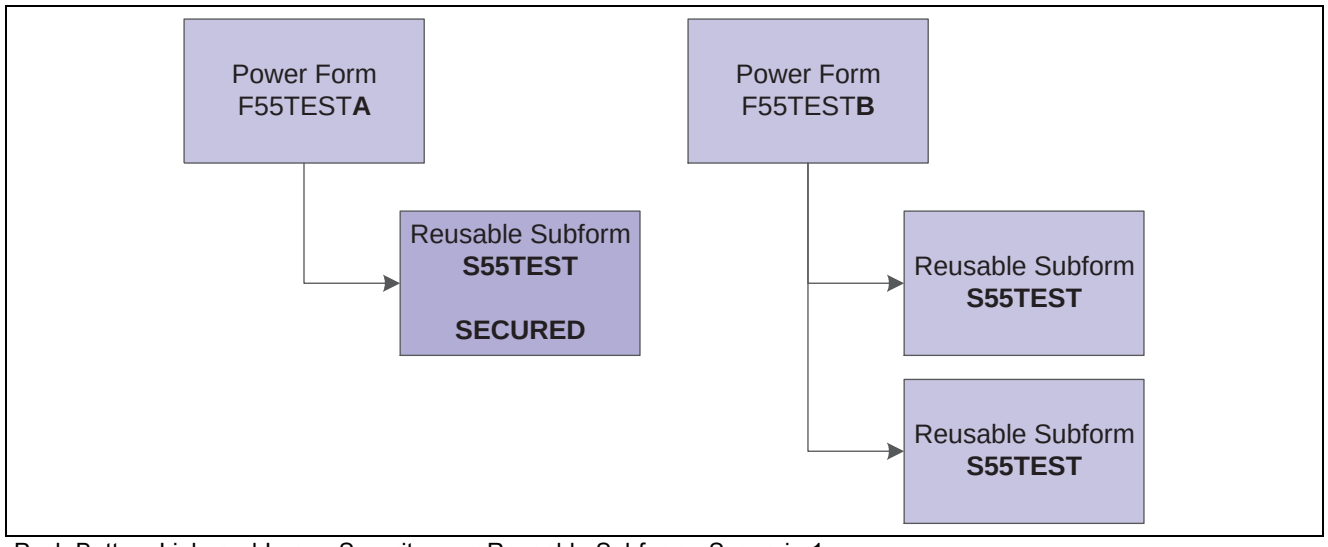
JD Edwards EnterpriseOne enables you to secure users from using or viewing push button, link, and image controls. You can secure users from using a control but still allow them to view it. Or you can prevent users from both using and viewing a control.

Note. In JD Edwards EnterpriseOne forms, static text and text boxes can be made into links. However, you can only apply security to static text links, not to text box links.

Security Workbench displays the objects that you want to secure in a hierarchical tree structure that contains nodes for each application, application version, and form. Security Workbench only displays the forms that contain push button, link, and image controls. You can secure an individual control by dragging the control from the UnSecured node to the Secured node. In addition, you can secure all controls—push buttons, links, or images—on a form by dragging the form node to the Secured node. You can perform the same action on applications and application versions. For example, to secure all the links within an entire application, you drag the application from the UnSecured node to the Secured node to secure all the links in every form within the application as well as within any versions of the application. If you drag an application version node to the Secured node, only the links in that application version are secured.

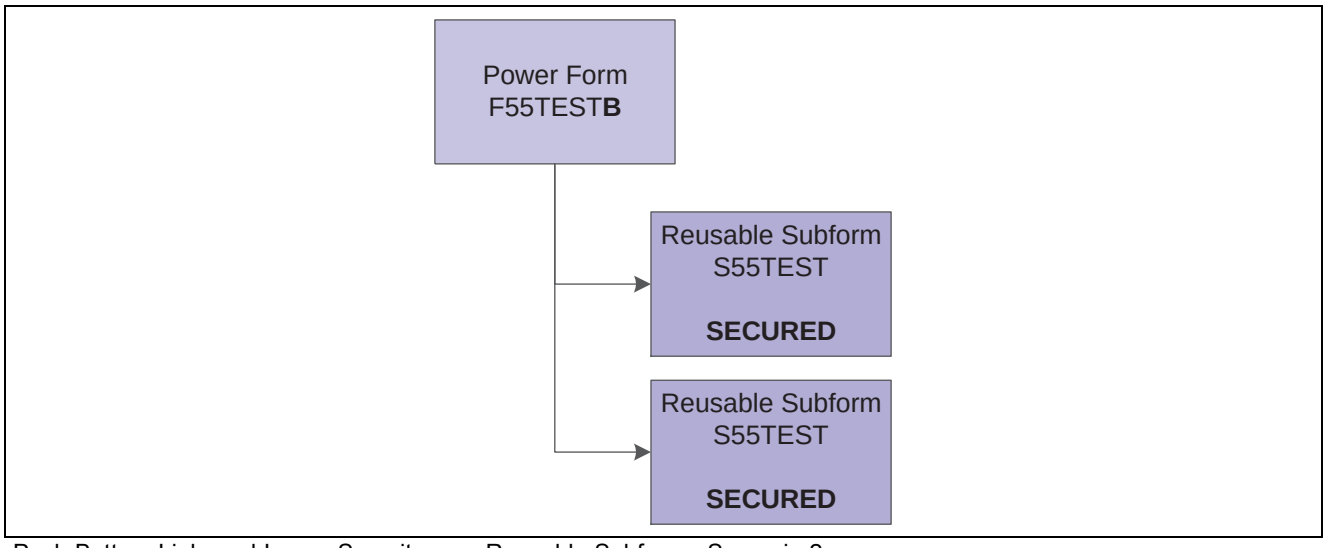
Push Button, Link, and Image Security on Subforms

You can secure push buttons, links, and images on both embedded and reusable subforms in JD Edwards EnterpriseOne. If you secure controls on an embedded subform, only the controls within that subform are secured. For reusable subforms, the behavior of the security depends upon the context in which the reusable subforms are used in power forms. If you apply security to a reusable subform under a power form, then only the controls in that reusable subform for that particular power form are secured, even if the reusable subform is used by another power form, as shown in this diagram:



Push Button, Link, and Image Security on a Reusable Subform - Scenario 1

However, if you apply security to a reusable subform under a power form, and that subform is reused in the same power form, the security is applied to both subforms, as shown in this diagram:



Push Button, Link, and Image Security on a Reusable Subform - Scenario 2

Because security functions differently on embedded subforms than it does on reusable subforms, Security Workbench provides a way for you to distinguish between the two forms. To make this distinction, the tree structure in Security Workbench displays the embedded subform using its form ID, and it displays the reusable subform using its form title.

Adding Push Button, Link, and Image Security

Enter *P00950* in the Fast Path to access the Work With User/Role Security form.

1. From the Form menu, select Set Up Security, and then select the menu for push buttons, links, or images, depending on the type of object that you want to secure.
2. Complete the User / Role field and click Find.

   Enter a complete user or role, which includes **PUBLIC*.
3. In the Display UnSecured Items region, complete the appropriate fields and then click Find:
   - Application

     Enter an interactive application name, such as *P01012*. Enter **ALL* to display all applications.

     Note. Batch applications are not supported.
   - Version

     You can enter a particular version of the application that you entered in the Application field. If you leave this field blank, Security Workbench displays all unsecured versions associated with the application in the UnSecured node.
   - Product Code

     Enter a product code to display all applications, versions, and forms associated with a particular product code. This field does not work in conjunction with the Application and Version fields.

   The search results appear under the UnSecured node.
4. Expand the UnSecured node to view the individual applications or versions, and the forms associated with each.

   Only the forms that contain controls are displayed.

5. Under the Create with region, select the type of security that you want to apply:
   - View

     This option prevents the user from using and viewing the control.
   - Enable

     This option prevents the user from using the control. However, the control is still visible.
6. Use one of these actions to secure the items:
   - Drag items from the UnSecured node to the Secured node.
   - From the Row menu, select All Objects to move all applications to the Secured node.

     The system displays the items under the Secured node that have the appropriate security. You can view the security for each item in the grid.

Removing Push Button, Link, and Image Security

Enter *P00950* in the Fast Path.

1. On the Work with User/Role Security form, select the Form menu, Set Up Security, and then the menu for push buttons, links, or images.
2. Enter a user or role ID from which you want to remove the security in the User / Role field.

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

   Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.
4. Perform one of these steps:
   - Under the Secured node, select an application or application version and click Delete.
   - Under the Secured node, drag an application or application version from the Secured node to the UnSecured node.
   - On the Row menu, select Remove All to move *all* items from the Secured node to the UnSecured node.

Managing Text Block Control and Chart Control Security

This section provides an overview of text block control and chart control security and discusses how to:

- Review current text block control and chart control security settings.
- Add text block control and chart control security.
- Remove text block control and chart control security.

Understanding Text Block Control and Chart Control Security

JD Edwards EnterpriseOne enables you to secure users from using or viewing text block and chart controls. You can secure users from using a control but still allow them to view it. Or you can prevent users from both using and viewing a control.

In JD Edwards EnterpriseOne, a text block or chart control can have separate segments that contain links to other objects. You cannot secure these individual segments of a control. When you secure a text block or chart control, security is applied to the entire control.

See Also

JD Edwards EnterpriseOne Tools 8.97 Development Tools: Form Design Aid Guide, "Understanding Text Block Controls"

Reviewing Current Text Block Control and Chart Control Security Settings

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select Set Up Security from the Form menu, and then select the menu for text block control or chart control.
2. Enter the user or role ID in the User / Role field and click Find.

   You can enter **PUBLIC* but not wildcards.

   The system displays the control security settings for the user or role under the Secured node in the tree.
3. To see if control security is applied to a particular application, version, or form, complete a combination of these fields in the Display UnSecured Items region, and then click Find:
   - Application

     Enter an application name, such as *P01012*.
   - Version

     Enter a version of the application entered in the Application field to see if control security is applied to the version.
   - Form Name

     Enter a form name, such as *W0101G*.
4. Expand the Secured node and click a secured item to view the current security settings for the user or role in the detail area.

Adding Text Block Control and Chart Control Security

Enter *P00950* in the Fast Path to access the Work With User/Role Security form.

1. From the Form menu, select Set Up Security, and then select the menu for text block control or chart control, depending on the type of control that you want to secure.
2. Complete the User / Role field and click Find.

   Enter a complete user or role, which includes **PUBLIC*.
3. In the Display UnSecured Items region, complete the appropriate fields and then click Find:

- Application

  Enter an interactive application name, such as *P01012*. Enter **ALL* to display all applications.

  Note. Batch applications are not supported.

- Version

  You can enter a particular version of the application that you entered in the Application field. If you leave this field blank, Security Workbench displays all unsecured versions associated with the application in the UnSecured node.

- Product Code

  Enter a product code to display all applications, versions, and forms associated with a particular product code. This field does not work in conjunction with the Application and Version fields.

The search results appear under the UnSecured node.

4. Expand the UnSecured node to view the individual applications or versions, and the forms associated with each.

   Only the forms that contain controls are displayed.

5. Under the Create with region, select the type of security that you want to apply:

   - View

     This option prevents the user from using and viewing the control.

   - Enable

     This option prevents the user from using the control. However, the control is still visible.

6. Use one of these actions to secure the items:

   - Drag the text block or chart control from the UnSecured node to the Secured node.
   - Select the control that you want to secure and then select Secure Selected from the Row menu.
   - From the Row menu, select All Objects to move all applications to the Secured node.

     The system displays the items under the Secured node that have the appropriate security. You can view the security for each item in the grid.

Removing Text Block Control and Chart Control Security

Enter *P00950* in the Fast Path.

1. On the Work with User/Role Security form, select the Form menu, Set Up Security, and then the menu for text block control or chart control security.
2. Enter a user or role ID from which you want to remove the security in the User / Role field.

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

3. Click Find.

   Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.

4. Perform one of these steps:

   - Under the Secured node, select an application or application version and click Delete.

- Under the Secured node, drag an application or application version from the Secured node to the UnSecured node.
- On the Row menu, select Remove All to move *all* items from the Secured node to the UnSecured node.

Managing Media Object Security

This section provides an overview of media object security and discusses how to:

- Review the current media object security settings for a user or role.
- Add media object security.
- Remove media object security.

Understanding Media Object Security

JD Edwards EnterpriseOne enables you to secure users from adding, changing, deleting, or viewing media objects within interactive applications, forms, or application versions. You can apply media object security to ensure that media object attachments cannot be modified or tampered with after they have been added.

If you apply view security to media object attachments, Security Workbench automatically prevents the user from adding, deleting, or changing media objects. If you apply change security to media object attachments, Security Workbench automatically prevents the user from deleting the media object.

Media object security enables you to use media object attachments as a mechanism for recording justifications for transactions and for legal purposes. For example, your company may have a business process that requires clerks to use media object attachments to document the reason or justification for adjusting a price on an item in a transaction. In this case, you would allow the clerks to add and view media object attachments in an application, but secure them from deleting or modifying them. In addition, this type of security prevents users from modifying or deleting attachments that others have added. As a result, the media object attachments provide secured information about previous transactions. This information can be reviewed by interested parties for legal or other purposes.

Note. Media object security is enforced only in interactive applications on the JD Edwards EnterpriseOne web client and the Portal. It is not supported on the Microsoft Windows client.

Also, media object system functions enforce media object security in the web client. When running applications that have media object security applied to them, the system logs the security information for the system functions in the web client debug log file.

Reviewing the Media Object Security Settings

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Media Object.
2. On the Media Object Security form, enter the user or role ID in the User / Role field and click Find.

   You can enter **PUBLIC* but not wildcards.

   The system displays current media object security settings for the user or role under the Secured node in the tree.

3. To see if a media object security is applied to a particular application, version, or form, complete a combination of these fields in the Display UnSecured Items region, and then click Find:
   - Application

     Enter an application name, such as *P01012*.
   - Version

     Enter a version of the application entered in the Application field to see if media object security is applied to the version.
   - Form Name

     Enter a form name, such as *W0101G*.
4. Expand the Secured node and click a secured item to view the current security settings for the user or role in the detail area.

Adding Media Object Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Media Object.
2. On the Media Object Security form, enter the user or role ID in the User / Role field and click Find.

   You can enter **PUBLIC* but not wildcards.

   Current media object security settings for the user or role appear under the Secured node in the tree.
3. To find the applications, versions, or forms to which you want to apply media object security, complete any of these fields in the Display UnSecured Items region, and then click Find:
   - Application

     Enter an application name, such as *P01012*. Enter **ALL* to display all applications.
   - Version

     Enter a version of the application you entered in the Application field. If you leave this field blank, all versions associated with the application will appear in the UnSecured node.
   - Product Code
4. Expand the Unsecured node to view individual applications, versions, and forms in the detail area.
5. In the Create with region, select any of these options:
   - Change
   - Add
   - Delete
   - View

   Note. If you apply view security to media object attachments, Security Workbench automatically prevents the user from adding, deleting, or changing media objects. If you apply change security to media object attachments, Security Workbench automatically prevents the user from deleting the media object.
6. To secure the media objects on an application, application version, or form, perform one of these steps:
   - Drag the application, version, or form from the UnSecured node to the Secured node.

- From the Row menu, select All Objects to move all items to the Secured node.
- From the Row menu, select Secure to All to move all objects beneath the UnSecured node to the Secured node.

  For example, to set delete security, select the Delete option. Next, drag the application from the UnSecured node to the Secured node. The detail area will reflect the media object security that you set for this application.

  The applications or forms now appear under the Secured node, and they have the appropriate media object security.

Removing Media Object Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Media Object.
2. In the User / Role field, enter a user or role ID from which you want to remove media object security.

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

   Current security settings for that user or role appear under the Secured node in the tree. Expand the node to view the individual secured applications. After you expand the node, the applications that are secured also appear in the detail area.
4. Perform one of these steps:
   - Under the Secured node, select an application or application version and click Delete.
   - Under the Secured node, drag the item that is secured from the Secured node to the UnSecured node.
   - On the Row menu, select Remove All to move *all* items from the Secured node to the UnSecured node.

Managing Data Browser Security

This section provides an overview of Data Browser security and discusses how to:

- Add Data Browser security.
- Remove Data Browser security.

Understanding Data Browser Security

Data Browser security enables you to grant permission to users, roles, or *PUBLIC to access the Data Browser program. There are two levels of Data Browser security that you can assign to users. The first level grants access to the Data Browser, which users can use to perform public or personal queries. After you grant this access, you can grant an additional level of security that allows Data Browser users to select a particular table or business view that they wish to query.

You can also use the Copy feature in Security Workbench to copy Data Browser security from one user or role to another.

See Also

JD Edwards EnterpriseOne Tools 8.97 Foundation Guide, "Using JD Edwards Web Applications and Reports," Viewing the Data in Tables and Business Views

Adding Data Browser Security

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, Set Up Security, Data Browser.
2. On the Data Browser Security form, enter the user or role ID in the User / Role field and click Find.

   You can enter **PUBLIC* but not wildcards.
3. In the Data Browser hierarchical security permissions region, select one or both of these options, depending on the level of security that you want to grant:
   - Allow access to launch Data Browser.

     This option gives users access to the Data Browser, which they can use to perform personal or public queries.
   - Allow access to Search and Select for Tables or Business View Queries.

     This option gives users the ability to search and select the table or business view that they want to query.

     Note. This option is enabled only after you select the first option.
4. Click OK.

   Note. To activate Data Browser security changes, you must refresh the jdbj security cache using the SAW.

Removing Data Browser Security

You can remove Data Browser security using the Data Browser Security form or the Work With User/Role Security form. To remove security using the Data Browser Security form, clear the security check boxes for a user, role, or *PUBLIC. Using the Work With User/Role Security form, search for the security record and then delete the Data Browser security record from the grid.

Managing Published Business Services Security

This section provides an overview of published business services security and discusses how to:

- Review the current published business services security records.
- Authorize access to published business services.
- Add multiple published business services security records at a time.
- Delete published business services security.

Understanding Published Business Services Security

JD Edwards EnterpriseOne provides security to ensure that web service consumers are authenticated in the JD Edwards EnterpriseOne system and authorized to access published business services. The authentication of users of published business service users is handled by the Business Services Server and EnterpriseOne security server. After a user is authenticated by the JD Edwards EnterpriseOne security server, the system checks if the user is authorized to run a published business service by retrieving records from the JD Edwards EnterpriseOne F00950 security table, which contains all the object security records.

Note. This section discusses only the authorization of users to access published business services.

For published business services, JD Edwards EnterpriseOne uses a "secure by default" security model which means that users cannot access a published business service unless a security record exists that authorizes access. For all other objects in JD Edwards EnterpriseOne, access is granted unless otherwise secured or restricted.

You manage published business services security using Security Workbench (P00950), the application used to manage all object security in JD Edwards EnterpriseOne. In P00950, you can add, copy, modify, or delete security records for published business services. When a user tries to access or run a published business service, verification of authorization is done through an API that queries records in the F00950 security table.

As with all object security in JD Edwards EnterpriseOne, you can assign published business service security to a user, role, or *PUBLIC. You can create a security record that allows a user or role access to:

- A particular method in a published business service.
- All methods in a published business service.
- All published business services.

It is recommended that you set up security by role first. This method makes setting up published business services security easier; instead of defining security for individual users, you can define security for the role and then assign users to the appropriate roles. If an individual in a role needs a different security setup, you can assign security at the user level, which overrides the role settings.

In addition, you can create a security record that disallows access to a published business service. Typically, there is no need to add security records that disallow access because by default, access to published business services is not allowed. However, creating a security record that disallows access can be an efficient method to set up published business services security. For example, to allow a role access to all but a small subset of published business services, you can:

- Enter *ALL in the fields for the published business service and published business service method to create a security record that allows the role access to all published business services.
- Create security records for the same role that disallows access to a subset of published business services.

Inherited Security

When creating a published business service, a developer can configure it to pass its context to any published business service that it calls. In this configuration, authorization for the called published business service is inherited; that is, if the calling business service is authorized, then the called business service is authorized as well. In this scenario, the system does not check the security for the called business service.

However, it is possible (though not supported) to configure a published business service so that it does not pass its context to another business service. In this scenario, the security or authorization for the called published business service is not inherited. Even if a user is authorized to access the calling or parent business service, the system also checks if access to the called business service is allowed. As a result, if there is not a security record that allows access to the called business service, the system will produce an exception or error, denying access to the called business service.

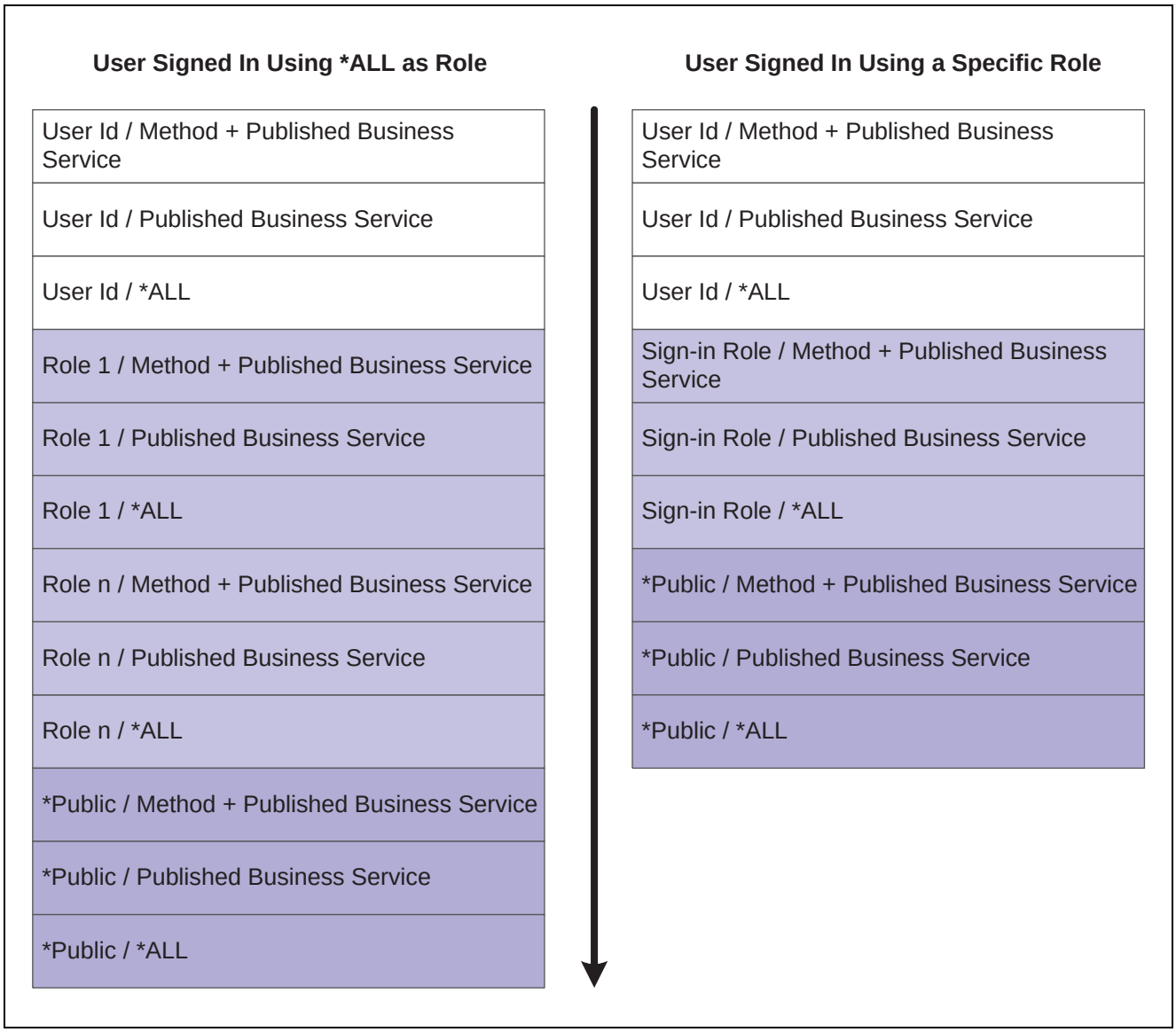
How JD Edwards EnterpriseOne Checks Published Business Services Security

JD Edwards EnterpriseOne checks security for published business services in the same sequence that it checks security for all other JD Edwards EnterpriseOne objects—first by user, then role, and finally *PUBLIC. The system applies the first security record found. In addition, for the user, role, and *PUBLIC, the system checks for published business services security in this sequence:

- Published business service + method.
- Published business service.
- *ALL.

Note. Using *ALL to set up object security in Security Workbench is not related to the *ALL functionality that is used to sign into JD Edwards EnterpriseOne. *ALL in Security Workbench enables you to assign a user, role, or *PUBLIC to all objects of a particular type. *ALL during sign-in enables users to sign into JD Edwards EnterpriseOne with all the roles that have been assigned to them.

This illustration shows how the system checks for published business services security for a user signed in with *ALL and a user signed in with a specific role:



*Role 1 has the highest role sequence.

If a user is assigned to multiple roles and signs in as *ALL, the system uses role sequencing to determine which security record is used. A system administrator sets up role sequencing when setting up user and role profiles.

See Chapter 3, "Working with User and Role Profiles," Sequencing Roles, page 25.

Published Business Services Security Log Information

The log file provides administrators with information that you can use for troubleshooting business service security without revealing details that could possibly create a gap in the security.

When a web service attempts to access a published business service in JD Edwards EnterpriseOne, the system records the authorization information in the log file. If the logging level is set to "Debug," the log file records whether authorization was granted or denied. If the log level is set to "Severe," the system only logs information if the attempt to access a web service fails. This is an example of the information provided in the log file:

```
Access to <method name> in <published business service name> is <granted/denied>⇒
 for <user name> with <role name>.
```


See Also

Server Manager Guide for information on how to view business service security log file information.

JD Edwards EnterpriseOne Business Services Server Reference Guide for information on how to configure JD Edwards EnterpriseOne to authenticate users of published business services.

Reviewing the Current Published Business Services Security Records

You can use the Work With User/Role Security form in P00950 to review existing published business services security records. The query by example row of the grid enables you to display all security records for published business services. You can further narrow the search by locating the records for a user, role, or a particular published business service.

In addition, you can review published business services security records by running the Security Audit Reports—Security by Object (R009501) and Security by User/Role (R009502).

See Chapter 7, "Using Security Workbench," Running a Report that Lists Published Business Service Security Records, page 108.

From the Security Maintenance menu (GH9052), select Security Workbench (P00950).

1. On the Work with User/Role Security form, enter *S* in the Security Type column and then click Find.
2. To narrow the search by user or role, enter a user or role in the query by example field in the User / Role column and then click Find.
3. To view the security records for a particular published business service, complete the query by example field at the top of the Published BSSV column and then click Find.

Authorizing Access to Published Business Services

In P00950, you can create security records that allow a user, role, or *PUBLIC access to:

- A particular method in a published business service.
- A published business service.
- All published business services.

From the Security Maintenance menu (GH9052), select Security Workbench (P00950).

1. On Work with User/Role Security, select the Form menu, Set Up Security, Published BSSV.

   By default, *PUBLIC is in the User / Role field. If any records exist for *PUBLIC, those records appear in the grid.
2. On Published Business Service Security Revision, enter the user, role, or *PUBLIC to which you want to allow access to a published business service.
3. To allow access to a particular method in a published business service:
   a. On Published Business Service Security Revision, click the visual assist in the Published BSSV column to search for and select a published business service.
   b. On the same form, click the visual assist in the Published BSSV Method column to select the method that you want to allow access to.

      On Published BSSV Method, you must enter the published business service again in the Published BSSV column to see a list of all the methods for the published business service. The system displays published

business services by the method that is being exposed in the published business service. A published business service that contains multiple methods will have multiple rows in the grid, one for each method.

c. Select the row that contains the method that you want to secure and then click the Select button.

d. On Published Business Service Security Revision, click the visual assist in the Execute Allowed column and then select *Y* to allow access to the published business service method.

4. To allow access to a published business service (including all its methods):

   a. Click the visual assist in the Published BSSV column to search for published business services.

   b. On Select Business Service, complete the Business Service field and click the Find button.

   c. Select the published business service that you want to secure and then click the Select button.

   d. On Published Business Service Security Revision, in the row that contains the published business service, enter **ALL* in the Published BSSV Method column.

   e. In the same row, click the visual assist in the Execute Allowed column and then select *Y* to allow access to the published business service.

5. To allow access to all published business services:

   a. Enter **ALL* in the row under the Published BSSV column.

   b. Enter **ALL* in the row under the Published BSSV Method column.

   c. Click OK.

   d. In the same row, click the visual assist and then select Y to allow access to the published business services objects.

      By default, users are not allowed access to published business services objects in JD Edwards EnterpriseOne. However, you can select N to create a security override that disallows access to an object.

Adding Multiple Published Business Services Security Records at a Time

Security Workbench provides a form that you can use to add multiple published business services security records at a time.

From the Security Maintenance menu (GH9052), select Security Workbench (P00950).

1. On Work with User/Role Security, select the Form menu, Set Up Security, Published BSSV.
2. On Published Business Service Security Revision, from the Form menu, select Secure by Method.
3. On the Secure by Method form, enter the user, role, or *PUBLIC for which you want to set up published business services security, and then click the Find button.

   The system displays published business services by the method that is being exposed in the published business service. A published business service that contains multiple methods will have multiple rows, one for each method.
4. Use the query-by-example fields at the top of the grid to refine your search. For example, if you want to set up security for all methods that perform an add or delete, you search for those methods by typing *add** or *delete** in the Published BSSV Method query by example field in the grid.
5. Select the check box next to the items that you want to secure.
6. Click either the Allow Execute or Disallow Execute button.
7. On Confirm Batch Secure, click OK.

   The system displays the number of records that were added or updated.

Deleting Published Business Services Security

To delete published business services security records, you can use the same form that you used to authorize access to published business services.

In addition to this method, you can use the Work with User/Role Security form in P00950 to delete the records in the same way that you would delete any other object security record.

See Chapter 7, "Using Security Workbench," Deleting Security on the Work With User/Role Security Form, page 103.

From the Security Maintenance menu (GH9052), select Security Workbench (P00950).

1. On Work With User/Role Security, select the Form menu, Set Up Security, Published BSSV.
2. On Published Business Service Security Revision, enter the user, role, or *PUBLIC from which you want to delete a published business services security record and then click Find.
3. Click the check box next to the each record that you want to delete and then click the Delete button.
4. Click OK to confirm the delete.

Copying Security for a User or a Role

This section provides an overview of copying security for a user or a role and discusses how to:

- Copy all security records for a user or a role.
- Copy a single security record for a user or a role.

Understanding How to Copy Security for a User or a Role

You can copy the security information for one user or role, and then use this information for another user or role. When you copy security, you can either overwrite the current security for the user or role, or you can add the new security information to the existing security information. You can also copy all of the security records for a user or role, or you can copy one security record at a time for a user or role.

Copying All Security Records for a User or a Role

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, select the Form menu, and then select Copy Security.
2. Select one of these options:
   - Copy and Add

     When you copy and add security settings, you do not overwrite preexisting security for user or role.
   - Copy and Replace

     When you copy and replace security settings, the software deletes the security information for a user or role, and then copies the new security information from the selected user or role.
3. Complete these fields and click OK:
   - From User / Role

- To User / Role

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

Copying a Single Security Record for a User or a Role

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, locate a security record.
2. Select the security record row that you want to copy, and then click Copy.
3. Complete the To User / Role field and click OK.

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

Reviewing and Deleting Security Records on the Work With User/Role Security Form

This section provides an overview on how to review security records and discusses how to:

- Review security on the Work With User/Role Security form.
- Delete security on the Work With User/Role Security form.

Understanding How to Review Security Records

On the Work With User/Role Security form in P00950, you can review security records for a user or role based on security type, such as action, application, row, or any of the other types of security that can be added in P00950. The system displays all the security records for the user or role based on the security type that you select. For example, when you search for application security records for the AP Role, the system displays all the application security records for the AP role in the application grid.

The settings for each security type are displayed as columns in the grid. The columns that appear in the grid are based on the security type that you select. For example, application security provides two different levels of security: run and install. When you search for application security records, P00950 displays only the columns for Run and Install in the grid. However, action security contains several settings, such as OK/Select, Copy, Delete, OK, and so forth. When you search for action security records, the grid displays only columns for each of these security settings. The value in the column, either Y or N, indicates whether or not each setting is secured.

In addition, you can search on all security records of a particular security type. As a result, the system displays records for every user and role with the security type that was specified. You can search on all Security Workbench records by clicking the Find button.

Note. You can also review and delete security records on the form used to add a particular type of object security record, such as application, action, row, and so forth. Refer to the section on how to manage a particular type of object security for more information.

Reviewing Security on the Work With User/Role Security Form

Enter *P00950* in the Fast Path to access the Work With User/Role Security form..

1. On the Work With User/Role Security form, click Find.
2. To search for records by user or role, complete the User/Role field and then click Find.
3. To narrow the search by security type, click the Search button in the Security Type column to select a code and then click the Find button.

Deleting Security on the Work With User/Role Security Form

Enter *P00950* in the Fast Path.

1. On the Work With User/Role Security form, click Find.
2. To search for records by user or role, complete the User/Role field and then click Find.
3. To narrow the search by security type, click the Search button in the Security Type column to select a code and then click the Find button.
4. Select a record in the grid, and then click Delete.
5. On Confirm Delete, click OK.

   Security Workbench deletes the security record and refreshes the grid.

Running Security Workbench Records Reports

This section provides an overview of the Security Workbench Records reports and discusses how to:

- Run the Security Audit Report by Object version (R009501, XJDE0001).
- Run the Security Audit Report by User version (R009502, XJDE0001).
- Run the Security Audit Report by Role version (R009502, XJDE0002).

Understanding the Security Workbench Records Reports

JD Edwards EnterpriseOne provides two Security Workbench Records reports—Security by Object (R009501) and Security by User/Role (R009502)—that you can run to review the current security records by object type and user or role. The Security Workbench Records reports list security records for these objects:

- Interactive and batch applications.
- Tables (rows and columns).
- Published business services.

Before choosing which report to run, you should consider the data that you want the report to produce. Run the Security by Object report (R009501) to generate a report that lists the security records based on a particular object, object type, or product code. You can refine the data selection for this report to list only records for a particular user ID, role, or a combination of user ID and role. Run the Security by User/Role report (R009502) to generate a report that lists all the application, row, column, and published business service security records for a particular user ID, role, or *PUBLIC.

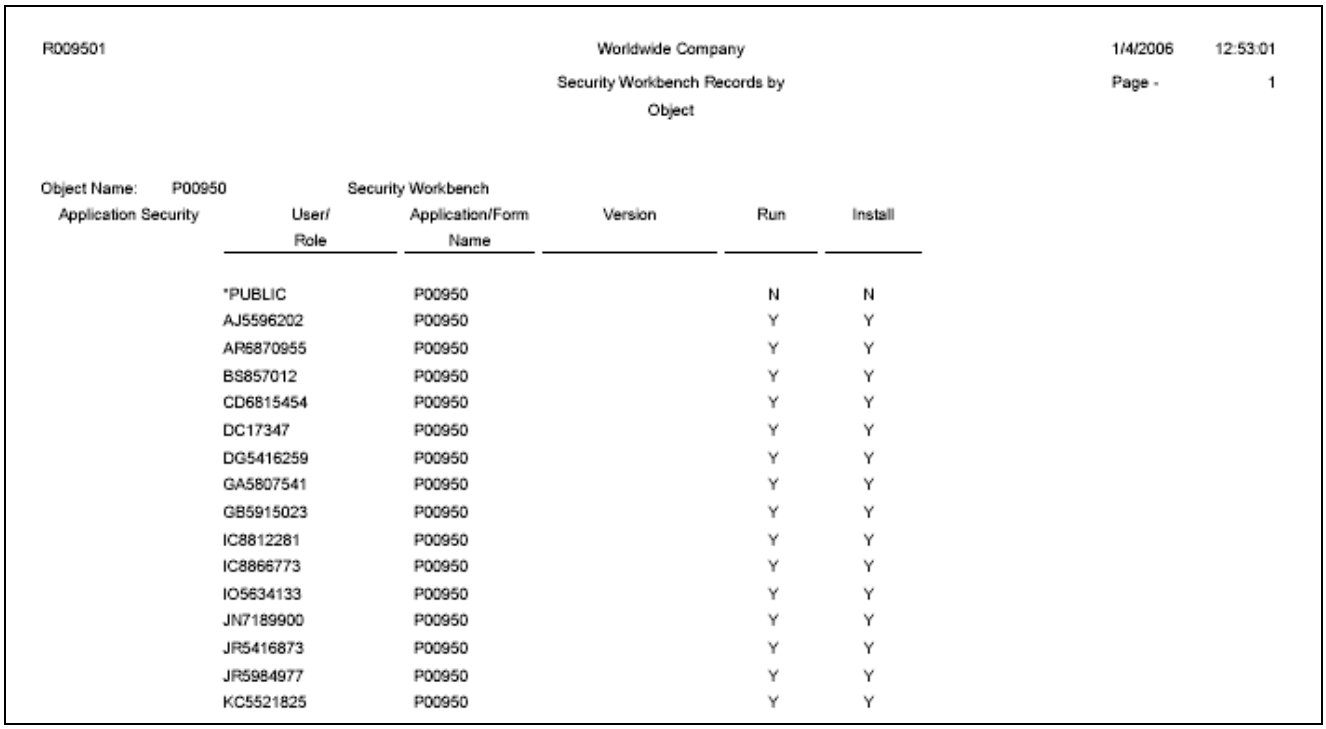
Each report contains processing options that you can use to define the output of the report. Along with the processing options, you can use the Data Selection form in the Batch Version program (P98305W) to further refine the data that the report produces.

Each security record in the report indicates the level of security, or type of security, that is applied to the object. For application security, each record indicates if a user or role has permission to install, run, or both install and run the application. For row security, each record indicates if view, add, change, or delete security have been applied. For column security, each record indicates if view, add, or change security have been applied. For published business service security, each record indicates whether a user or role has access to the published business service object.

How you set up your report determines how readily you can find gaps in your security plan. For example, if you have a highly sensitive application and you want to ensure that only the appropriate users have access to it, you can refine the R009501 report (Security Audit Report by Object) to list only the security records for that particular application.

Example of Security by Object Report (R009501)

This example shows the results of running the R009501 report. The report has been set up to list all the security records for the P00950 program.



R009501 Worldwide Company 1/4/2006 12:53:01
Security Workbench Records by Object Page - 1

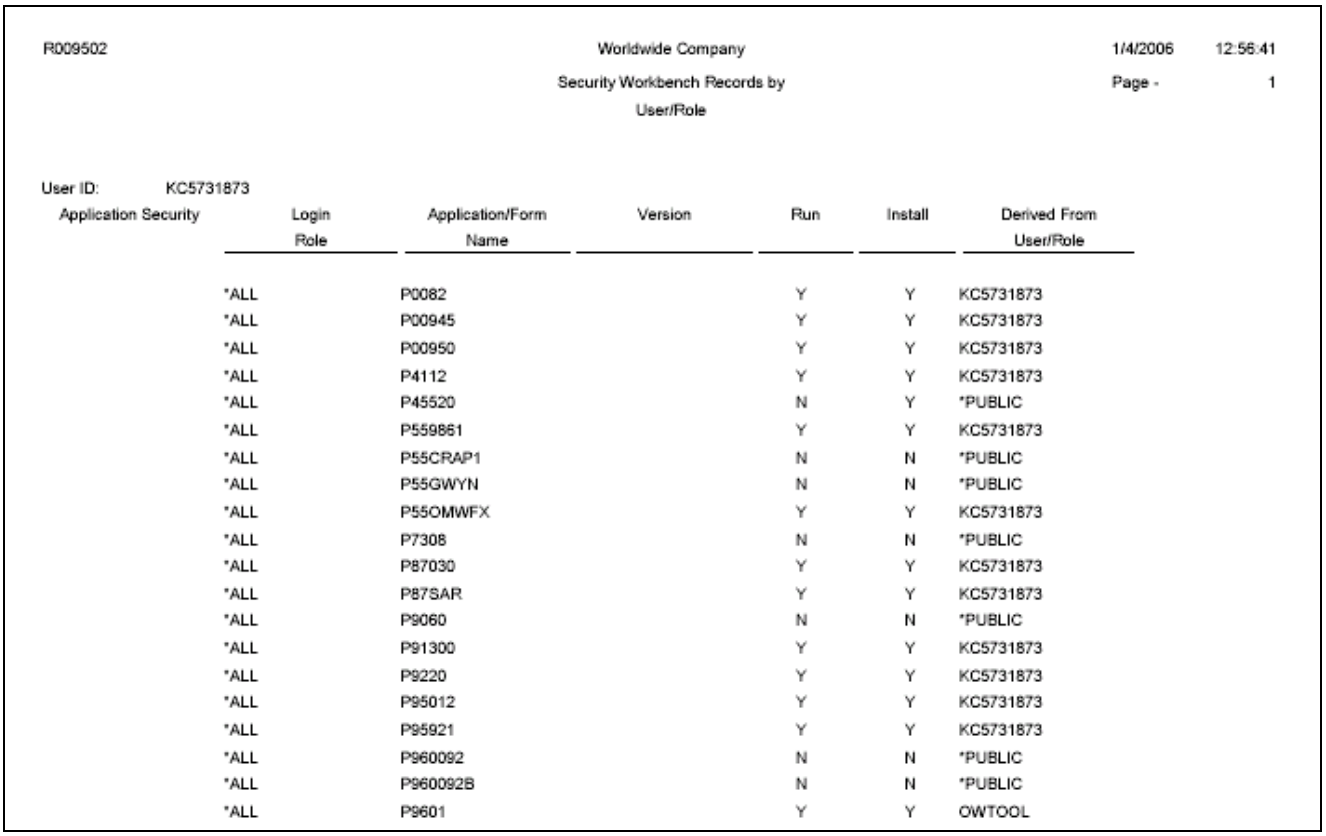
Object Name: P00950 Security Workbench

Application Security	User/ Role	Application/Form Name	Version	Run	Install
	*PUBLIC	P00950		N	N
	AJ5596202	P00950		Y	Y
	AR6870955	P00950		Y	Y
	BS857012	P00950		Y	Y
	CD6815454	P00950		Y	Y
	DC17347	P00950		Y	Y
	DG5416259	P00950		Y	Y
	GA5807541	P00950		Y	Y
	GB5915023	P00950		Y	Y
	IC8812281	P00950		Y	Y
	IC8866773	P00950		Y	Y
	IO5634133	P00950		Y	Y
	JN7189900	P00950		Y	Y
	JR5416873	P00950		Y	Y
	JR5984977	P00950		Y	Y
	KC5521825	P00950		Y	Y

Example of Security by Object Report.

Example of Security Audit Report by User (R009502, XJDE0001)

This example shows the results of running the Security Audit Report by User version of the R009502 report. The report lists the security records for a particular user in order of application, row, and then column. This example shows only the first page of the report, which lists the application security records for the user ID.



R009502 Worldwide Company 1/4/2006 12:56:41
Security Workbench Records by Page - 1
User/Role

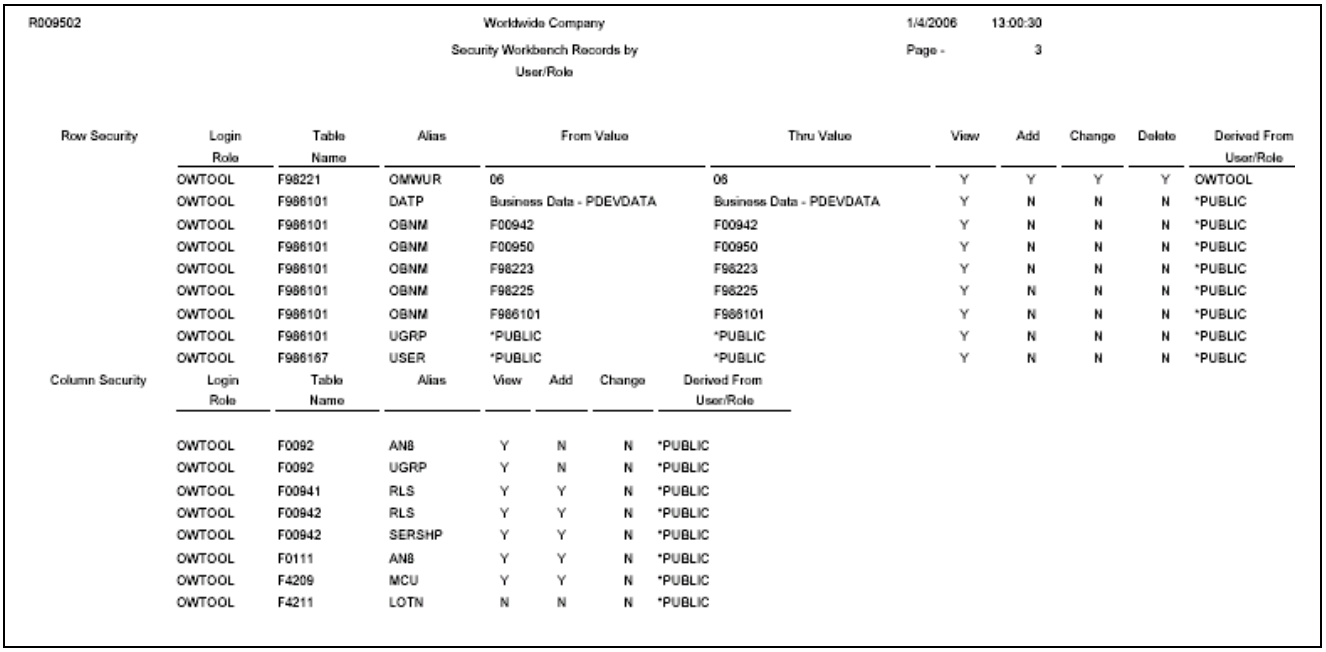
User ID: KC5731873

Application Security	Login Role	Application/Form Name	Version	Run	Install	Derived From User/Role
	*ALL	P0082		Y	Y	KC5731873
	*ALL	P00945		Y	Y	KC5731873
	*ALL	P00950		Y	Y	KC5731873
	*ALL	P4112		Y	Y	KC5731873
	*ALL	P45520		N	Y	*PUBLIC
	*ALL	P559861		Y	Y	KC5731873
	*ALL	P55CRAP1		N	N	*PUBLIC
	*ALL	P55GWYN		N	N	*PUBLIC
	*ALL	P55OMWFX		Y	Y	KC5731873
	*ALL	P7308		N	N	*PUBLIC
	*ALL	P87030		Y	Y	KC5731873
	*ALL	P87SAR		Y	Y	KC5731873
	*ALL	P9060		N	N	*PUBLIC
	*ALL	P91300		Y	Y	KC5731873
	*ALL	P9220		Y	Y	KC5731873
	*ALL	P95012		Y	Y	KC5731873
	*ALL	P95921		Y	Y	KC5731873
	*ALL	P960092		N	N	*PUBLIC
	*ALL	P960092B		N	N	*PUBLIC
	*ALL	P9601		Y	Y	OWTOOL

Example of Security Audit Report by User Report

Example of Security Audit Report by Role (R009502, XJDE0002)

This example shows the results of running the Security Audit Report by Role version of the R009502 report. The data selection of the report has been defined to list security records for the OWTOOL role. This example shows the third page of the report, which lists the row and column security records for the OWTOOL role.



R009502 Worldwide Company 1/4/2006 13:00:30
Security Workbench Records by Page - 3
User/Role

Row Security	Login Role	Table Name	Alias	From Value	Thru Value	View	Add	Change	Delete	Derived From User/Role
	OWTOOL	F98221	OMWUR	06	06	Y	Y	Y	Y	OWTOOL
	OWTOOL	F986101	DATP	Business Data - PDEVDATA	Business Data - PDEVDATA	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	OBNM	F00942	F00942	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	OBNM	F00950	F00950	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	OBNM	F98223	F98223	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	OBNM	F98225	F98225	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	OBNM	F986101	F986101	Y	N	N	N	*PUBLIC
	OWTOOL	F986101	UGRP	*PUBLIC	*PUBLIC	Y	N	N	N	*PUBLIC
	OWTOOL	F986167	USER	*PUBLIC	*PUBLIC	Y	N	N	N	*PUBLIC

Column Security	Login Role	Table Name	Alias	View	Add	Change	Derived From User/Role
	OWTOOL	F0092	AN8	Y	N	N	*PUBLIC
	OWTOOL	F0092	UGRP	Y	N	N	*PUBLIC
	OWTOOL	F00941	RLS	Y	Y	N	*PUBLIC
	OWTOOL	F00942	RLS	Y	Y	N	*PUBLIC
	OWTOOL	F00942	SERSHP	Y	Y	N	*PUBLIC
	OWTOOL	F0111	AN8	Y	Y	N	*PUBLIC
	OWTOOL	F4209	MCU	Y	Y	N	*PUBLIC
	OWTOOL	F4211	LOTN	N	N	N	*PUBLIC

Example of Security Audit Report by Role

Run the Security Audit Report by Object Version (R009501, XJDE0001)

Access the Work With Batch Versions - Available Versions form. To do so, enter *P98305W* in the Fast Path.

1. In the Batch Application field, enter *R009501* and click the Find button.
2. Select the Security Audit Report by Object version.
3. To define processing options for the report, select Processing Options from the Row menu, and then complete the processing options as appropriate:
   - User ID or Role (optional)

     Enter a user ID or role to refine the report to generate only records based on that particular user ID or role.
   - Report on Application Security

     Leave blank if you want the report to include application security records. Enter *1* to exclude application security records.
   - Report on Row Security

     Leave blank if you want the report to include row security records. Enter *1* to exclude row security records.
   - Report on Column Security

     Leave blank if you want the report to list application security records. Enter *1* to exclude application security records.
   - Report on Published BSSV Security

     Leave blank if you want the report to list published business service security records. Enter *1* to exclude published business service security records.

   Note. In addition, to generate a report that displays published business service security records, you need to add an additional condition in the Data Selection form, as discussed below.

   ---
4. On the Work With Batch Versions - Available Versions form, click Select.
5. On the Versions Detail form, select the Data Selection check box and click the Submit button.
6. On the Data Selection form, you can add a condition to filter on a particular object, object type, or product code.

   If the processing option is set to list published business service security records, you must add the following condition after the default `Where` condition:

   ```
   And BC Source Language (F9860) (SRCLNG) [BC] is equal to "SBF"
   ```
7. Click the OK button.
8. On the Printer Selection form, define the location for the output of the report and then click OK to submit it.

Run the Security Audit Report by User Version (R009502, XJDE0001)

Access the Work With Batch Versions - Available Versions form. To do so, enter *P98305W* in the Fast Path.

1. In the Batch Application field, enter *R009502* and click the Find button.
2. Select the Security Audit Report by User version.
3. To define processing options for the report, select Processing Options from the Row menu, and then complete the processing options as appropriate:
   - Role (optional)

     To refine the report to generate only records based on a particular role of the user, enter a role.
   - Report on Application Security

     Leave blank if you want the report to include application security records. Enter *1* to exclude application security records.
   - Report on Row Security

     Leave blank if you want the report to include row security records. Enter *1* to exclude row security records.
   - Report on Column Security

     Leave blank if you want the report to list column security records. Enter *1* to exclude column security records.
   - Report on Published BSSV Security

     Leave blank if you want the report to list published business service security records. Enter *1* to exclude published business service security records.
4. On the Work With Batch Versions - Available Versions form, click Select.
5. On the Versions Detail form, select the Data Selection check box and click the Submit button.
6. On the Data Selection form, use the User ID left operand to define the user ID that you want the report to list security records for.
7. Click OK.
8. On the Printer Selection form, define the location for the output of the report and then click OK to submit it.

Run the Security Audit Report by Role Version (R009502, XJDE0002)

Access the Work With Batch Versions - Available Versions form. To do so, enter *P98305W* in the Fast Path.

1. In the Batch Application field, enter *R009502* and click the Find button.
2. Select the Security Audit Report by Role version.
3. To define processing options for the report, select Processing Options from the Row menu, and then complete the processing options as appropriate:
   - Role (optional)

     Do not use this option for this report. Instead, enter the role in the Data Selection form.

- Report on Application Security

  Leave blank if you want the report to include application security records. Enter 1 to exclude application security records.

- Report on Row Security

  Leave blank if you want the report to include row security records. Enter 1 to exclude row security records.

- Report on Column Security

  Leave blank if you want the report to list application security records. Enter 1 to exclude application security records.

- Report on Published BSSV Security

  Leave blank if you want the report to list published business service security records. Enter *1* to exclude published business service security records.

4. On the Work With Batch Versions - Available Versions form, click Select.
5. On the Versions Detail form, select the Data Selection check box and click the Submit button.
6. On the Data Selection form, use the User ID left operand to define the role that you want the report to list security records for.
7. Click OK on the Data Selection form.
8. On the Printer Selection form, define the location for the output of the report and then click OK to submit it.

Running a Report that Lists Published Business Service Security Records

You can use the Security Workbench Records reports to generate a list of published business service security records by object, user, or role. However, before you run the report, you must use the Data Selection form to specify the published business service object type.

Access the Work With Batch Versions - Available Versions form. To do so, enter *P98305W* in the Fast Path.

1. In the Batch Application field, enter either *R009501*or *R009502* and click the Find button.
2. Select the version of the report that you want to run.
3. On the Work With Batch Versions - Available Versions form, click Select.
4. On the Versions Detail form, select the Data Selection check box and click the Submit button.
5. On the Data Selection form, enter these conditions and then click OK:

   ```
   Where BC Object Type (F9860) (FUNO) is equal to "BSFN"
   And BC Source Language (F9860) (SRCLNG) [BC] is equal to "SBF"
   ```

6. On the Printer Selection form, define the location for the output of the report and then click OK to submit it.

CHAPTER 8

Setting Up Address Book Data Security

This chapter provides an overview of Address Book data security, lists prerequisites, and discusses how to:

- Set up permission list definitions.
- Set up permission list relationships.

Understanding Address Book Data Security

The Address Book data security feature enables you to restrict users from viewing address book information that you have determined is personal. After performing the required setup for this feature, secured users can see the fields that you specify as secured, but the fields are filled with asterisks and are disabled. You can set up data security for these fields:

- Tax ID
- Addl Ind Tax ID (additional tax ID)
- Address

  Includes Address Lines 1-7, City, State, Postal Code, Country, and County.
- Phone Number

  Includes phone number and phone prefix.
- Electronic Address

  Includes only electronic addresses with Type E.
- Day of Birth, Month of Birth, and Year of Birth.
- Gender

Note. In addition to these fields, the system enables you to designate up to eight other user-defined fields as secured. Included in the eight fields are: five string, one math numeric, one character, and one date type. To secure additional fields, you must modify the parameter list in the call to the business function B0100095. For example, if you want to designate Industry Class as a secured field, you must modify the call to the B0100095 business function to map Industry Class in the parameter list.

The Address Book data security feature provides an additional level of security by not allowing secured users to locate valid personal information using the query based example (QBE) line. For example, if a user enters numbers in the Tax ID field of the QBE line, the system does not display the matching record in the event that the user happens to enter a valid tax ID number.

Setting up Address Book data security involves these steps:

1. Selecting the Activate Personal Data Security constant in the Address Book Constants.

Personal data security is inactive unless the Activate Personal Data Security constant is selected.

2. Setting up permission list definitions.

   Use the Address Book Data Permissions program (P01138) to create one or more permission lists that specify which fields in the Address Book are secured.

3. Setting up permission list relationships.

   Use the Permission List Relationships program (P95922) to determine the users or roles that are subject to each permission list.

Once you have set up Address Book data security, keep in mind that users can still view their own address book information, and secured fields are not protected under these circumstances:

- Adding new Address Book records.
- Running reports that contain the secured fields.
- Viewing records in the Universal Table Browser (UTB).

You can set up data security for any other system within JD Edwards EnterpriseOne. To use the data security feature for another system, you must create new programs and related tables for permission list definitions.

Prerequisites

Select the Activate Personal Data Security constant in the Address Book Constants.

See Setting Up the Address Book System in the *JD Edwards EnterpriseOne 8.12 Address Book Guide.*

Set up users and roles in the User Profiles program (P0092) for each user that you want to secure from Address Book information.

See Chapter 3, “Working with User and Role Profiles,” Setting Up User Profiles, page 9.

Setting Up Permission List Definitions

This section provides an overview of permission list definitions and discusses how to set up permission list definitions.

Understanding Permission List Definitions

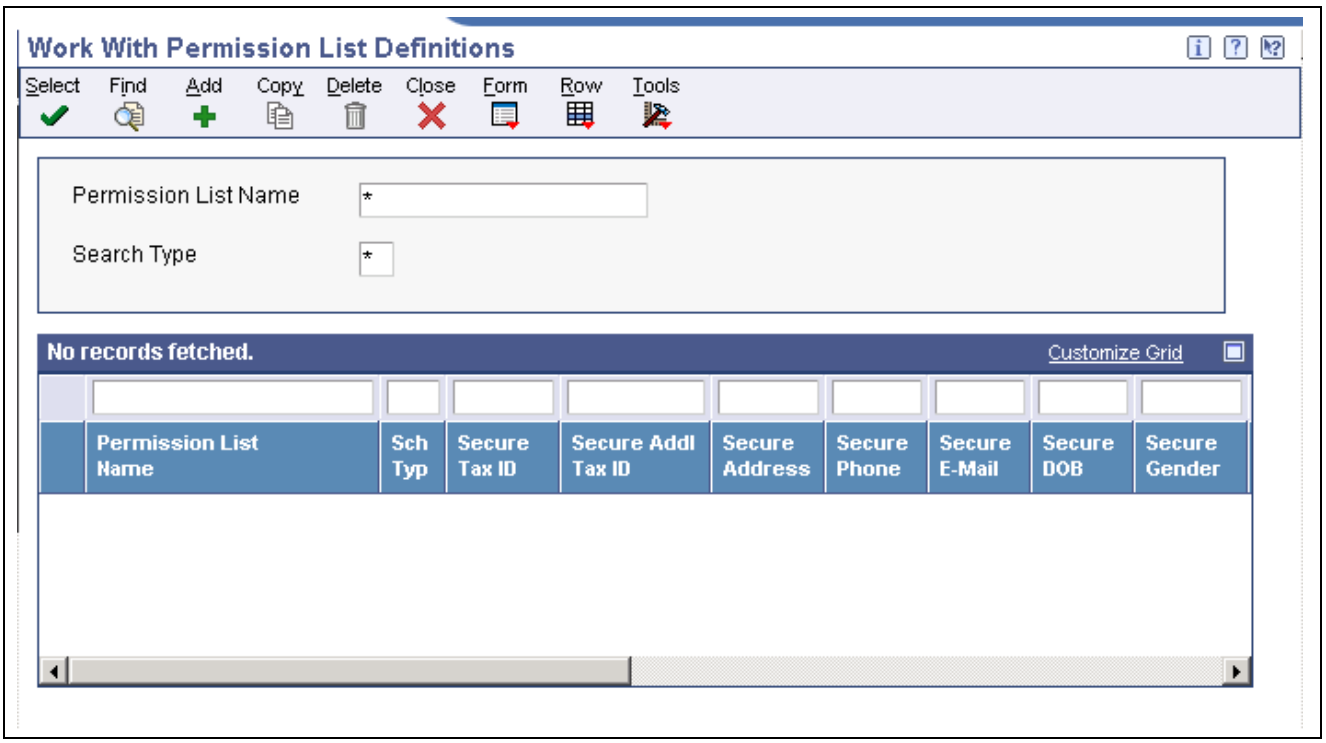
The Permission List Definition program enables you to create multiple lists that determine which Address Book fields are secure. When you create permission lists, you specify a permission list name and a search type, and then select each field that you want to secure. The system stores permission list definitions in the F01138 table.

Forms Used to Set Up Permission List Definitions

Form Name	FormID	Navigation	Usage
Work With Permission List Definitions	W01138A	• Permission List Management (JDE029160), Address Book Data Permission • Enter *P01138* in the Fast Path.	Review existing permission list definitions.
Add/Edit Permission List Definitions	W01138B	Select Add from the Work With Permission List Definitions form.	Create new permission list definitions or revise existing definitions.

Creating Permission List Definitions

Access the Add/Edit Permission List Definitions form.



Add/Edit Permission List Definitions form

After entering the Permission List Name and the Search Type, select each field that you want to secure.

Permission List Name Enter a name for the permission list. Enter up to 15 alphanumeric characters.

Search Type Select the search type for which the permission list applies.

Setting Up Permission List Relationships

This section provides an overview of permission list relationships and discusses how to set up permission list relationships.

Understanding Permission List Relationships

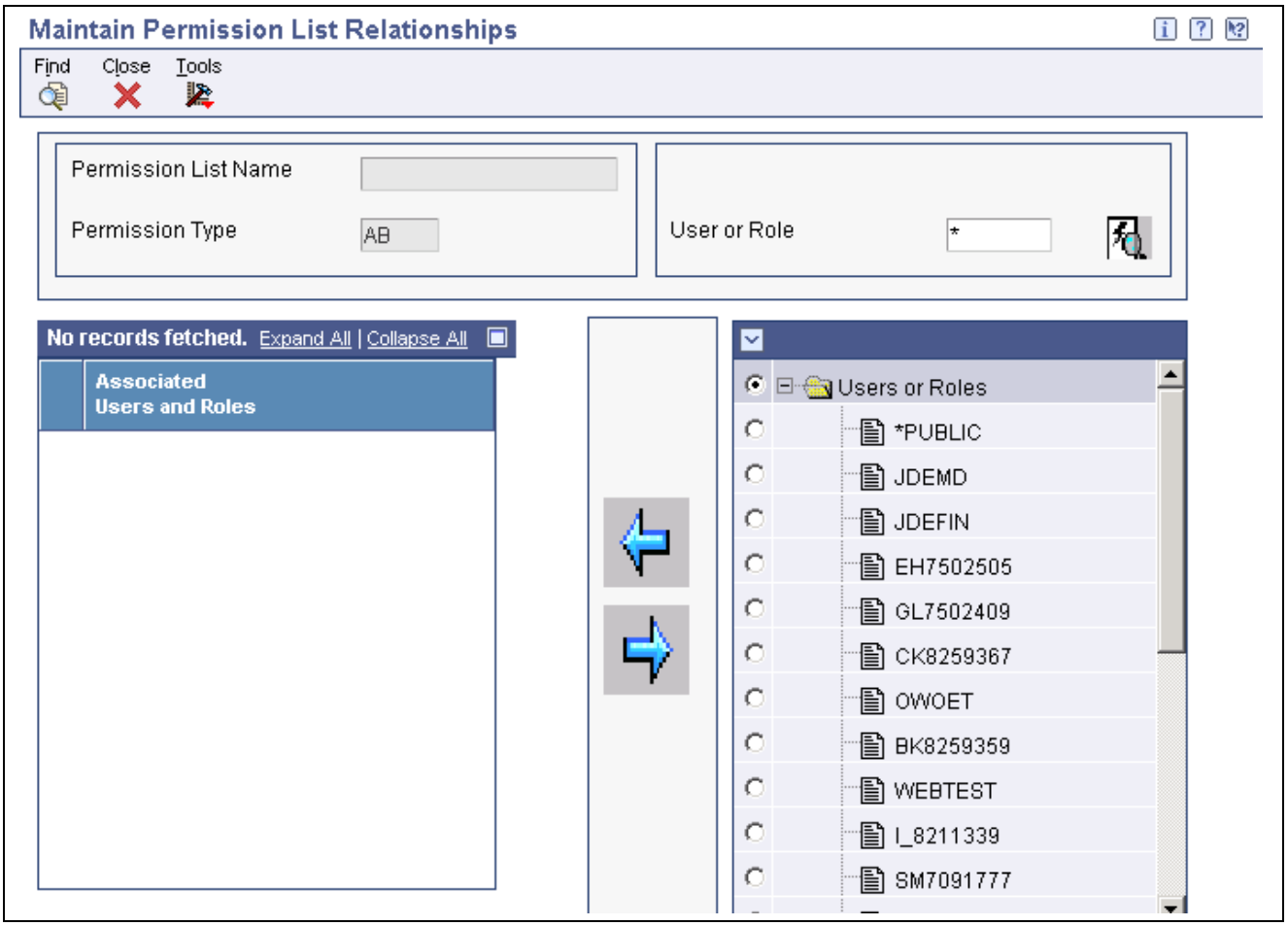
After you set up permission list definitions, use the Permission List Relationships program to assign them to previously defined user IDs and roles. You can attach a user ID or role to only one permission list. The system stores permission list relationships in the F95922 table.

Forms Used to Create Permission List Relationships

Form Name	FormID	Navigation	Usage
Work With Permission List Relationships	W95922A	• Permission List Management (JDE029160), Work With Permission List Relationships • Enter *P95922* in the Fast Path.	Search for a permission list.
Maintain Permission List Relationships	W95922D	Click Select on the Work With Permission List Relationships form.	Set up permission list relationships.

Creating Permission List Relationships

Access the Maintain Permission List Relationships form.



Maintain Permission List Relationships form

User or Role Enter the User ID or Role that you want to attach to a permission list.

Click the Find.gif button after entering a value in the User or Role field.

Click the right_arrow.gif button to attach a User ID or Role to a permission list.

Click the left_arrow.gif button to remove a User ID or Role from a permission list.

CHAPTER 9

Setting Up Business Unit Security

This chapter provides an overview of business unit security and discusses how to:

- Work with user defined code (UDC) sharing.
- Work with transaction security.

Understanding Business Unit Security

JD Edwards EnterpriseOne business unit security provides the ability to filter data by business unit for UDCs and for transaction tables. For UDCs, you create subgroups of values that can be shared among various business units or may be unique to one particular business unit. This is referred to as UDC sharing. For transaction tables, business unit security enables you to limit the transaction records that a user has access to based on business unit. This is called transaction security.

UDC Sharing

With UDC sharing, JD Edwards EnterpriseOne provides the ability to control, or regulate, how organizational data among different business units is shared. UDC sharing enables you to define a subset of UDC values for a business unit. You can share multiple UDC values among multiple business units.

For example, a company's customer service department may provide support for appliances, consumer electronics, and sporting goods. Typically, a representative would choose from an extensive list of values to specify the repair code for a particular type of product. However, with UDC sharing, the company can associate a subset of the repair code UDC values, such as for appliances, to a business unit. As a result, the representatives associated with the business unit would only have to choose from a list of repair codes relevant to appliances.

Note. UDC sharing can impact system performance because of the time it takes the system to determine the UDC values that are associated with each business unit.

Transaction Security

Another feature of JD Edwards EnterpriseOne business unit security is transaction security. Transaction security enables you to determine the transaction records a user can view. Transaction security ensures that users can only access and modify transaction data for the business unit to which they are associated.

See Also

Setting Up Business Units in the JD Edwards EnterpriseOne Financial Management Solutions Application Fundamentals Guide.

Working with UDC Sharing

This section provides overviews of the UDC sharing setup and business unit security for UDC sharing and discusses how to:

- Set up UDC sharing.
- Set up business unit security for UDC sharing.
- Revise a UDC group.
- Delete a UDC group.

Understanding the UDC Sharing Setup

Use the UDC Sharing application (P95130) to set up UDC sharing. This wizard-like program leads you through the appropriate tasks to configure these items:

- UDC group

  A UDC group serves as a container for the UDC values that you want to share among different business units. You create the UDC group by naming it and assigning the UDC types that contain UDC values. For example, if you are sharing UDC values that represent various states and countries in geographic regions, you might name the UDC group GEO, and then assign the UDC types that contain the appropriate UDC values for the states or countries.

- Set-ID

  A set-ID enables you to further categorize the UDC values within a UDC group. For example, you can further categorize the UDC values in the GEO UDC group into subsets, such as Europe, Canada, Pacific Rim, and so forth. Each subset, or set-ID, can contain values that are specific to that region.

Understanding Business Unit Security for UDC Sharing

JD Edwards EnterpriseOne provides a wizard-like program to assist you with setting up business unit security for UDC sharing. The program leads you through these tasks:

- Define a business unit type.

  A business unit type serves as a logical grouping of business units. To define it, you give it a name and then specify the table (typically the F0006 table) and the data item within the table that contains the business unit values.

- Associate a user ID or role to a business unit.

  Note. You can associate users to business units when setting up UDC sharing or when setting up transaction security.

- Associate a UDC group to a business unit.

Setting Up UDC Sharing

Enter *GH9052* in the Fast Path, select Business Unit Security, and then select Set-up UDC Sharing to access the UDC Group Revisions form.

Note. You can access this form on the Microsoft Windows client and the web client.

1. Complete these fields to name and describe the UDC group:
   - UDC Group
   - Group Description
2. In the detail area, click the search button in these fields to add UDC types to the UDC group:
   - Product Code

     Select the product code of the UDC type that you want to add.
   - User Defined Code

     Select the UDC type that contains the values for the UDC group.

     Note. A UDC type cannot be associated with more than one UDC group.
3. Click Next.
4. On Set-ID Definition Revisions, complete these fields to create set-IDs for the UDC group:
   - Set-ID

     Enter a name for the set-ID.
   - Description
5. Click Next.

   On Maintain Set-ID, in the right pane, the system displays the UDC types that you assigned to the UDC group. The left pane contains the set-IDs that you defined for the UDC group.
6. Assign UDC values to the Set-IDs.
   a. Select a set-ID in the left pane.
   b. Click a UDC type in the right pane, and then select from the list of UDC values.
   c. Click the left arrow to assign the UDC value to the chosen Set-ID.
7. After you assign UDC values to the set-IDs, click Done.

Setting Up Business Unit Security for UDC Sharing

Enter *GH9052* in the Fast Path, double-click Business Unit Security, and then select Set-up Business Unit Security to access the Business Unit Security Definition Revisions form.

1. Complete these fields in this order:
   - Business Unit Type
   - Business Unit Definition Table

     Enter the table object name that contains the individual business unit values (for example, F0006).
   - Business Unit Definition Data Item

     Enter the data item in the Business Unit Definition Table that contains the unique business unit name (for example, MCU).
2. Press TAB and then click Next to continue.

3. On User/Role to Business Unit Relationships, assign the users or roles in the right panel to the appropriate business units in the left panel.

   You can search for particular business unit values and users or roles by clicking the search button next to the Business Unit Value and User/Role fields, respectively.

   Note. You can click the Skip button if you choose not to perform this step at this time. You can also assign users to business units when setting up transaction security.

4. After securing users to the appropriate business units, click Next to continue.
5. On Maintain Transaction Security Tables, click the Skip button.

   This form is only used for transaction security.
6. On UDC Group/Set-ID/Business Unit Relationship, assign the set-IDs within the UDC groups to the appropriate business units in the left panel.

   You can search for particular business unit values and UDC groups by clicking the search button next to the Business Unit Value and UDC Group fields, respectively.

   Remember that you must first configure UDC sharing to be able to assign set-IDs to business units on this form.
7. Click Done.

Revising UDC Groups

Enter *GH9052* in the Fast Path, double-click Business Unit Security, and then select Maintain UDC Sharing to access the Work With UDC Sharing form.

You can access this form in the Microsoft Windows client and the web client.

1. Select the UDC group that you want to revise.
2. To add or delete a UDC type in a UDC group, from the Row menu, select Group Revisions.
3. To add or delete a set-ID, from the Row menu, select Set-ID Definition.

   Note. You cannot delete a set-ID that is part of a business unit and UDC group relationship.

4. To revise the UDC values that are assigned to the set-IDs, from the Row menu, select Maintain Set-ID.

Deleting a UDC Group

On the Work With UDC Sharing form, select the UDC group and then click Delete.

Note. You cannot delete a UDC group that is part of a business unit relationship.

Working with Transaction Security

This section provides an overview of how to set up transaction security and discusses how to:

- Set up transaction security.
- Set processing options for Maintain Business Unit Transaction Security (R95301).
- Set processing options for Business Unit Security Maintenance application (P95300).

- Revise transaction security.

Understanding How to Set Up Transaction Security

Transaction security enables you to define which transaction records a user can access, based on the business units they are associated with. Transaction security for business units is inclusive, which means that you define which transactions users can access based on the business unit to which the user ID or role is associated. To set up transaction security, you must define these items:

- Business unit type.

  A business unit type serves as a logical grouping of business units. To define it, you name it and then specify the table (typically the F0006 table) and the data item within the table that contains the business unit values.

  Note. If you are setting up transaction security for an existing business unit type, use the Maintain Business Unit Security menu to add transaction security.

- Tables to include in a transaction security definition.
- Users associated with the business units.

The application that you use to set up transaction security, the Business Unit Security Maintenance program (P95300), is available in two modes: a mode that you can use for the initial transaction security setup and another mode to revise transaction security. The mode for the initial setup uses a director or wizard-like process to lead you through the P95300 application forms used to set up transaction security.

See Chapter 9, "Setting Up Business Unit Security," Setting Up Transaction Security, page 120.

The mode to revise transaction security provides access to the same forms that are used for the initial setup, but without the wizard functionality. You can use these forms to add, update, or delete transaction security.

See Chapter 9, "Setting Up Business Unit Security," Revising Transaction Security, page 121.

Generating Transaction Security Records

When you set up or revise transaction security, JD Edwards EnterpriseOne does not automatically enable transaction security in the software. The new or revised transaction security records must be added to the Security Workbench table (F00950). JD Edwards EnterpriseOne provides different mechanisms for updating transaction security records in the F00950 table, depending on whether you are performing an initial setup of transaction security or revising transaction security.

After you perform an initial setup, you must run the Maintain Business Unit Transaction Security batch application (R95301) to generate the transaction security records. You can set processing options for this batch application that enable you to review the records in a "proof" mode before the records are updated in the F00950 table.

See Chapter 9, "Setting Up Business Unit Security," Setting Processing Options for Maintain Business Unit Transaction Security (R95301), page 120.

If you are revising transaction security, you can set processing options to control how the transaction security records are updated in the F00950 table. You can set these processing options on the Maintain Business Unit Security menu, which is the JD Edwards EnterpriseOne menu that launches the forms used for revising transaction security.

See Chapter 9, "Setting Up Business Unit Security," Setting Processing Options for Business Unit Security Maintenance Application (P95300), page 121.

Note. The data in the F00950 table is cached. Therefore, you must restart the server to clear the cache in order for the updated security records to take affect.

Setting Up Transaction Security

Access the Business Unit Security Definition Revisions form. Enter *GH9052* in the Fast Path, and then select Business Unit Security , Set-up Business Unit Security.

1. On the Business Unit Security Definition Revisions form, complete these fields in order:
   - Business Unit Type
   - Business Unit Definition Table

     Enter the table object name that contains the individual business unit values (for example, F0006).
   - Business Unit Definition Data Item

     Enter the data item in the Business Unit Definition Table that contains the unique business unit name (for example, MCU).
2. Press TAB and then click Next to continue.
3. On User/Role to Business Unit Relationships, assign the users or roles in the right panel to the appropriate business units in the left panel.

   You can search for particular business unit values and users or roles by clicking the search button next to the Business Unit Value and User/Role fields, respectively.
4. After securing users to the appropriate business units, click Next to continue.
5. On Maintain Transaction Security Tables, complete these columns in the grid:
   - Transaction table

     Enter the table name that contains the data item that you want to secure.
   - Data item

     Enter the data item of the column that you want to secure.

     You can use this form to secure multiple tables.
6. Click Next to continue.
7. On UDC Group/Set-ID/Business Unit Relationship, click Done.

Setting Processing Options for Maintain Business Unit Transaction Security (R95301)

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

Transaction Security

These processing options are used to specify how the system processes the transaction security records.

1. Add Transaction Security Records	Specify whether to run the report in Final mode or Proof mode. Use the Proof mode to generate a report of the transaction security records that will be updated in the Security Workbench table (F00950). Use the Final mode to update the records.
2. Add Transaction Security Records	Specify whether to add or to not add transaction security records. Values are: 1: Add 0: Do not add
3. Delete Transaction Security Records	Specify whether to delete or to not delete transaction security records. Values are: 1: Delete 0: Do not delete

Setting Processing Options for Business Unit Security Maintenance Application (P95300)

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

You can access these processing options from the JD Edwards EnterpriseOne Menu by right-clicking the Maintain Business Unit Security menu , and then selecting Prompt for Values.

Mode

This processing option is used to specify the business unit security mode.

1. Business Unit Security Mode	Specify whether to run the report in Director Mode (A) or Maintenance Mode (D).

Transaction Security

These processing options are used when working with business unit security in Maintenance mode only.

1. In Maintenance mode, automatically add transaction security records.	Specify whether to automatically add transaction security records. Values are: 1: Add 0: Do not add
2. In Maintenance mode, automatically delete transaction security records.	Specify whether to automatically delete transaction security records. Values are: 1: Delete 0: Do not delete

Revising Transaction Security

Access the Work With Business Unit Security form. Enter *GH9052* in the Fast Path, and then select Business Unit Security, Maintain Business Unit Security.

1. On the Work With Business Unit Security form, select the business unit security type record that you want to revise.
2. To revise the users or roles associated to a business unit, from the Row menu, select Associate User/Role.
3. To revise the UDC values that are assigned to business units, from the Row menu, select UDC Groups for BU.
4. To revise a transaction table record, from the Row menu, select Transaction Tables.
5. To delete transaction security for a business unit type, select the record and then click Delete.

CHAPTER 10

Setting Up Application Failure Recovery

This chapter provides an overview of application failure recovery and discusses how to:

- Assign an administrator for the application failure recovery applications.
- Grant user access to failed application data.

Understanding Application Failure Recovery

JD Edwards EnterpriseOne enables web client users to recover data from failed applications due to:

- Catastrophic errors
- Transaction failures
- Session time outs
- Voluntary exits

The Application Failure Recovery program (P95400) enables users to access and recover data from any failed transaction in which they are involved. Using P95400, users can save and copy the data from failed transactions back into the appropriate application to complete the transaction. However, users must be granted permission by an administrator to recover data from applications other than their own. For example, an administrator might give a sales department supervisor the permission to recover data from transactions performed by other users in the department.

To set up application failure recovery, you must first use the Application Failure Administration program (P95410) to assign an application failure administrator. The administrator can grant users permission to recover failed application data from application transactions entered by other users. You can grant this permission to a user, role, or all users.

See Also

JD Edwards EnterpriseOne Tools 8.97 Foundation Guide, "Using JD Edwards Web Applications and Reports," Recovering Data

Prerequisites

Use the Security Workbench program (P00950) to secure P95410 to system administrators only.

See Chapter 7, "Using Security Workbench," Managing Application Security, page 68.

You must configure the AppRecovery setting in the [OWWEB] section of the jas.ini file for the system to save the data from a failed application.

See *JD Edwards EnterpriseOne Tools 8.97 HTML Web Server Reference Guide*

Assigning an Administrator for the Application Failure Recovery Applications

Use P95410 to assign an administrator for the application failure recovery applications.

In the JD Edwards EnterpriseOne web client, enter *P95410* in the Fast Path to access the Work with Application Failure Administrators form.

1. Click Add.
2. On Add Application Failure Administrator, in the User field, enter the user ID of the individual that you want to assign as administrator, and then click OK.

Granting User Access to Failed Application Data

In the JD Edwards EnterpriseOne web client, enter *P95400* in the Fast Path to access the Work with Application Failure Records form.

1. From the Form menu, select Time Out Subscriptions.
2. On the Work with Time Out Subscriptions form, click Add.
3. On the Add Time Out Subscription form, in the User field, enter the user ID or role that you want to permit access to the failed application data. Enter **Default* to allow access to all users.
4. In the Application Name field, enter the application that the user or role can recover data from.

CHAPTER 11

Enabling LDAP Support in JD Edwards EnterpriseOne

This chapter provides an overview of Lightweight Data Access Protocol (LDAP) support in JD Edwards EnterpriseOne and discusses how to:

- Configure LDAP support in JD Edwards EnterpriseOne.
- Modify the LDAP default user profile settings.
- Use LDAP Bulk Synchronization (R9200040).
- Use LDAP over SSL.
- Export user data to the LDAP server.

Important! This chapter does not provide instructions for installing and configuring an LDAP-compliant directory service, such as Microsoft Windows Active Directory or IBM Directory Server. For more information, refer to the Prerequisites section in this chapter.

Understanding LDAP Support in JD Edwards EnterpriseOne

This section discusses:

- LDAP support overview.
- User Profile Management in LDAP-Enabled JD Edwards EnterpriseOne
- LDAP and JD Edwards EnterpriseOne relationships.
- Application changes in LDAP-enabled JD Edwards EnterpriseOne.
- LDAP server-side administration.
- JD Edwards EnterpriseOne server-side administration.

LDAP Support Overview

LDAP is an open industry standard protocol that directory services use to manage user profiles, such as user IDs and passwords, across multiple application systems. You can enable JD Edwards EnterpriseOne to use an LDAP-compliant directory service to manage JD Edwards EnterpriseOne user profiles and user-role relationships. After enabling JD Edwards EnterpriseOne for LDAP, user profiles can be administered through an LDAP version 3 compliant directory server, otherwise referred to as the LDAP server. System administrators use a third-party LDAP-enabled application to access the LDAP server.

LDAP provides these benefits:

- Central administration and repository for user profiles.

  You can easily maintain user profiles in a single location that serves multiple end user applications, including JD Edwards EnterpriseOne applications.

- Reduced complexity.

  You are not required to use several applications to maintain user profiles. In addition, users are not required to maintain multiple passwords across multiple systems.

Note. LDAP support does not address single sign-on functionality that might exist through other JD Edwards EnterpriseOne functionality.

User Profile Management in LDAP-Enabled JD Edwards EnterpriseOne

When JD Edwards EnterpriseOne is enabled for LDAP, the features used to manage user profiles in the User Profile Revisions application (P0092) are disabled. Instead, you must use a third-party, LDAP-enabled application to manage JD Edwards EnterpriseOne user profiles.

Note. JD Edwards EnterpriseOne does not provide an application for managing LDAP user profiles.

Additionally, JD Edwards EnterpriseOne provides a self-service version of P0092. This self-service application is used to manage only self-service user profile information for the Manufacturing Sourcing module; not JD Edwards EnterpriseOne user profiles. However, if you are enabling JD Edwards EnterpriseOne for LDAP and your company is using this self-service application, you can add parameters for it when you define the LDAP server settings. In this configuration, any self-service user profiles that are added are synchronized with the LDAP server.

Note. Even though self-service user profiles are synchronized with the LDAP server, you cannot use this self-service application to manage JD Edwards EnterpriseOne or LDAP user profiles.

See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Configuring the LDAP Server Settings, page 139.

LDAP and JD Edwards EnterpriseOne Relationships

The LDAP system administrator must understand the logical and database-dependent relationships between the LDAP server and JD Edwards EnterpriseOne. The administrator directly or indirectly controls the logical flow of events and where specific data resides based on the setting of system variables in the JD Edwards EnterpriseOne enterprise server jde.ini file and settings specified in the LDAP Server Configuration Workbench program (P95928).

The security kernel on the JD Edwards EnterpriseOne enterprise server is responsible for ensuring the integrity of the security within JD Edwards EnterpriseOne. If this kernel is not running correctly or cannot locate requisite data, users cannot sign in to JD Edwards EnterpriseOne. However, when the security kernel is properly configured, the system verifies the user credentials from data within the user profiles. In this case, the following two scenarios are possible:

- You can configure JD Edwards EnterpriseOne to use LDAP to manage user profiles.
- You can configure JD Edwards EnterpriseOne to use LDAP to manage user-role relationship data.

LDAP does not support certain user profile information. Such information remains in the domain of the JD Edwards EnterpriseOne server and must be maintained by the JD Edwards EnterpriseOne system administrator. Therefore, two distinct and separate user profiles may exist:

- LDAP user profile

  This profile includes the user ID and password and can include user-role relationships.

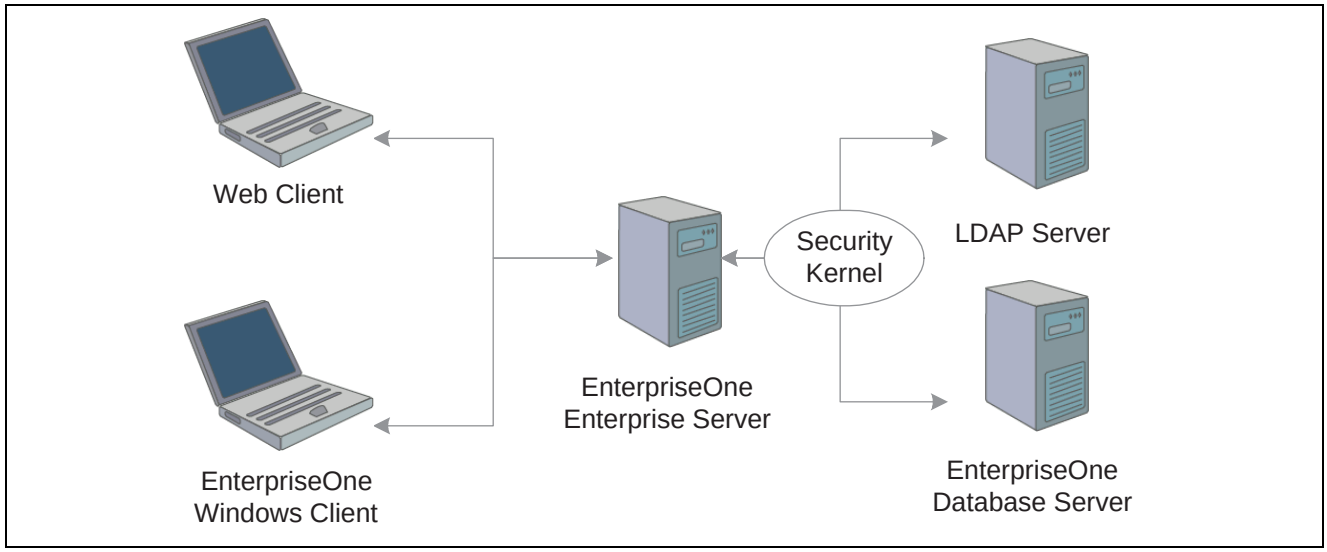
- JD Edwards EnterpriseOne user profile

  The information contained in this profile is stored in the JD Edwards EnterpriseOne database. Examples of such information include the date separator, the decimal separator, and so on.

User Authentication Using the LDAP Server

When LDAP is enabled, all systems (including JD Edwards EnterpriseOne) are directed to perform user authentication through the LDAP server.

This diagram shows how LDAP and JD Edwards EnterpriseOne handle authentication:



LDAP and JD Edwards EnterpriseOne authentication

In this illustration, the security kernel in the JD Edwards EnterpriseOne enterprise server performs authentication against the LDAP server when LDAP is enabled in the [SECURITY] section of the jde.ini file of the JD Edwards EnterpriseOne enterprise server. Otherwise, when LDAP is disabled, the security kernel authenticates the user against the JD Edwards EnterpriseOne enterprise server database.

JD Edwards EnterpriseOne User Data

The security kernel in JD Edwards EnterpriseOne requires specific attributes to be defined for all users. These attributes generally include:

- User ID.
- User password.
- User-role relationship.
- JD Edwards EnterpriseOne system user.
- Definition of role.
- JD Edwards EnterpriseOne user profile settings.

User Data Managed by LDAP

When you configure JD Edwards EnterpriseOne to use LDAP, the JD Edwards EnterpriseOne security kernel uses the following data stored in the LDAP server:

- User ID
- User password
- User-role relationship (optional)

Data Managed by LDAP and JD Edwards EnterpriseOne

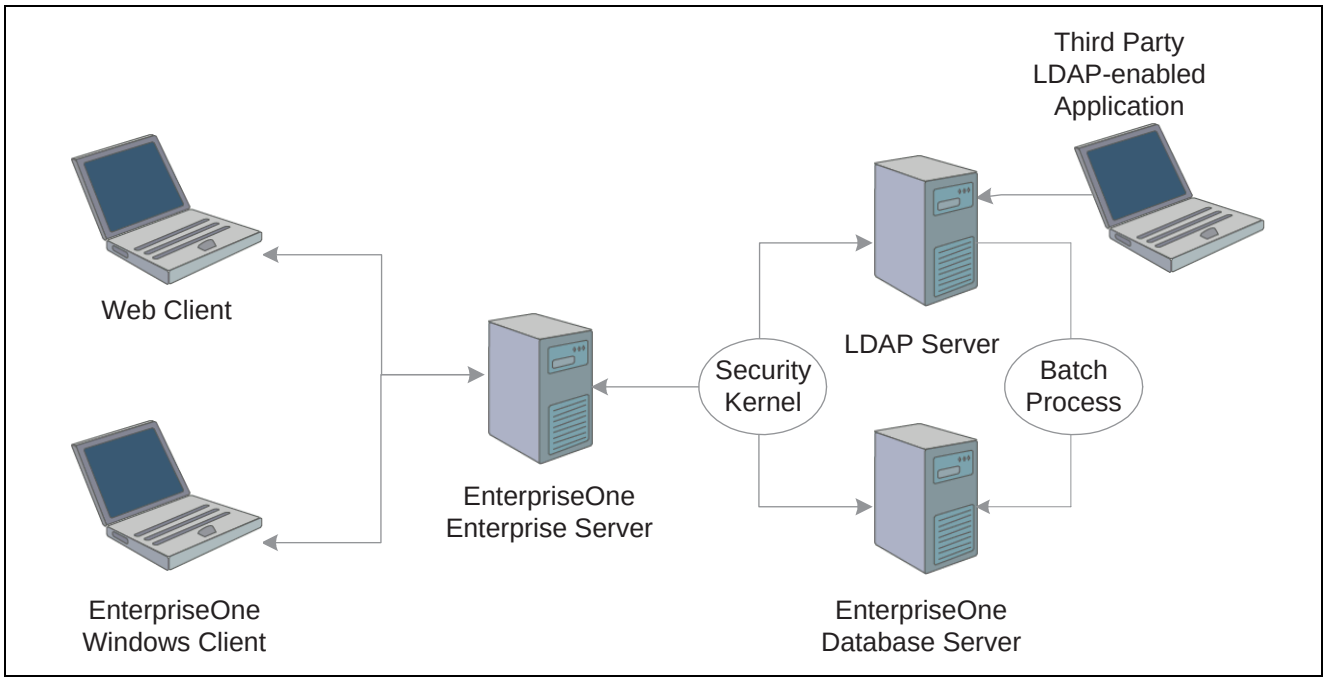
This table explains how user data is managed by LDAP and JD Edwards EnterpriseOne, as well as how the security kernel uses this information:

Data Category	LDAP	JD Edwards EnterpriseOne	Comment
EnterpriseOne User ID	Yes	Yes F0092	If you enable LDAP support in JD Edwards EnterpriseOne, the security kernel validates the user from the LDAP database. The security kernel synchronizes this data from LDAP to JD Edwards EnterpriseOne only when this data is in the LDAP server and not in JD Edwards EnterpriseOne.
EnterpriseOne User Password	Yes	Yes F98OWSEC	If LDAP is enabled, the user password is always stored in LDAP. If LDAP is not enabled, the user password is stored in the F98OWSEC table in JD Edwards EnterpriseOne.
User-Role Relationship	Yes	Yes F95921	If the user-role relationship is defined to execute through LDAP, the user-role relationship is synchronized from the LDAP server to JD Edwards EnterpriseOne. If the user-role relationship is defined to execute through JD Edwards EnterpriseOne, the data is stored in the JD Edwards EnterpriseOne database in the F95921 table.
EnterpriseOne System User	No	Yes F98OWSEC	Not managed in the LDAP server. JD Edwards EnterpriseOne requires each user to have a system user specified for access to the JD Edwards EnterpriseOne database. The database user is set by the JD Edwards EnterpriseOne system administrator in the JD Edwards EnterpriseOne security table, F98OWSEC. If there are no valid system user settings, the JD Edwards EnterpriseOne security kernel will not validate the user.

Data Category	LDAP	JD Edwards EnterpriseOne	Comment
Definition of Role	Yes	Yes F0092	The user-role relationship is synchronized from the LDAP server to the JD Edwards EnterpriseOne database for roles defined in the JD Edwards EnterpriseOne database. However, the system does not synchronize role definitions from the LDAP server to the JD Edwards EnterpriseOne database. Therefore, role definitions must exist in both systems.
EnterpriseOne User Profile Attributes	No	Yes F00921 and F0092	Not managed in LDAP. JD Edwards EnterpriseOne requires additional user profile attributes that are not generally defined through equivalent attributes in LDAP. Therefore, you can manually set these attributes. You can also specify these values in the default user profile settings for LDAP so that these settings are included for each user that is synchronized from LDAP to JD Edwards EnterpriseOne. See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Modifying the LDAP Default User Profile Settings, page 144. Some of these attributes include: • Address Book Number • Decimal Separator • Time Zone • Currency • Date Format

User Data Synchronization in LDAP-Enabled JD Edwards EnterpriseOne

This diagram shows the synchronization of user data from the LDAP server to JD Edwards EnterpriseOne:



User data synchronization

In this configuration, a third-party LDAP-enabled application is being used to add, modify, and delete LDAP user information. In addition, the system uses the following methods to synchronize user data from LDAP to the JD Edwards EnterpriseOne database:

- At user sign-in, using the JD Edwards EnterpriseOne security kernel.
- Using the LDAP Bulk Synchronization batch application (R9200040).

  R9200040 enables you to perform bulk synchronization of user profile records from the LDAP server to the JD Edwards EnterpriseOne database.

Application Changes in LDAP-Enabled JD Edwards EnterpriseOne

When LDAP support is enabled in JD Edwards EnterpriseOne, some of the user profile tasks that you typically perform in JD Edwards EnterpriseOne, such as adding and deleting users, are disabled. You must use LDAP to modify these records, not JD Edwards EnterpriseOne. This section summarizes the following changes in JD Edwards EnterpriseOne menus and applications that result from using LDAP to manage user profile information:

- User password changes.
- User Profile Revisions application changes.
- Security Revisions application changes.
- Role Relationships application changes.
- Scheduler application changes.

User Password Changes

In JD Edwards EnterpriseOne, users can change their passwords using the User Default Revisions application. However, when LDAP is enabled, users must contact a system administrator for password changes. If a user attempts to select the Change Password option in the User Default Revisions form, the system displays this error:

```
Error: LDAP authentication is enabled.
Solution: Users must contact a security administrator to have their passwords⇒
 changed.
```

User Profile Revisions Application (P0092) Changes

The following functions for managing user information in P0092 are disabled:

- Add
- Copy
- Delete

This ensures that users can only be managed through LDAP.

EnterpriseOne Security Application (P98OWSEC) Changes

When LDAP is enabled, P98OWSEC only allows you to add or change specific security settings for specified users. This section discusses the features that you can use in this application when LDAP is enabled.

When an existing *single* user is selected for security revisions, the User ID field contains the selected user ID.

On the Security Detail Revisions form, you can enable the User Status and Allowed Password Attempts fields by selecting these corresponding options:

- User Status
- Attempts

When you are updating security for *all* users, you click the Revise All button from the Form menu in the Work With User/Role Profiles form. The Security Detail Revisions form appears.

On the Security Detail Revisions form, you can enable the User Status and Allowed Password Attempts fields for all users by selecting these corresponding options:

- User Status
- Attempts

Role Relationships Application (P95921) Changes

When LDAP is enabled, P95921 has been modified to enable or disable certain functionality, depending on whether roles are managed in LDAP. When roles are managed in LDAP, you cannot use JD Edwards EnterpriseOne to add or delete a role for an individual user. However, you can add roles to the default user for LDAP, which is _LDAPDEFLT. Additionally, you can modify the role expiration date.

If you attempt to add a role to an individual user in JD Edwards EnterpriseOne, the system displays this error:

```
Error: Role Relationship is managed by LDAP.
```

Similarly, if you attempt to delegate, remove, or add a role for an individual user, the system will display the same error.

Note. When LDAP is enabled and roles are managed in LDAP, you can use a third-party LDAP-enabled application to add, delete, or modify role relationships for any user.

Schedule Jobs Application Changes

The Schedule Jobs application (P91300) displays a password column which is written to the F91300 table. The password stored in this column provides the password that P91300 uses to connect to the JD Edwards EnterpriseOne database. The column is only stored for program use and the actual database record contains an encrypted blob that cannot be viewed or decrypted by the system administrator. However, you can enter the password in the Scheduler Password field of the Scheduling Advance Options form.

The Scheduler kernel validates the user ID and password stored in F91300. The job cannot be launched if the validation fails. Therefore, if the user changes their password after the job is scheduled, the job cannot be launched. In such cases, the user must use P91300 to revise the job.

LDAP Server-Side Administration

This section assumes that JD Edwards EnterpriseOne is using the LDAP server for user profile administration. Using a third-party LDAP-enabled application to access the LDAP server, you can add, modify, or delete attributes of user profiles. This table lists the items that you can manage and actions that you can perform from the LDAP server:

User Profile Attribute	Action	Description
User ID and Password Values	Add Modify Delete	The user ID and password values must be alphanumeric and cannot exceed 10 characters in length. Unicode is supported. At sign-in, logic on the JD Edwards EnterpriseOne server automatically performs one-way, real-time synchronization of user IDs from the LDAP server to the JD Edwards EnterpriseOne database. You can run a separate batch program on the JD Edwards EnterpriseOne enterprise server to initially migrate user IDs from LDAP to the JD Edwards EnterpriseOne database.

User Profile Attribute	Action	Description
User-Role Relationship	Add Modify Delete	At sign-in, logic on the JD Edwards EnterpriseOne server will automatically perform one-way real-time synchronization of this data from the LDAP server to the JD Edwards EnterpriseOne database. You can run a separate batch program on the JD Edwards EnterpriseOne server to initially migrate this data from LDAP to the JD Edwards EnterpriseOne database. Only valid JD Edwards EnterpriseOne user-role relationships will be synchronized from LDAP to the JD Edwards EnterpriseOne database.
Role Definitions	Add Modify Delete	You must manually set up role definitions in LDAP and JD Edwards EnterpriseOne because there is no automated method to synchronize this data.

JD Edwards EnterpriseOne Server-Side Administration

When JD Edwards EnterpriseOne is enabled for LDAP, there are still some user profile administrative tasks that you manage on the JD Edwards EnterpriseOne enterprise server, such as:

- Tasks that are not supported by LDAP.
- Tasks that are not synchronized automatically.
- Tasks that are not synchronized through a batch process.

You can modify the following items on the JD Edwards EnterpriseOne enterprise server:

JD Edwards EnterpriseOne Attributes	Action	Description
System User ID and Password	Add Modify Delete	Required to set system values not supported by LDAP. System information is used to connect to the database. It includes database system user name, system user password, and data source name (system key).
User-Role Relationship	Add Modify Delete	Required if user-role relationships are managed in JD Edwards EnterpriseOne.
User-Role Relationship Attributes	Add Modify Delete	Required to set attributes not supported by LDAP, such as *ALL and Expiration Dates, when you manage user-role relationships in LDAP.

JD Edwards EnterpriseOne Attributes	Action	Description
User Status	Modify	Allowed statuses include: • Enabled • Disabled There is no automatic or batch synchronization between LDAP and JD Edwards EnterpriseOne for this function.
Allow Password Attempts for EnterpriseOne User	Modify	The number of invalid sign-on attempts a user can make before that user profile is disabled.
Role Definitions	Modify	You must always define the role definition in JD Edwards EnterpriseOne, regardless of any LDAP considerations.

Configuring LDAP Support in JD Edwards EnterpriseOne

This section provides an overview of the steps to enable LDAP support in JD Edwards EnterpriseOne, how JD Edwards EnterpriseOne uses LDAP server settings, lists prerequisites, and discusses how to:

- Create an LDAP configuration.
- Configure the LDAP server settings.
- Configure LDAP to JD Edwards EnterpriseOne enterprise server mappings.
- Change the LDAP configuration status.
- Enable LDAP authentication mode.
- Export user data to the LDAP server.

Note. If you are creating an LDAP configuration for Oracle Internet Directory, the specific settings for this configuration are listed in an appendix in this guide.

See Appendix A, "Creating a JD Edwards EnterpriseOne LDAP Configuration for OID," page 213.

Overview of Steps to Enable LDAP Support in JD Edwards EnterpriseOne

You must follow these high-level steps in the specified order to properly configure the JD Edwards EnterpriseOne enterprise server to support LDAP:

1. Disable LDAP authentication by ensuring that the [Security] section of the JD Edwards EnterpriseOne enterprise server jde.ini file contains this setting:

   ```
   LDAPAuthentication=false
   ```

2. Use the LDAP Server Configuration Workbench application (P95928) to create an LDAP configuration, configure the LDAP server settings, and configure the LDAP to JD Edwards EnterpriseOne enterprise

server mappings. The P95928 application is available on the Microsoft Windows client and the web client.

Note. JD Edwards EnterpriseOne provides two versions of this application. You can use ZJDE0001 to create a template for creating an LDAP configuration. Create the template by adding specific attributes to the LDAP configuration that can be defined later. This section uses ZJDE0002 of the application to show all possible attributes that can be mapped in the LDAP configuration.

---

3. Use the Configure LDAP Defaults form to enter the required LDAP default user profile settings.

   See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Modifying the LDAP Default User Profile Settings, page 144.

4. Change the LDAP configuration status.
5. Enable LDAP authentication by changing the setting in the [Security] section of the JD Edwards EnterpriseOne enterprise server jde.ini file:

   ```
   LDAPAuthentication=true
   ```

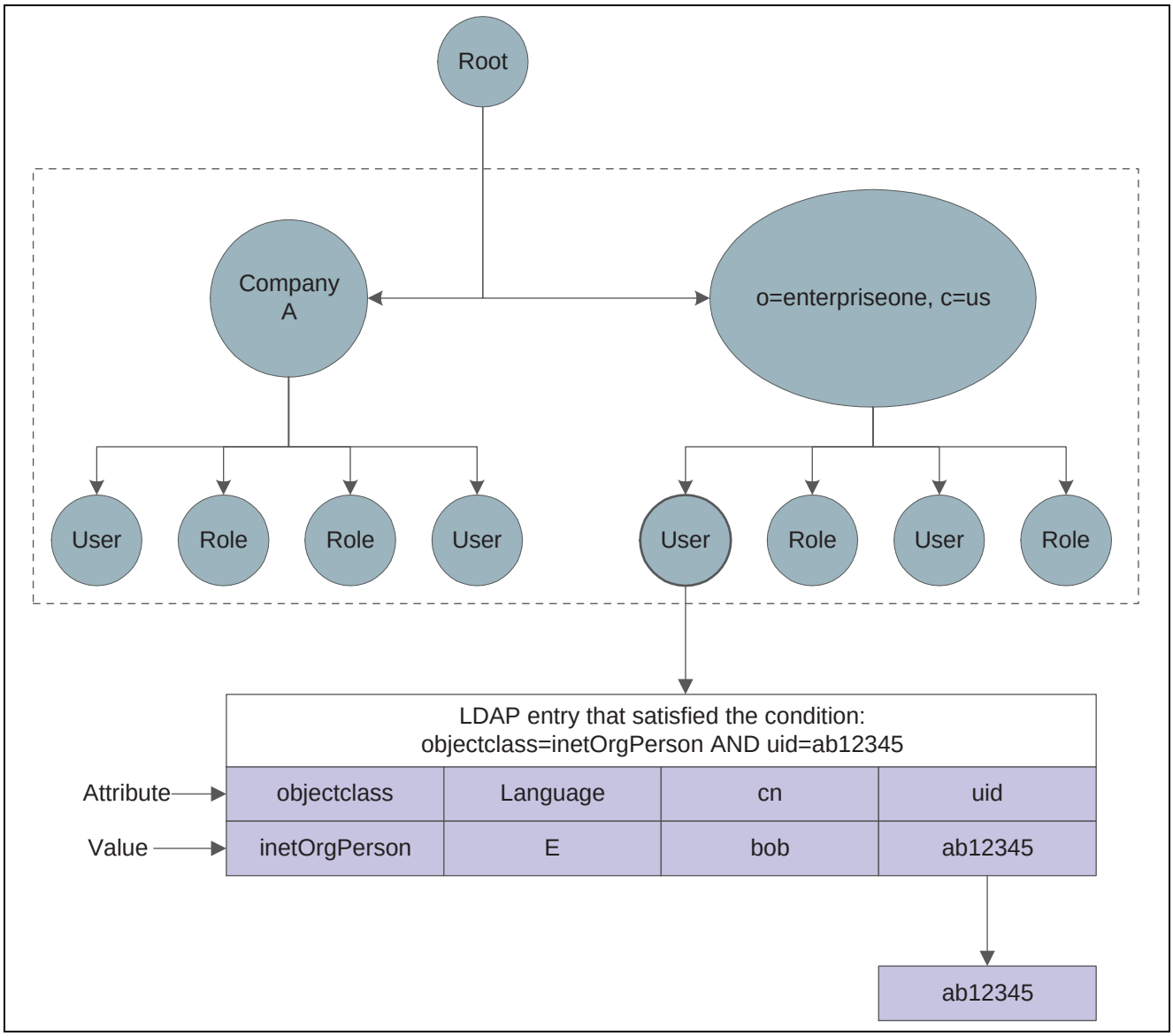
6. Restart the JD Edwards EnterpriseOne enterprise server.

How JD Edwards EnterpriseOne Uses LDAP Server Settings

Part of creating an LDAP configuration for JD Edwards EnterpriseOne involves configuring LDAP server settings. The LDAP server settings are in compliance with the standard syntax specified by the LDAP Data Interchange Format (LDIF). These settings, or attributes, when configured correctly, determine how JD Edwards EnterpriseOne searches for user profile data in the LDAP server. The attributes that you configure differ depending on whether you are:

- Creating a standard JD Edwards EnterpriseOne configuration for the LDAP server.
- Using Secure Socket Layer with the LDAP server.
- Using the self-service version of the user profile application for the Manufacturing Sourcing module.

This diagram shows how JD Edwards EnterpriseOne uses the LDAP server settings to search for user profiles in the LDAP server:



User data search hierarchy in the LDAP server

In this diagram, the JD Edwards EnterpriseOne application requests a search of the Directory Information Tree for a JD Edwards EnterpriseOne user in the United States with an ab12345 user ID. The user can only be found if these attributes contain valid values:

Attribute	Value
USRSRCHBAS (User Search Base)	o=enterpriseone, c=us
USRSRCHSCP (User Search Scope)	subtree
USRSRCHFLT (User Search Filter)	objectclass=inetOrgperson
USRSRCHATR (User Search Attribute)	uid
E1USRIDATR (EnterpriseOne User ID Attribute)	uid

1. JD Edwards EnterpriseOne starts the search using the criteria specified in the User Search Base attribute.
2. JD Edwards EnterpriseOne uses the value in the User Search Scope attribute to determine the scope of the search.
3. JD Edwards EnterpriseOne uses the following Search Filter parameter to search for the user in LDAP:

   (&((*User Search Filter value*), ((*User Search Attribute value*)= “ab12345”)))
4. JD Edwards EnterpriseOne retrieves the user ID from the EnterpriseOne User ID Attribute.

Prerequisites

To configure LDAP support in JD Edwards EnterpriseOne, you must have a system administrator who understands LDAP and understands how to use an LDAP-compliant directory service to manage user profile information.

For more information on LDAP, refer to these resources on the web:

- The IETF LDAPv3 Working Group.

  See http://www.ietf.org/html.charters/ldapbis-charter.html
- The LDAPv3 Working Group archived newsgroup.

  See http://www.openldap.org/lists/ietf-ldapbis/
- RFC 3377, the current definition of LDAPv3.

  See ftp://ftp.rfc-editor.org/in-notes/rfc3377.txt

For more information about a specific LDAP-compliant directory service, refer to that particular directory service’s documentation.

If you are configuring the directory service with SSL, refer to the directory service documentation for instructions.

Forms Used to Configure LDAP Support in JD Edwards EnterpriseOne

Form Name	FormID	Navigation	Usage
Available LDAP Configurations	W95928F	Enter *P983051* in the Fast Path. On the Work With Interactive Versions form, enter P95928 in the Interactive Version field and click Find. Select ZJDE0002 and then select Run from the Row menu. The P95928 application is available on the Microsoft Windows client and the web client.	Add an LDAP configuration record.
LDAP Server Information	W95928A	On the Available LDAP Configurations form, click Add.	Complete the fields that are required for the LDAP configuration record.
LDAP Server Attribute Values	W95928E	On the Available LDAP Configurations form, select a configuration record and then select Values from the Row menu.	Enter LDAP server attribute values.
LDAP Server Mappings	W95928B	On the Available LDAP Configurations form, select Mappings from the Row menu.	Configure LDAP to JD Edwards EnterpriseOne enterprise server mappings.

Creating an LDAP Configuration

Access the Available LDAP Configurations form.

1. Click Add to add a new configuration record.
2. On the LDAP Server Information form, complete these fields and then click OK:

Field	Description
Server Configuration Name	Enter a unique name for the server configuration, and then tab to the next field and enter a description.
Enterprise Server Location	Enter the location of the enterprise server.
Enterprise Server Port	Enter the port used to connect to the enterprise server.
LDAP Server Location	Enter the location (machine name or IP address) of the LDAP server on the network.
LDAP Server Port	Enter the port used to connect to the LDAP server.

Field	Description
LDAP Server Type	Click the search button to select the type of LDAP server: Microsoft, IBM, or Domino. **Note.** If you are configuring LDAP for Oracle Internet Directory, you must add OID to the list of options and select it here. See Appendix A, "Creating a JD Edwards EnterpriseOne LDAP Configuration for OID," page 213.
LDAP Admin ID	Enter the administrator's ID for the LDAP server.
LDAP Admin Password	Enter the administrator's password for the LDAP server.
SSL Enabled LDAP Server	Select this option if you want to set up Secure Socket Layer (SSL) communication between JD Edwards EnterpriseOne security kernel and the LDAP server. **Note.** This requires the LDAP server to be configured for SSL. See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Using LDAP Over SSL, page 148.
Role Enabled in LDAP	Select this option if you are managing user-role relationships in LDAP.

Configuring the LDAP Server Settings

Access the LDAP Server Attribute Values form. To do so, on the Available LDAP Configurations form, select a configuration record and then select Values from the Row menu.

1. Click the search button in the Enterprise Server Attribute Name column to select the attributes to include in the LDAP server settings.

   After selecting the attributes, you must enter the appropriate LDAP value for the attribute in the LDAP Server Attribute Value column.

2. To configure the standard JD Edwards EnterpriseOne settings for LDAP server, enter values for these attributes:

Attribute	Description
USRSRCHBAS	User search base. Specifies that the system searches for user information at the root of the directory information tree. This value specifies the "container" in which to begin the search. For example, `USRSRCHBAS=o=jdedwards,c=us`
USRSRCHFLT	User search filter. Specifies that a search is performed at the base level for the user ID in the LDAP server using the specified criteria. For example, `USRSRCHFLT=objectclass=inetOrgPerson` If you do not specify this value, no search filtering occurs.

Attribute	Description
USRSRCHSCP	User search scope. Specifies the level, or scope, at which the system searches for user information. Valid values are: • *base* The query searches only the value you specified in the USRSRCHBAS setting. • *subtree* This is the default value. The query searches the value in the Search Base field and all entries beneath it. • *onelevel* The query searches only the entries one level down from the value in the Search Base field.
ROLSRCHBAS	Role search base (use only if roles are enabled in LDAP). Specifies that a search is performed at the base level for the UserIDAttri in the LDAP database. For example, `ROLSRCHBAS=o=jdedwards,c=us`
ROLSRCHFLT	Role search filter (use only if roles are enabled in LDAP). This specifies that a search is performed at the base level for the role in the LDAP database using the specified criteria. For example, `ROLSRCHFLT=objectclass=groupOfNames` If you do not specify this value, no search filtering occurs.
ROLSRCHSCP	Role search scope (use only if roles are enabled in LDAP). This specifies the level, or scope, at which the system searches for role information. Valid values are: • *base* The query searches only the value you specified in the ROLSRCHBAS setting. • *subtree* This is the default value. The query searches the value in the Search Base field and all entries beneath it. • *onelevel* The query searches only the entries one level down from the value in the Search Base field.

3. When using Secure Socket Layer (SSL) with LDAP server, enter values for these attributes:

Attribute	Description
SSLPORT	SSL Port for the LDAP server. Specifies the SSL port on the LDAP server.

Attribute	Description
CERTDBPATH	Dir path for cert7.db (SSL) For Windows and UNIX: This specifies the directory path to the cert7.db file (SSL). This file should generally be located in the system\bin32 directory on the JD Edwards EnterpriseOne enterprise server. For iSeries: This specifies the directory path and file name for the cert.kdb file on the iSeries-based JD Edwards EnterpriseOne enterprise server machine, for example `/QIBM/USERDATA/ICSS/CERT/SERVER/CERT.KDB`. You should use the Digital Certificate Manager (DCM) to verify the location of the certificate for your installation.
CERTDBCLBL	Do not use this attribute. This is for future use only.
CERTDBPSWD	For iSeries only. This is the password to the key database. Specifies the password to the key database (files with a "kdb" extension). The key database is used to store a uniquely identified name, or label, associated with the client private key/certificate pair.
SSLTIMEOUT	For iSeries only. This specifies the time-out value for the SSL connection.

4. If you are using the self-service version of the user profile application for the Manufacturing Sourcing module, enter values for these attributes:

Note. You cannot use this application to manage LDAP user profiles.

Attribute	Description
USRACNTCTL	User Account Control. Specifies the authority attached when creating a user in Active Directory, for example `USRACNTCTL=512` creates an enabled user in Active Directory only.
USRADDLOC	User Add Location. Specifies the location in LDAP where users will be added, for example `USRADDLOC=O=jdedwards`.
USRCLSHRCY	User Class Hierarchy. Specifies the class hierarchy needed to create a user in LDAP, for example `USRCLSHRCY=top,person,organizationalPerson,inetOrgPerson`.
ROLADDLOC	Role Add Location (use only if roles are enabled in LDAP). Specifies the location in LDAP that contains the user-role relationship, for example `ROLADDLOC=O=jdedwards`.
ROLCLSHRCY	Do not use this attribute. This is for future use only.

Configuring LDAP to JD Edwards EnterpriseOne Enterprise Server Mappings

You can map attributes for users or for user-role relationships, depending upon your configuration. If you are entering mappings for user-role relationships, you must also ensure that the LDAP configuration record is enabled for roles.

Access the LDAP Server Mappings form. To do so, on the Available LDAP Configurations form, select Mappings from the Row menu.

1. Click the search button in the Enterprise Server Attribute Name column to select the attributes to include in the mappings.

   After selecting the attributes, you must enter the appropriate LDAP value for the attribute in the LDAP Server Actual Attribute column.

2. To configure the LDAP to JD Edwards EnterpriseOne enterprise server mappings for a standard setup, enter values for these attributes:

Attribute	Description
E1USRIDATR	EnterpriseOne User ID Attribute. Specifies the user ID attribute in LDAP that is used for JD Edwards EnterpriseOne users. The system uses this attribute when creating users in LDAP during JD Edwards EnterpriseOne sign-in, for example `E1USRIDATR=cn`.
USRSRCHATR	User ID Search Attribute. Specifies the search criteria for the sign-on user ID. This is the value that maps the sign-on user ID in LDAP to the sign-in user ID in JD Edwards EnterpriseOne, for example `USRSRCHATR=cn`. The USRSRCHATR and E1USRIDATR attributes should be mapped to the same value.
EUSRIDATR	Enterprise User ID Attribute. Specifies the User ID attribute in LDAP that is used for Enterprise users. The system uses this attribute to search for Enterprise users for single sign-on between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne, for example `EUSRIDATR = cn`.
ROLNAMEATR	Role Name Attribute (use only if roles are enabled in LDAP). This value maps the role in LDAP to the role in JD Edwards EnterpriseOne, for example `ROLENAMEATR=cn`
ROLSRCHATR	Role Search Attribute (use only if roles are enabled in LDAP). Specifies the search attribute for the role in the LDAP server. The system uses this attribute to search LDAP for a list of roles for a user, for example `ROLSRCHATR=member`.
LANGUAGATR	Language Attribute. Specifies the language attribute used within LDAP, for example `LANGUAGATR= preferredLanguage`

3. If you are using the self-service version of the user profile application for the Manufacturing Sourcing module, enter values for these attributes:

Note. You cannot use this application to manage LDAP user profiles.

Attribute	Description
CMNNAME	Common Name. Specifies the Common Name for a user in LDAP. The system uses this attribute when creating users in LDAP, for example `CMNNAME=cn`
GIVENNAME	Specifies the Given Name for a user in LDAP. It is used when creating users in LDAP, especially in Active Directory, for example `GIVENNAME=givenName`.
SURNAME	Specifies the SUR Name for a user in LDAP. This attribute is used when creating users in LDAP, for example `SURNAME=sn`.
PASSWORD	Specifies the password associated with the account that you specify with the ConnectDN (distinguished name) of the LDAP server.
OBJCLASS	Object Class. Specifies the Object Class attribute for a user in LDAP it is used when creating users in LDAP, for example `OBJCLASS=objectCLASS`.
ACNTCTLATR	Account Control Attribute. Specifies the attribute used in Active Directory for user authority in Active Directory, for example `ACNTCTLATR=userAccountControl`. If the attribute `USRACNTCTL=512` is used in conjunction with `ACNTCTLATR`, the JD Edwards EnterpriseOne API will create an enabled user in Active Directory only.
ACTNAMEATR	Account Name Attribute. Specifies the attribute used only in Active Directory for creating a signon user account, for example `ACNTCTLATR=sAMAccountName`.

Changing the LDAP Configuration Status

After you add an LDAP configuration, by default the configuration is disabled or non-active. You must change the status to active to enable the configuration.

Note. You can have only one active LDAP configuration per port.

Access the Available LDAP Configurations form.

Select a configuration record and then select Change Status from the Row menu.

The system changes the status in the Status column to AV (active) or NA (not active).

Enabling LDAP Authentication Mode

Access the jde.ini file on the JD Edwards EnterpriseOne enterprise server.

In the [SECURITY] section, enter *true* for the LDAPAuthentication setting to enable security authentication. The default value for this setting is *false*, which disables the LDAP authentication mode.

Modifying the LDAP Default User Profile Settings

This section provides an overview of the LDAP default user profile settings and discusses how to:

- Review the current LDAP default settings.
- Modify the default user profile settings for LDAP.
- Modify the default role relationships for LDAP.
- Modify the default user security settings for LDAP.

Understanding LDAP Default User Profile Settings

You must configure and review the default LDAP user profile settings that are in the JD Edwards EnterpriseOne database. The system requires the default settings for user profile synchronization. These values are synchronized from LDAP to JD Edwards EnterpriseOne by the LDAP synchronization mechanisms (security kernel and batch report). The default user profile settings are written to the F0092 table.

Note. You must add the default LDAP user profile settings before enabling LDAP authentication in the jde.ini file of the JD Edwards EnterpriseOne security server.

The Configuring LDAP Defaults form shows whether the following items exist for the default user:

- User profile
- Role relationships
- Data source/system user

Important! Changes made in this application can affect almost all JD Edwards EnterpriseOne users when synchronizing data from LDAP to the JD Edwards EnterpriseOne database.

Forms Used to Modify the LDAP Default User Profile Settings

Form Name	FormID	Navigation	Usage
Configure LDAP Defaults	W0092M	In Solution Explorer, from the System Administration Tools menu (GH9011), select Security Maintenance, Security Maintenance Advanced and Technical Operations, Configure LDAP Defaults.	Review the current LDAP default settings.
User Profile Revisions	W0092A	On the Configure LDAP Defaults form, click the User Profile link.	Modify the default user profile settings for LDAP.
Work with Role Relationships	W95921C	On the Configure LDAP Defaults form, click the Role Relationships link.	Add roles to the default user.
Work With User Security	W98OWSECE	On the Configure LDAP Defaults form, click the Data Source/System User link.	Add or modify the data source or system user settings.
Data Source Revisions	W98OWSECH	On the Work With User Security form, select a security record and then click Select.	Assign a different system user to the data source.
Security Revisions	W98OWSECB	On the Work With User Security form, click Add.	Add an additional data source.

Reviewing the Current LDAP Default Settings

Access the Configure LDAP Defaults form.

Note. All user values are assigned per user ID the first time, and the first time only, that a user signs in. During this initial sign-in, the values are synchronized from LDAP to the JD Edwards EnterpriseOne database. The default role relationship is synchronized only if roles are managed by JD Edwards EnterpriseOne.

LDAP Authentication Indicates whether LDAP authentication is enabled or disabled.

Role Management Indicates whether roles are managed by LDAP. You can enable JD Edwards EnterpriseOne to manage roles in LDAP through the P95928 application.

See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Creating an LDAP Configuration, page 138.

User Profile Indicates whether a default user profile exists within the JD Edwards EnterpriseOne database. Click this link to modify the default user profile settings.

See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Modifying the LDAP Default User Profile Settings, page 144.

Role Relationships Indicates whether a default role relationship exists. If LDAP authentication is enabled, and if user-role relationships are set to be managed by LDAP,

then this option is disabled. This means that the system does not use the default user-role relationship when synchronizing users from LDAP to the JD Edwards EnterpriseOne database.

Click this link to revise the default role relationship.

See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Modifying the Default Role Relationships for LDAP, page 146.

Data Source/System User Indicates whether a default data source or system user exists. Click this link to add or change the data source or system user.

See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Modifying the Default User Security Settings for LDAP, page 146.

Modifying the Default User Profile Settings for LDAP

Access the User Profile Revisions form. To do so, on the Configure LDAP Defaults form, click the User Profile link.

Modify the appropriate fields.

Note. The User ID field always contains the default user ID for the LDAP system. This field is read only.

Modifying the Default Role Relationships for LDAP

Access the Work With Role Relationships form. To do so, on the Configure LDAP Defaults form, click the Role Relationships link.

Note. If LDAP authentication is enabled and user-role relationships are being managed by LDAP, then this option is disabled. This means that user-role relationship functionality from within JD Edwards EnterpriseOne is disabled.

On the Work With Role Relationships form, you can highlight a role in either the Assigned Roles or Available Roles menus, and then click the appropriate directional arrow button to add or remove the role for the default user.

Note. These values are only synchronized between JD Edwards EnterpriseOne and LDAP if the role is being managed by JD Edwards EnterpriseOne.

Modifying the Default User Security Settings for LDAP

Access the Configure LDAP Defaults form.

1. In the Configure Defaults area, click the Data Source/System User link.

   If the default data source or system user does not exist, the Security Revisions form appears.

2. On the Security Revisions form, complete the System User field to add or change the data source or system user.

   If the default data source is defined, the Work With User Security form appears.

3. To assign a different system user to the data source, on the Work With User Security form, select the security record and then click Select.

4. On Data Source Revisions, click the search button in the System User field to assign a different system user.
5. To add an additional data source, on the Work With User Security form, click Add.
6. On the Security Revisions form, complete the fields as appropriate.

Using LDAP Bulk Synchronization (R9200040)

This section provides an overview of LDAP bulk synchronization and discusses how to run the LDAP Bulk Synchronization batch process (R9200040).

Understanding LDAP Batch Synchronization

The LDAP server contains user profile data for multiple users. This data must also exist in the JD Edwards EnterpriseOne database server. The LDAP Bulk Synchronization batch process (R9200040) enables you to perform bulk synchronization of user profile records from the LDAP server to the JD Edwards EnterpriseOne database. Therefore, this report is beneficial because it populates data that is required for JD Edwards EnterpriseOne functionality.

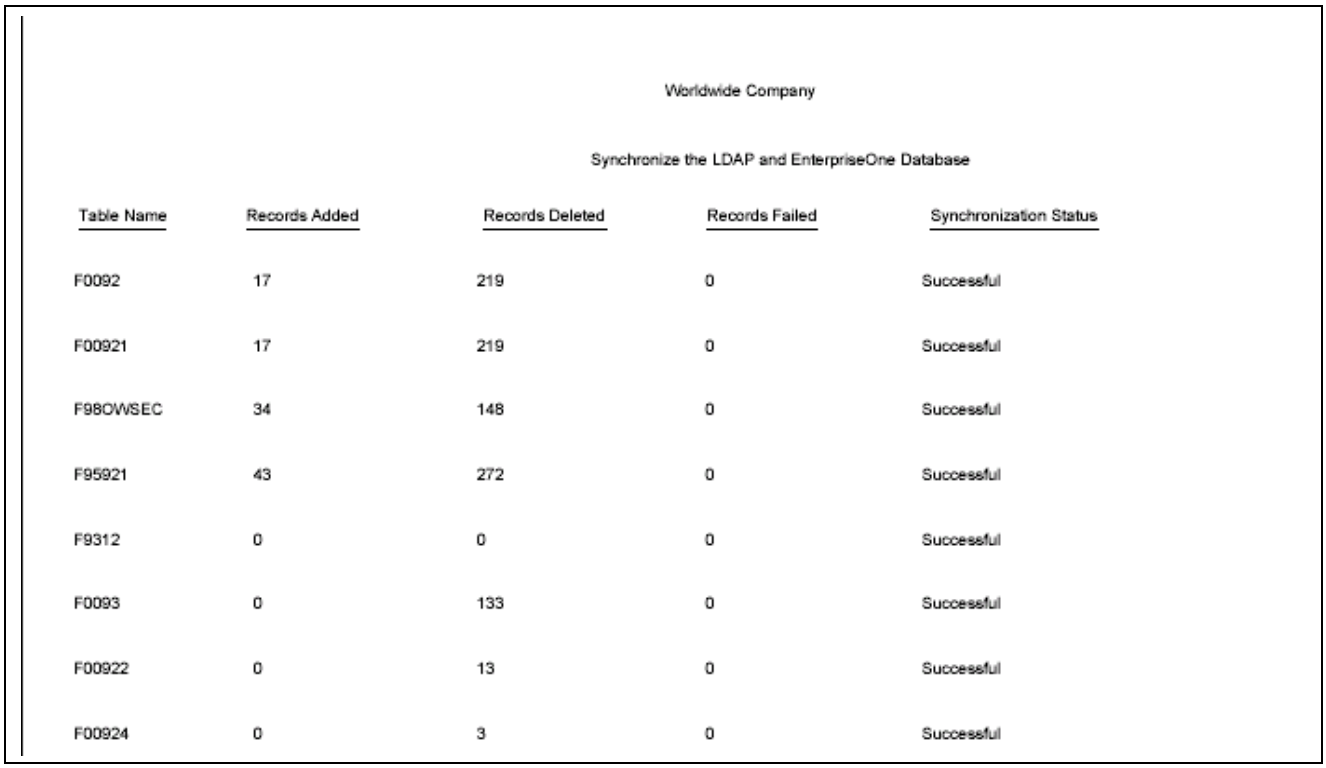
Note. If the JD Edwards EnterpriseOne database contains user profile records that are not in the LDAP server, this data cannot be synchronized from JD Edwards EnterpriseOne to the LDAP server using the R9200040 batch process. JD Edwards EnterpriseOne does not provide a utility to perform this function.

Running the report synchronizes user profile data obtained from the LDAP server to the following JD Edwards EnterpriseOne database tables:

Table	Description
F0092	Library List User
F00921	User Display Preferences
F98OWSEC	Security settings
F95921	Role Relationship
F0093	Library List Control
F00922	User Display Preferences Tag File
F00924	User Install Package
F00926	Anonymous User Access Table
F9005	Variant Description - Control Tables
F9006	Variant Detail - Control Tables
F00927	E1 Users PIM Information

Example: LDAP Bulk Synchronization (R9200040)

The following example shows the PDF output of the R9200040 batch process. Note that if the data on the LDAP server is already the same as the corresponding data on the JD Edwards EnterpriseOne database server, the report lists the affected tables and shows a zero record synchronization, which indicates the data exists, but is identical.



Worldwide Company

Synchronize the LDAP and EnterpriseOne Database

Table Name	Records Added	Records Deleted	Records Failed	Synchronization Status
F0092	17	219	0	Successful
F00921	17	219	0	Successful
F98OWSEC	34	148	0	Successful
F95921	43	272	0	Successful
F9312	0	0	0	Successful
F0093	0	133	0	Successful
F00922	0	13	0	Successful
F00924	0	3	0	Successful

LDAP Bulk Synchronization output

Running the LDAP Bulk Synchronization Batch Process (R9200040)

Access the Batch Versions program (P98305). To do so, enter *P98305* in the Fast Path.

1. On the Work With Batch Versions – Available Versions form, enter *R9200040* in the Batch Application field and click Select.
2. On the Version Prompting form, click Submit.

Using LDAP Over SSL

This section provides an overview on how to enable LDAP authentication over Secure Socket Layer (SSL) and discusses how to:

- Enable LDAP authentication over SSL for Windows and UNIX.
- Enable LDAP authentication over SSL for iSeries.

Understanding LDAP with SSL

You can establish a secure LDAP connection between the JD Edwards EnterpriseOne server and the LDAP server.

LDAP Authentication Over SSL for Windows and UNIX

The JD Edwards EnterpriseOne server uses Netscape's certificate database, cert7.db. You can obtain a cert7.db using the PKCS Utilities distributed by Netscape. Refer to Netscape's documentation for more information on obtaining and using the PKCS Utilities.

For Windows and UNIX, establishing the secure connection between the JD Edwards EnterpriseOne application server and the LDAP server requires these items:

- Cert7.db certificate database from Netscape.
- A server certificate for the LDAP server.
- The trusted root certificate from the certificate authority (CA) that issues the server certificate.

LDAP Authentication Over SSL for iSeries

The JD Edwards EnterpriseOne server uses IBM certificate database (.kdb) to store certificates on iSeries. You can create a certificate database on iSeries using Digital Certificate Manager.

For iSeries, establishing a secure connection between the JD Edwards EnterpriseOne application server and the LDAP server requires these items:

- IBM Certificate store (.kdb) certificate database.
- A server certificate for the LDAP server.
- The trusted root certificate from the certificate authority (CA) that issues the server certificate.

Enabling LDAP Authentication Over SSL for Windows and UNIX

To enable LDAP authentication over SSL for Windows or UNIX:

1. Follow the documentation for your directory server to add the server certificate to the directory server.
2. Using Netscape's PKCS Utilities, add the CA's trusted root certificate to the cert7.db certificate database.
3. Enable SSL for the LDAP configuration using the LDAP Server Configuration Workbench application.
4. Specify the SSL parameters.

   See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Configuring the LDAP Server Settings, page 139.
5. Restart the JD Edwards EnterpriseOne server.

Enabling LDAP Authentication Over SSL for iSeries

To enable LDAP authentication over SSL for iSeries:

1. Follow the documentation for your directory server to add the server certificate to the directory server.
2. Use Digital Certificate Manager to add and export the CA's trusted root certificate to the certificate database (.kdb file).

3. Enable the SSL for the LDAP configuration using the LDAP Server Configuration Workbench application.
4. Specify the SSL parameters.

   See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Configuring the LDAP Server Settings, page 139.
5. Restart the JD Edwards EnterpriseOne server.

Exporting User Data to the LDAP Server

This section provides an overview of the data4ldap utility, lists prerequisites, and discusses:

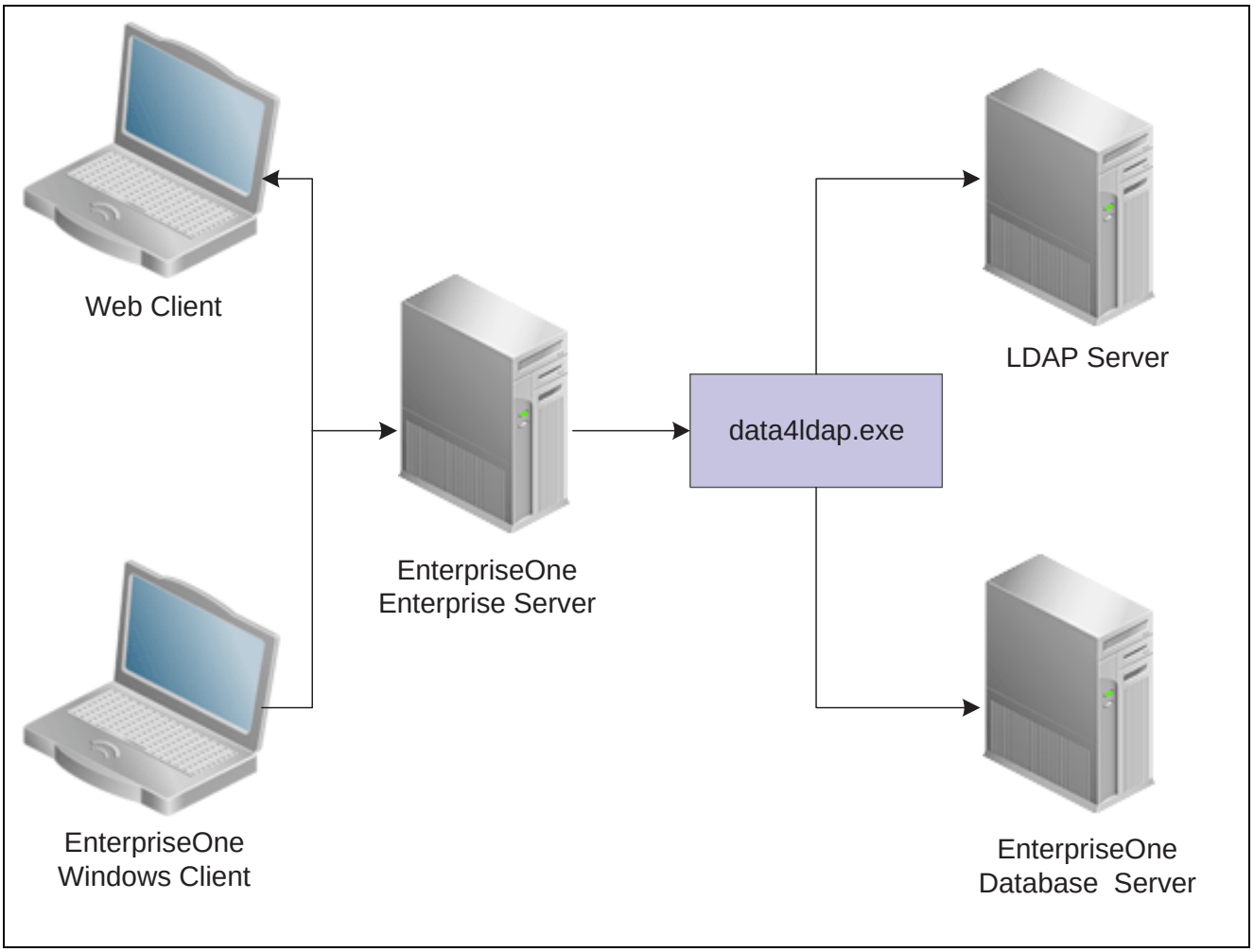
- Granting access to the data4ldap utility.
- Configuring parameters required to run the data4ldap utility.
- Running the data4ldap utility on Windows.
- Running the data4ldap utility on UNIX or Linux.
- Running the data4ldap utility on iSeries.
- Scenarios for Uploading Users to the LDAP server.
- LDAP server behavior.

Understanding the data4ldap Utility

The data4ldap utility automates the process of uploading JD Edwards EnterpriseOne user data to the LDAP server. The JD Edwards EnterpriseOne user data includes:

- EnterpriseOne user ID
- Password
- Language attribute
- User-role relationship

If you do not use this utility, you would have to populate the repository manually, which can lead to data being entered incorrectly. This illustration shows the data4ldap.exe utility uploading the JD Edwards EnterpriseOne user data to the LDAP server.



Uploading user data to the LDAP server with data4ldap.exe

The Language attribute is uploaded only for those JD Edwards EnterpriseOne users who are specifically assigned a language. By default, no language is assigned to a user when a user is added to JD Edwards EnterpriseOne. In such a case, no language is available for the particular user in the LDAP server. For example, if User 1 is assigned language E and User 2 is not assigned to any language, the language attribute is uploaded to the LDAP server only for User 1 and not for User 2.

Expired JD Edwards EnterpriseOne users and roles are also exported to the LDAP server. If a JD Edwards EnterpriseOne user record does not exist in the table F98OWSEC, then the particular user would not be exported to the LDAP server.

Prerequisites

Before you use the data4ldap utility, you must:

- Use the LDAP Server Configuration Workbench program (P95928) to map these items:
  - User Search Attribute
  - User Search Base
  - User Class Hierarchy
  - Role Search Attribute

  - Role Name Attribute
  - Role Search Base
  - Role Class Hierarchy
  - Object Class
  - Password

    If these fields are left blank, no operation is performed; the utility generates an appropriate error message and exits.

- For Microsoft Active Directory, map the following attributes in addition to the above mentioned ones:
  - User Account Control
  - Account Control Attribute
  - Account Name Attribute
- Use the LDAP Administrator user ID and password. If either the LDAP Administrator user ID or password field is blank in P95928, the utility cannot export JD Edwards EnterpriseOne user-role data to the LDAP server. It will generate an error message and exit.
- Disable the password policies of the LDAP server. For further information, refer to the documentation of the directory server that you are using for the LDAP server or contact your LDAP Administrator.

Granting Access to the data4ldap Utility

The data4ldap utility involves working with secured data, so you must ensure that only authorized users are able to access and run it. Use the External Calls Security form in the Security Workbench program (P00950) to grant a user or administrator access to this utility.

See Chapter 7, "Using Security Workbench," Adding External Call Security, page 84.

Configuring Parameters Required to Run the data4ldap Utility

The data4ldap utility can run only on the Enterprise Server and not on the client.

To run the data4ldap utility, you must configure these parameters:

```
data4ldap <UserID> <Environment> <Role> <IsRoleIncluded (*YES/*NO)> <IsOverwrite⇒
Allowed (*YES/*NO)>
```

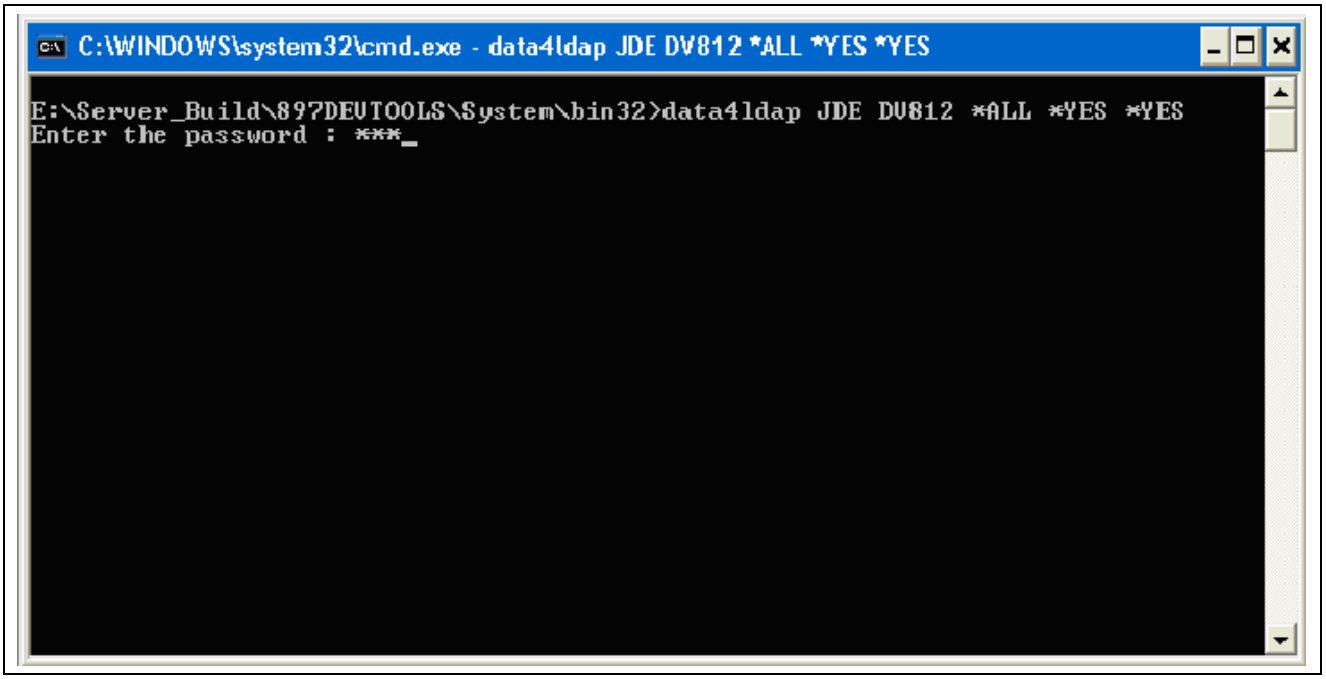
Parameter	Description
UserID	Enter a valid JD Edwards EnterpriseOne user ID that has been granted access to the utility from External Call Security.
Environment	Enter a valid JD Edwards EnterpriseOne environment.
Role	Enter a valid JD Edwards EnterpriseOne role.

Parameter	Description
IsRoleIncluded	Specify whether or not JD Edwards EnterpriseOne role information is included in the export to the LDAP server. Enter *YES to export role information. Enter *NO to not export role information.
IsOverwriteAllowed	Determine whether you want to override the LDAP server entries with the JD Edwards EnterpriseOne user-role data: Enter *YES to overwrite the LDAP server entries with the JD Edwards EnterpriseOne user-role data. Enter *NO if you do not want to overwrite the LDAP server entries with the JD Edwards EnterpriseOne user-role data.

Note. The IsOverwriteAllowed parameter is used in case the LDAP server already contains user data that is identical to JD Edwards EnterpriseOne user data. In this case, you have the option to overwrite the existing LDAP server user IDs with the current JD Edwards EnterpriseOne user IDs.The value of IsOverwriteAllowed parameter is valid only for user data (common name, language, password, and given name whichever is configured through the application P95928) and not for user-role relationship data.

Running the data4ldap Utility on Windows

In the command prompt, navigate to Enterprise Server System\bin32.



Windows command prompt.

1. Enter the valid parameters. For example:

   ```
   data4ldap JDE DV812 *ALL *YES *YES
   ```

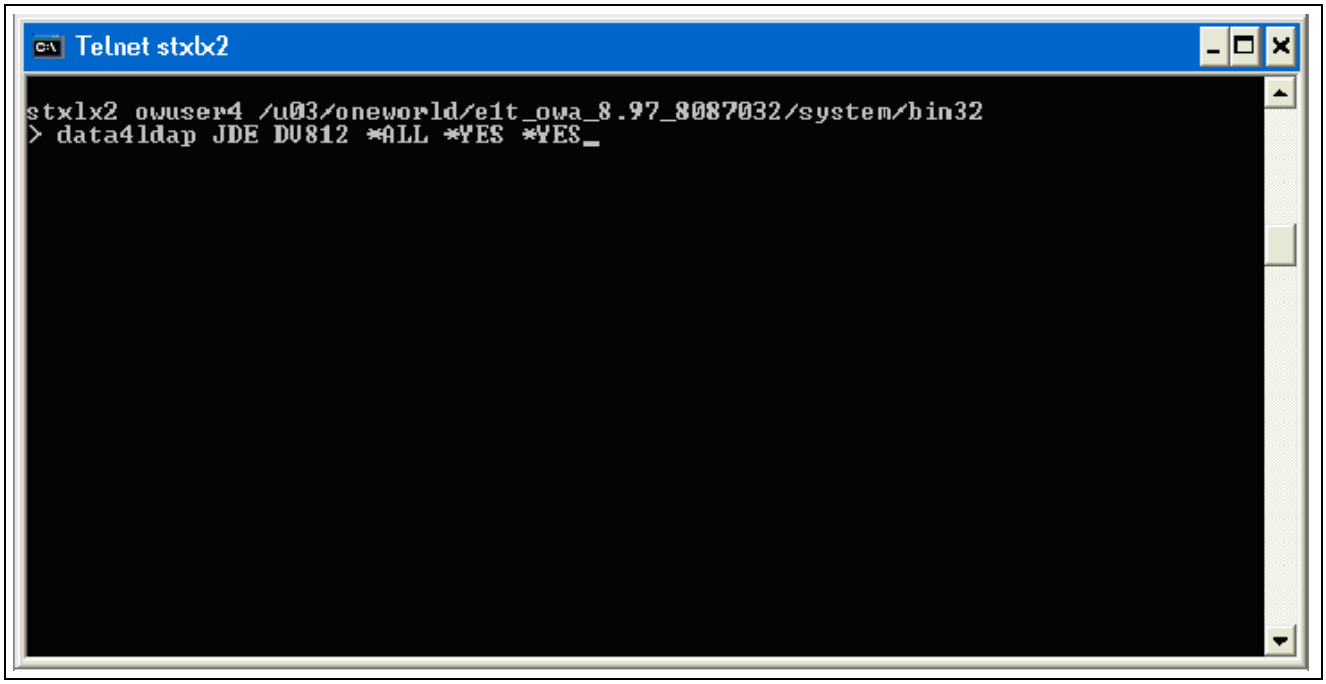
2. Press ENTER.

   The utility prompts for User – Password.

3. Enter the password for the JD Edwards EnterpriseOne account.

Running the data4ldap Utility on Unix or Linux

In the command prompt, navigate to Enterprise Server System\bin32.



Unix-Linux command prompt.

1. Enter the valid parameters. For example:

   ```
   data4ldap JDE DV812 *ALL *YES *YES
   ```

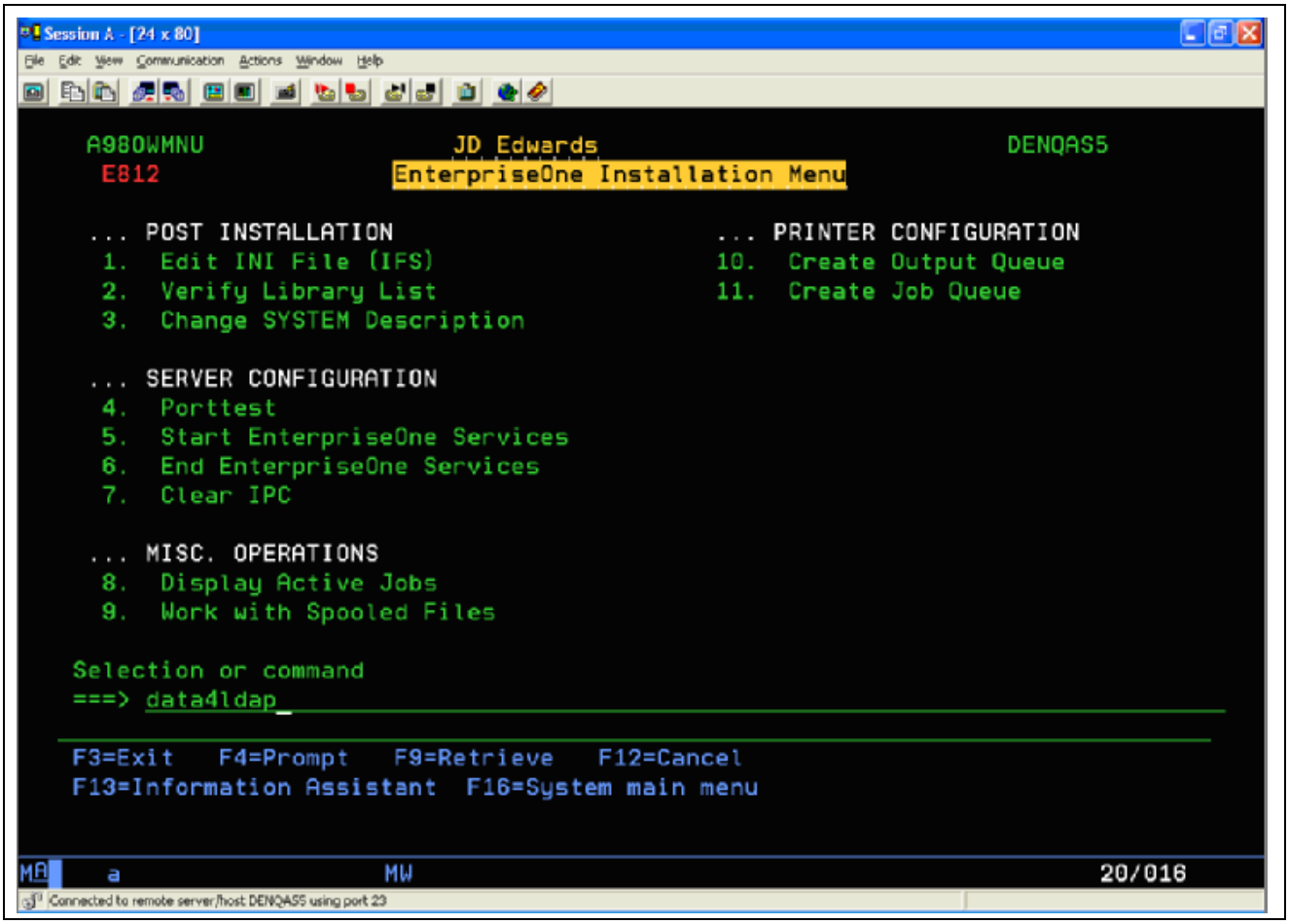
2. Press ENTER.

   The utility prompts for User – Password.

3. Enter the password for the JD Edwards EnterpriseOne account.

Running the data4ldap utility on iSeries

Access the iSeries command prompt.



iSeries command prompt.

1. Type *data4ldap* and press F4.

   Some default values that are editable appear on the screen.

2. Enter the valid parameters, for example:

   ```
   data4ldap JDE Password DV812 *ALL *YES *YES
   ```

3. Press ENTER.

Scenarios for Uploading Users to the LDAP Server

This section discusses the following scenarios for uploading users to the LDAP server:

- data4ldap JDE DV812 *ALL *NO *YES
- data4ldap JDE DV812 *ALL *YES *YES
- data4ldap JDE DV812 *ALL *YES *NO
- data4ldap JDE DV812 *ALL *NO *NO

data4ldap JDE DV812 *ALL *NO *YES

All JD Edwards EnterpriseOne users are uploaded to the LDAP server and existing LDAP user data is overwritten. However, JD Edwards EnterpriseOne user-role relationship data is neither uploaded nor overwritten in the LDAP server.

data4ldap JDE DV812 *ALL *YES *YES

All JD Edwards EnterpriseOne user and user-role relationship data is uploaded to the LDAP server. The existing LDAP user data and LDAP role-relationship data is overwritten.

data4ldap JDE DV812 *ALL *YES *NO

All JD Edwards EnterpriseOne users who do not exist in the LDAP server are uploaded to the LDAP server. The existing LDAP users are not be overwritten.

All JD Edwards EnterpriseOne user-role relationship data is uploaded to the LDAP server and the existing LDAP role-relationship data is overwritten.

data4ldap JDE DV812 *ALL *NO *NO

All JD Edwards EnterpriseOne users who do not exist in the LDAP server are uploaded to the LDAP server, and the existing LDAP users are not overwritten.

However, JD Edwards EnterpriseOne user-role relationship data would neither be uploaded nor overwritten in the LDAP Server.

LDAP Server Behavior

This section provides information about LDAP server and:

- Tree Delete control
- Microsoft Active Directory

Tree Delete Control

IBM Directory Server (IDS) and Microsoft Active Directory support Tree Delete Control. The Tree Delete Control extends the delete operation and allows the removal of sub trees within a directory using a single delete request.

It is always recommended that if the Role data are managed by the LDAP server, include the Role data (isRoleIncluded = *YES) while choosing the Overwrite option (isOverwriteAllowed = *YES).

For more details on Tree Delete Control, see:

- http://www-128.ibm.com/developerworks/tivoli/library/t-ldap-controls/index.html
- http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzahy/rzahycontrols.htm

---

Note. Oracle Internet Directory (OID) does not support Tree Delete Control.

Microsoft Active Directory

Microsoft Active Directory 2003 uses “inetOrgPerson” and a user password can be stored in the Active Directory attribute called “userPassword”. However, Active Directory 2003 must be configured to store a user password in the “userPassword” attribute. It can be configured by setting the 9th bit of dsHeuristics value. It is located in CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=domain. object. The value should look like this: 000000001. For details refer to:

http://technet2.microsoft.com/windowsserver/en/library/bb99fdd4-f8e0-490f-adae-6814cf081ff71033.mspx?mfr=true

Consider the following items when using Microsoft Active Directory:

- EnterpriseOne application P95928 should be configured accordingly for “InetOrgPerson” and “userPassword”.
- For Microsoft Active Directory 2003, the EnterpriseOne data can be dynamically uploaded only over a SSL connection. Even the LDIF (Lightweight Directory Interchange Format) file generated with the help of the data4ldap utility can be uploaded to the LDAP server only over SSL connection. This is due to the Microsoft Active Directory restriction.
- Microsoft Active Directory 2003 user-password authentication is case sensitive. The uploaded user passwords are stored in upper-case in LDAP servers. During sign-in, other LDAP servers, except Microsoft Active Directory 2003, ignore the case of the supplied password, whereas Microsoft Active Directory 2003 fails to authenticate a user if the supplied password is not in uppercase.
- In case a user does not get uploaded to Microsoft Active Directory, all of the roles assigned to the particular user would also not be uploaded to Microsoft Active Directory. This restriction is valid only for Microsoft Active Directory and not for OID / IDS.

CHAPTER 12

Understanding JD Edwards EnterpriseOne Single Sign-On

This chapter provides an overview of JD Edwards EnterpriseOne single sign-on and discusses:

- Authenticate tokens.
- Nodes.
- How a node validates an authenticate token.
- Single sign-on scenarios.

JD Edwards EnterpriseOne Single Sign-On Overview

JD Edwards EnterpriseOne single sign-on enables users that are signed in to either PeopleSoft Enterprise Portal or JD Edwards Collaborative Portal to access JD Edwards EnterpriseOne applications without re-entering a user ID and password. Single sign-on provides these benefits:

- Allows users to navigate between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne applications seamlessly.
- Increases the security for the JD Edwards EnterpriseOne system since passwords are no longer passing between different sub-systems in JD Edwards EnterpriseOne.

Note. JD Edwards EnterpriseOne does not support single sign-on between JD Edwards EnterpriseOne applications and third-party applications.

Authenticate Tokens

JD Edwards EnterprisOne uses an authenticate token to achieve single sign-on. The authenticate token contains criteria that grants access to a JD Edwards EnterpriseOne application from PeopleSoft Enterprise Portal or JD Edwards Collaborative Portal. When a user signs on to either system, after successful authentication, the system generates an authenticate token. When a user accesses an JD Edwards EnterpriseOne application, the system uses the generated token to validate the user against the JD Edwards EnterpriseOne security server. As a result, the user does not have to manually sign on to the system again.

When a user signs on to either system, an authenticate token is generated after successful authentication. When the user accesses an EnterpriseOne application, the system uses the generated token to validate the user against the EnterpriseOne security server. As a result, the user does not have to manually sign on to the system again.

For security purposes, all authenticate tokens expire after a certain period of time and contain a digital signature that ensures the token cannot be tampered with.

An authenticate token contains these properties:

Property	Description
User ID	The user ID that the server issued the token for. When the browser submits this token for single sign-on, this is the user that the application server signs in to the system.
Language Code	The language code of a user. When the system uses a token for single sign-on, it sets the language code for the session based on this value.
Date and Time Issued	The date and time the token was first issued. The system uses this field to enforce a timeout interval for the single sign-on token. Any application server that accepts tokens for sign-on compares this value against the amount of time set in the application server to accept tokens. The value is in Greenwich Mean Time (GMT) so it does not matter which time zone the application server is in. **Note.** The system date and time is used to validate the expiration of a token. Changing these values on the server may expose a potential security risk.
Issuing Node Name	The name of the machine that issued the token.
Signature	A digital signature that the application server (node) uses to validate the token for single sign-on by ensuring that the token has not been tampered with since it was originally issued. The machine issuing the token generates the signature by concatenating the contents of the token (all the fields that appear in this table) with the message node password for the local node. Then the system hashes the resulting string using the SHA1 hash algorithm. For example ("+" means concatenation), signature = SHA1_Hash (UserID + Lang + Date Time issued + Issuing Node Name+ Issuing Node Password) There is only one way to derive the 160 bits of data that make up the signature, and that is by hashing exactly the same User ID, Language, Date Time, Issuing System, and node password.

Nodes

A node is a machine that can generate or validate an authenticate token. The node contains properties that you set to control security and specify parameters for which tokens the node will accept. The system stores the node properties in the database or the jde.ini files, depending on your particular setup.

Each node contains these properties:

Property	Description
Node name	A logical name associated with this node. The length of the node name cannot exceed 15 characters.
Node password	Each node has a password which is known only by the system administrator. It serves as a key to ensure that the token does not get tampered with after it is generated.
Physical machine name	The physical machine name in which the node resides.
Trusted nodes list	This property contains the list of nodes that can be trusted by this node. For security purposes, only tokens that are generated by predefined machines can be accepted. These predefined machines are called trusted nodes. The trusted node is one-way, for example if you set up node A to trust node B, it does not mean that node B trusts node A.
Token lifetime properties	When validating a token, the node checks the time the token was issued against the amount of time that you set in the token lifetime properties. For example, if you set the token lifetime for six hours, and the node receives a token that was originally issued seven hours prior, the node will not accept the token. You can use these two properties to specify the token lifetime: • Regular token lifetime This property specifies the expiration time for a regular token. A regular token gives a user the authority to run a regular short-run process, such as a business function. The default value for this property is 12 hours. • Extended token lifetime This property specifies the expiration time for an extended token. An extended token gives a user the authority to run a long-run process, such as a UBE, after it is issued. The default value for this property is 30 days.

Note. On the iSeries platform, GMT time calculation does not take into account daylight savings time. Consequently, there can be a one hour difference in GMT time calculation between tokens generated on iSeries and Windows platforms. If you set the token timeout values as 12 hours (the default) or longer, you will notice this issue in sessions running for longer than 11 hours. If you set the token timeout values as less than one hour, then the tokens generated on Windows will automatically expire on iSeries. To resolve this issue, on the iSeries server, you should change the QUTCOFFSET value manually whenever there is a change in daylight savings time to ensure proper calculation of GMT time.

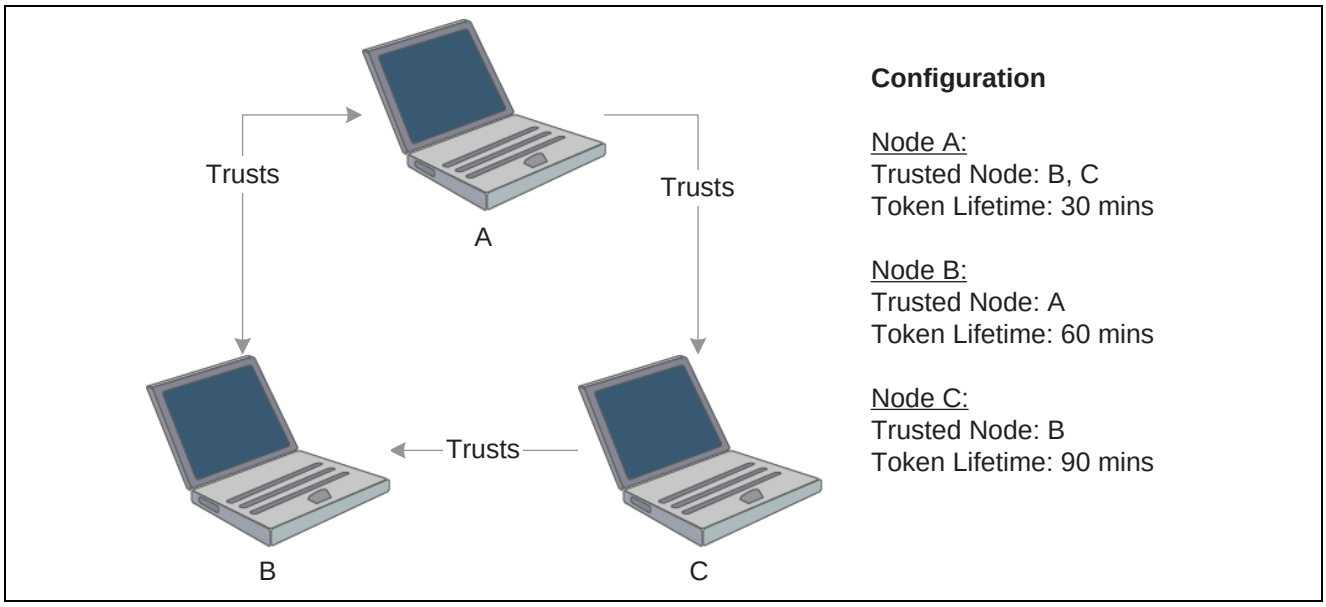
How a Node Validates an Authenticate Token

The node validates an authenticate token by checking whether:

- The token signature has been changed.
- The token is expired.

- The token is generated by a trusted node.

This diagram is an example of token validation in a multiple node setup:



Token validation in a multiple node setup

According to this configuration, the following tokens are validated by a node:

- Node A validates tokens generated by node B and node C if received less than 30 minutes from generation.
- Node B validates tokens generated by node A if received less than 60 minutes from generation.
- Node C validates tokens generated by node B if received less than 90 minutes from generation.

The following tokens are not validated by a node:

- Node B cannot accept a token generated by node C, even though node C trusts node B.
- A node will not accept a token if the time between its generation and reception by the node is greater than the token lifetime set for that node. For example, node A cannot accept a token from node B if the token was generated more than 30 minutes prior to being received by node A.

Note. No node will accept a token if its signature has been changed. The system verifies this by comparing the token signature and the hash value of the token body.

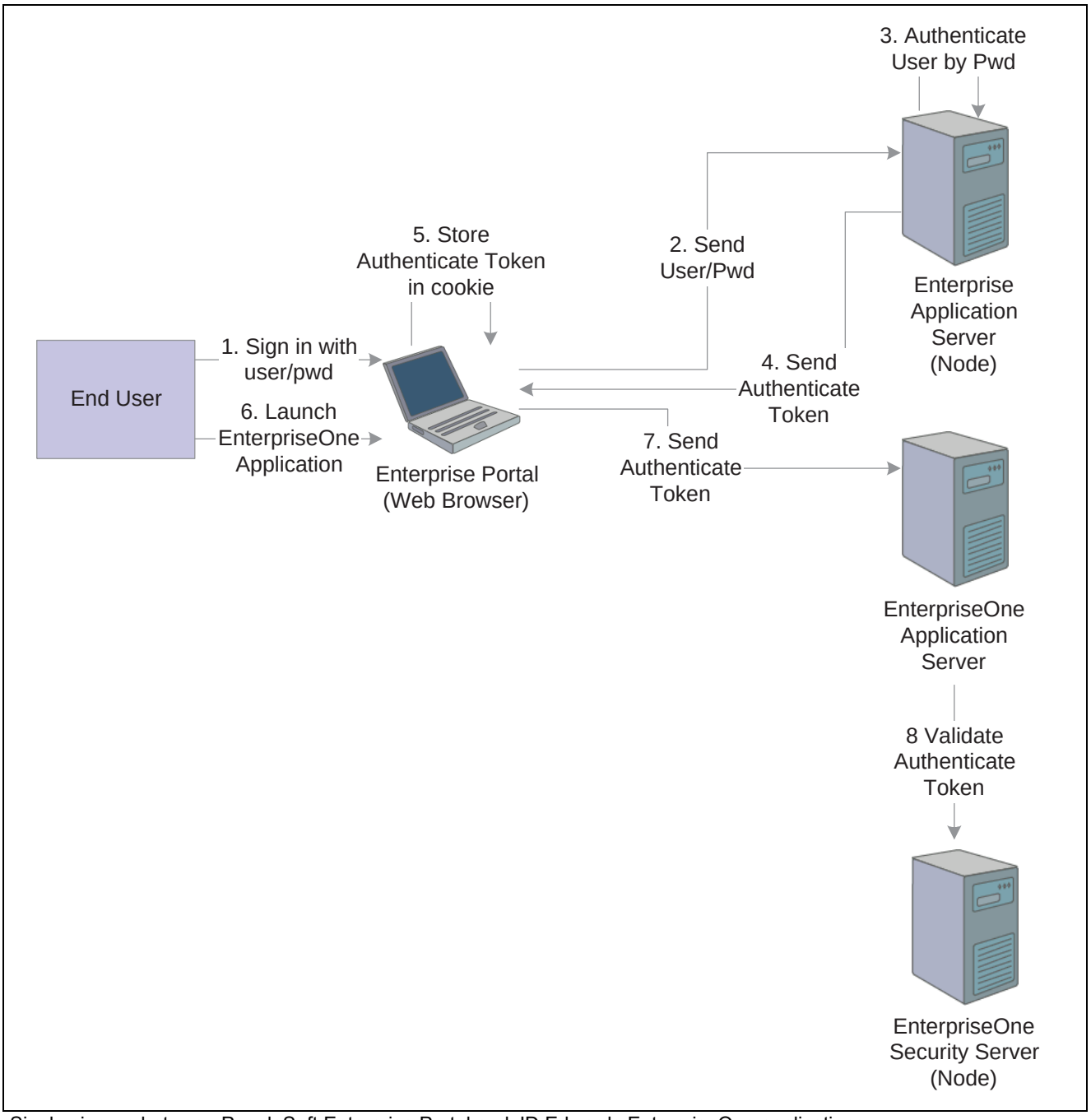
Single Sign-On Scenarios

This section discusses how single sign-on works in these scenarios:

- Launching a JD Edwards EnterpriseOne application from PeopleSoft Enterprise Portal.
- Launching a JD Edwards EnterpriseOne application from JD Edwards Collaborative Portal.

Launching a JD Edwards EnterpriseOne Application from PeopleSoft Enterprise Portal

The illustration and steps in this section explain how single sign-on works when a user signs in to PeopleSoft Enterprise Portal and launches a JD Edwards EnterpriseOne application:



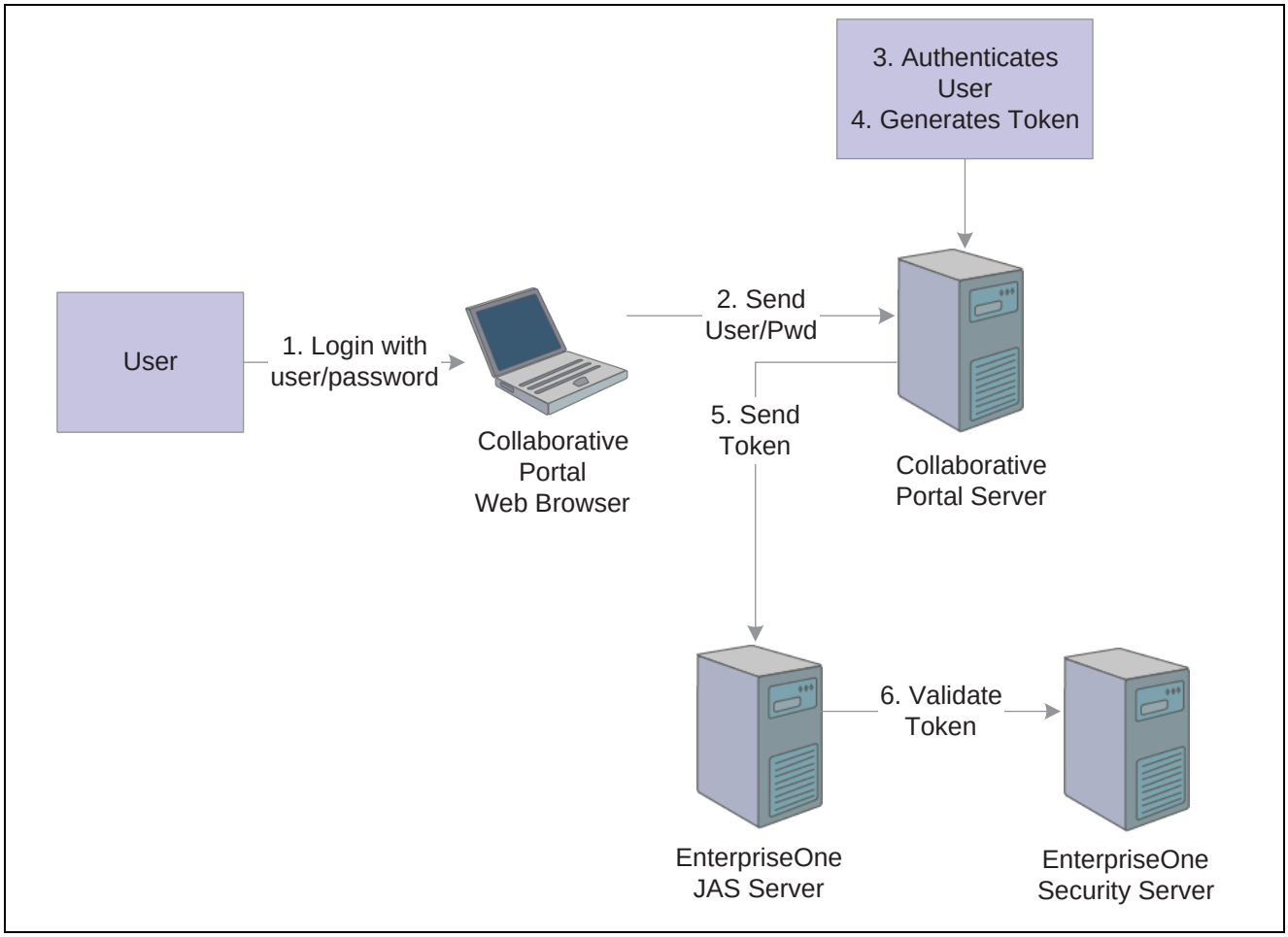
Single sign-on between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne applications

1. The user signs in to PeopleSoft Enterprise Portal in a Web browser using a PeopleSoft Enterprise user ID and password.
2. The web browser sends the user ID and password to the PeopleSoft Enterprise application server (node).
3. The PeopleSoft Enterprise application server authenticates the user credentials and generates an authenticate token.
4. The PeopleSoft Enterprise application server delivers a cookie containing an authenticate token to the Web browser.
5. The web browser stores the cookie on the local machine.

6. The end user tries to launch a JD Edwards EnterpriseOne application through PeopleSoft Enterprise Portal.
7. The PeopleSoft Enterprise Portal sends the authenticate token to the JD Edwards EnterpriseOne application server.
8. The JD Edwards EnterpriseOne application server validates the token (through the JD Edwards EnterpriseOne security server).

Launching a JD Edwards EnterpriseOne Application from JD Edwards Collaborative Portal

The illustration and steps in this section explain how single sign-on works when a user signs in to JD Edwards Collaborative Portal and launches a JD Edwards EnterpriseOne application:



Single Sign-on between JD Edwards Collaborative Portal and JD Edwards EnterpriseOne applications

1. The user signs in to JD Edwards Collaborative Portal through a web browser using a JD Edwards EnterpriseOne user ID and password.
2. The system sends the user ID and password to the JD Edwards Collaborative Portal.
3. JD Edwards Collaborative Portal authenticates the user ID and password against either LDAP, JD Edwards EnterpriseOne tables, or WebSphere security.
4. A token is generated for the user ID.

5. When single sign-on is required for JD Edwards EnterpriseOne, the token is sent to either a JAS Server or a JD Edwards EnterpriseOne application server.
6. The JD Edwards EnterpriseOne security server validates the token and grants access to the JD Edwards EnterpriseOne application.

CHAPTER 13

Setting Up JD Edwards EnterpriseOne Single Sign-On

This chapter provides an overview of the default settings for the single sign-on node configuration and discusses how to:

- Set up a node configuration.
- Set up a token lifetime configuration record.
- Set up a trusted node configuration.
- Configure single sign-on for a pre-EnterpriseOne 8.l1 release.
- Configure single sign-on without a security server.
- Configure single sign-on for JD Edwards Collaborative Portal.
- Configure single sign-on for portlets.
- Configure single sign-on between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne.

Understanding the Default Settings for the Single Sign-On Node Configuration

By default, when there is no configuration table specifications in the system and no configurations in the jde.ini file, the security server uses these settings for node information:

Setting	Description
Logical Node Name	_GLOBALNODE
Physical machine name	N/A (The default settings are all the same independent of the physical machine that it is residue in.)
Regular token timeout	12 hours
Extended token timeout	30 days
Trusted node	_GLOBALNODE

As a result, the EnterpriseOne system will generate a token with node name _GLOBALNODE, and it will only accept a token with node name _GLOBALNODE.

Note. Using default settings may expose a potential security risk. Thus, it is highly recommend to overwrite the single sign-on settings using the single sign-on configuration applications discussed in this section.

Setting Up a Node Configuration

This section provides an overview of the single sign-on configurations and discusses how to:

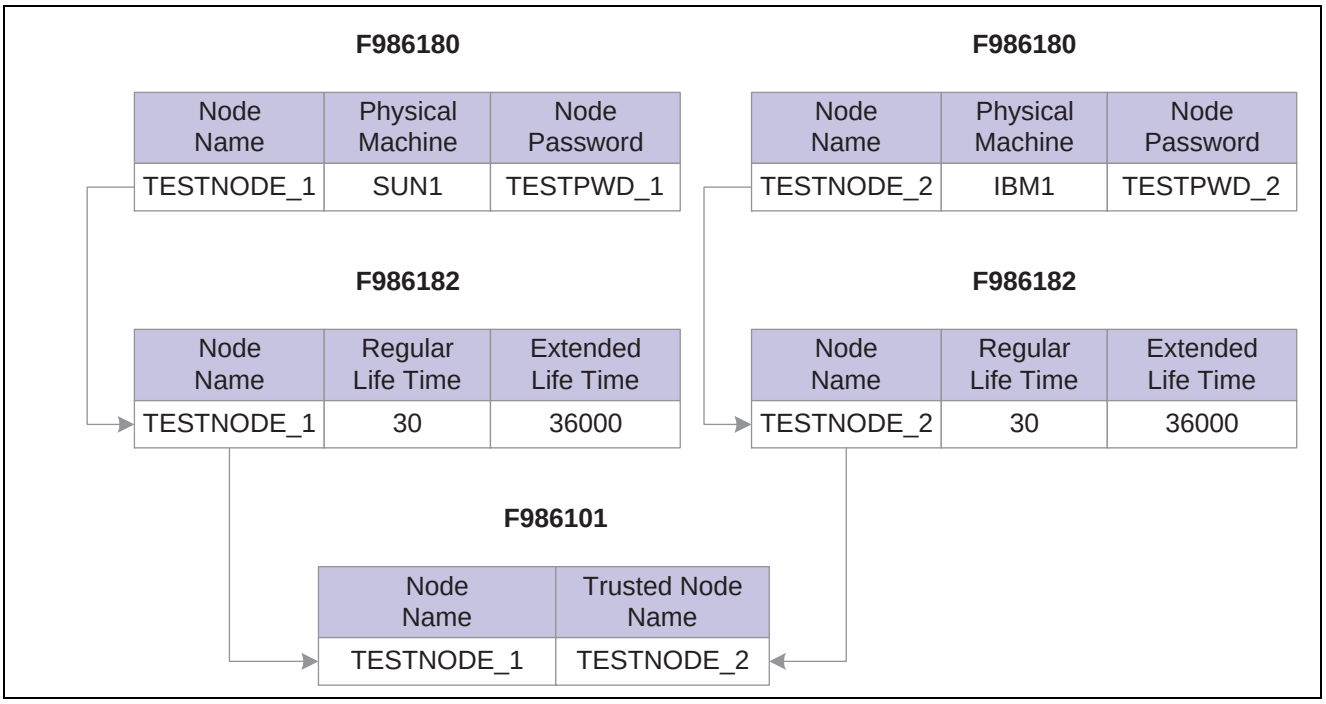
- Add a node configuration.
- Revise a node configuration
- Change the status of a node.
- Delete a node configuration.

Understanding Single Sign-On Configurations and Their Relationships

In JD Edwards EnterpriseOne, the node configurations are stored in a database. The node lifetime configuration is the configuration for the existing node, and the nodes in the trusted node configuration must have an existing node that has the lifetime configurations. The node properties are stored in these three database tables:

- Node Configuration Table (F986180). This table contains the information of a node in the single sign-on environment, such as the node name, description, machine name, node status (active/inactive), and the password.
- Node Lifetime Configuration Table (F986182): This table contains the lifetime information for an existing node. The node lifetime configuration information, such as the node name, regular token lifetime, and extended token lifetime.
- Trusted Node Configuration Table (F986181): This table contains the trust relationship between two nodes.

This diagram shows the relationship among these tables:



Single sign-on table relationships

This configuration requires that you configure the single sign-on settings in this order:

1. Set up node information.
2. Set up node lifetime.
3. Establish the trust between nodes.

You should delete the single sign-on settings in this order:

1. Delete the trusted node relationship.
2. Delete the node lifetime.
3. Delete the node information.

Alternatively, you can delete the node information directly by deleting the node record in the F986180 table. The system will automatically delete the record's corresponding entries in the Node Lifetime (F986181) and Trusted Node (F986182) tables.

Adding a Node Configuration

Access the SSO Environment Configuration Tools form. In JD Edwards Solution Explorer, select System Administration Tools (GH9011), User Management, User Management Advanced and Technical Operations, and then double-click SSO Environment Configuration Tools.

1. Click the Single Signon Node Configuration link.
2. On the Work With Node Configuration form, click Add.
3. On the SSO Node Configuration Revisions form, complete these fields:

Field	Description
Node Name	Enter a logical name associated with this node. The length of the node name cannot exceed 15 characters.
Node Description	Enter a description of the node.
Machine Name	Enter the physical machine name where the node resides.
Node Status	Specify whether the node is active or inactive.
Node Password	Enter a password for the node. The password ensures that tokens that are generated from the node do not get tampered with.
Verify Node Password	Re-enter the password.

Revising a Node Configuration

Access the Work With Node Configuration form.

1. Select a node and then click Select.
2. On SSO Node Configuration Revision, modify the appropriate fields.

Changing the Status of a Node

Access the Work With Node Configuration form.

Select the node and then from the Row menu, select Active/Inactive to change the status of the node.

Deleting a Node Configuration

Deleting an existing node configuration results in the removal of its lifetime configuration and trusted node configuration records in F986181 and F986182 respectively.

Access the Work With Node Configuration form.

1. Select the node that you want to delete and click Delete.

   A warning message appears informing you of the corresponding records that are deleted when you delete a node configuration.
2. Click OK to delete the node configuration.

Setting Up a Token Lifetime Configuration Record

A node that has a token lifetime configuration always generates a pair of lifetime configuration records—one for the regular token and one for the extended token. The trusted node configuration depends on the token lifetime configuration. You can add a pair of new token lifetime configuration records for an existing node.

This section discusses how to:

- Add a token lifetime configuration record.

- Delete a token lifetime configuration record.

Adding a Token Lifetime Configuration Record

Access the SSO Environment Configuration Tools form. In JD Edwards Solution Explorer, select System Administration Tools (GH9011), User Management, User Management Advanced and Technical Operations, and then double-click SSO Environment Configuration Tools.

1. Click the Single Signon Token Lifetime Configuration link.
2. On the Work With Token Lifetime Configuration form, click Add.
3. On the Token Lifetime Configuration Revision form, complete these fields:
   - Regular Token Lifetime

     Specify the expiration time for a regular token. The default value for a node is 720 minutes (12 hours).
   - Extended Token Lifetime

     Specify the expiration time for an extended token. The default value is 4320 minutes (three days). However, the recommended value for this setting is 43,200 minutes (30 days).

Deleting a Token Lifetime Configuration Record

Access the Work With Token Lifetime Configuration form.

Note. If one token lifetime configuration record is deleted, then another token lifetime configuration for the same node and the trusted node configurations that have this node in it will be deleted as well.

On the Work With Token Lifetime Configuration form, select a node and then click the Delete button.

Note. A dialog box appears warning you that if you delete this record, the system will delete the extended and regular token lifetime configuration records and the trusted node configuration records of this node.

Setting Up a Trusted Node Configuration

This section discusses how to:

- Add a trusted node configuration.
- Delete a trusted node configuration.

Adding a Trusted Node Configuration

The nodes that you add to a new trusted node configuration must already be defined and have token lifetime configuration records.

Access the SSO Environment Configuration Tools form. In JD Edwards Solution Explorer, select System Administration Tools (GH9011), User Management, User Management Advanced and Technical Operations, and then double-click SSO Environment Configuration Tools.

1. Click the Single Signon Trusted Node Configuration link.
2. On the Work With Trusted Node Configuration form, click Find, select a record, and then click Add.

3. On the Trusted Node Configuration Revision form, enter a node in the Node Name field and then click OK.

Deleting a Trusted Node Configuration

Access the Work With Trusted Node Configuration form.

Select a record and then click Delete.

Configuring Single Sign-On for a Pre-EnterpriseOne 8.11 Release

JD Edwards EnterpriseOne stores single sign-on node configuration information in new tables (F986180, F986181 and F986182). These tables are not available in pre-8.11 releases (such as release 8.94). However, you can still configure single sign-on for the pre-release through single sign-on node settings in the jde.ini file.

This section discusses how to:

- Modify jde.ini file node settings for single sign-on.
- Work with sample jde.ini node settings for single sign-on.

Modifying jde.ini file Node Settings for Single Sign-On

JD Edwards EnterpriseOne comes with standard default settings for single sign-on. If you do not want to accept the default settings, you can overwrite the default single sign-on node settings by configuring the jde.ini file.

See Chapter 13, "Setting Up JD Edwards EnterpriseOne Single Sign-On," Understanding the Default Settings for the Single Sign-On Node Configuration, page 167.

Access the jde.ini file to modify the single sign-on node settings.

In the [TRUSTED NODE] section of the jde.ini file, add the appropriate values to these settings:

Setting	Description
numTrustedNodes	Enter the number of trusted nodes.
RegularLifeTime	Enter the expiration time (in minutes) for a regular token.
ExtendedLifeTime	Enter the expiration time (in minutes) for an extended token.
NodeName	Enter the logical name for the first node.
MachineName	Enter the number of trusted nodes.
NodePassword	Enter the password for the first node.
NodeName1	Enter the logical name for the second node.

Setting	Description
MachineName1	Enter the physical machine name for the second node.
NodePassword1	Enter the password for the second node.

Working with Sample jde.ini Node Settings for Single Sign-On

This section contains examples of node settings in the jde.ini file for single sign-on configurations:

Example 1:

A system administrator wants to install the EnterpriseOne system on three machines: SUN1, IBM1 and HP1. He wants all three machines to trust each other, and no other machines will be trusted. In this case, the administrator can configure the jde.ini as follows and deploy it on SUN1, IBM1, and HP1:

```
[TRUSTED NODE]
numTrustedNodes=3
```

For Sun:

```
NodeName=NodeSUN1
MachineName=SUN1
NodePassword=NodePwd
```

For IBM:

```
NodeName1=NodeIBM1
MachineName1=IBM1
NodePassword1=IBM1Pwd
```

For HP:

```
NodeName2=NodeHP1
MachineName2=HP1
NodePassword2=HP1Pwd
```

Example 2:

A system administrator wants all EnterpriseOne servers in the network to trust each other. Moreover, he wants to change the default node configuration as follows:

- Change the node password to NewPwd.
- Change the regular token lifetime to 30 minutes instead of 12 hours.
- Change the extended token lifetime to 60 minutes instead of 30 days.

In this case, the administrator can configure the jde.ini as follows and deploy it to all the enterprise servers in the network:

```
[TRUSTED NODE]
numTrustedNodes=1
RegularLifeTime=30
ExtendedLifeTime=60
NodeName=_GLOBALNODE (The node name must be _GLOBALNODE)
MachineName=_GLOBALNODE (The machine name must be _GLOBALNODE)
NodePassword=NewPwd
```

Configuring Single Sign-On Without a Security Server

When there is no security kernel available in the system, a user can directly sign in to the JD Edwards EnterpriseOne Windows client without using the security server. To sign in to JD Edwards EnterpriseOne without a security server, you must:

- Set SecurityServer=<blank> in the [SECURITY] section of the client jde.ini file.
- Sign on to EnterpriseOne using the system (database) user ID and password.

In this case, the EnterpriseOne Windows client generates an authenticate token locally. This token is referred to as a local token. A local token is very similar to a regular token except that it has a fixed node name (_LOCALNODE) and contains the system user name and password. A local token can only be accepted by a local fat client or an enterprise server without a security server, for example SecurityServer=<blank> in the server jde.ini.

Note. If you sign in to JD Edwards EnterpriseOne without a security server, you can only run the business functions and UBEs that are mapped to either the local machine or the enterprise server without a security server.

When a local token is used, the default value for regular token lifetime is 12 hours and the default value for extended token lifetime is 30 days. You can override these default values for the local token using the SSO Environment Configuration Tools application or by modifying the appropriate settings in the jde.ini file of the Windows client, deployment server, and enterprise server.

These are sample jde.ini node settings to override _LOCALNODE for the local token:

```
[TRUSTED NODE]
numTrustedNodes=1
RegularLifeTime=4320
ExtendedLifeTime=43200
NodeName=_LOCALNODE
MachineName=_LOCALNODE
```

Note. You cannot override the node password for _LOCALNODE in the jde.ini file; you must use the SSO Environment Configuration Tools application to do this.

Configuring Single Sign-On for JD Edwards Collaborative Portal

The JD Edwards Collaborative Portal now uses token-based authentication for single sign-on between the JD Edwards Collaborative Portal and the JD Edwards EnterpriseOne HTML Web Server or EnterpriseOne enterprise server.

Portlets that access information on JD Edwards EnterpriseOne server generate a token based on the user ID, and send the token to the JD Edwards EnterpriseOne server. The server validates the token and enables the user to sign in. The requested information is returned to the portlet.

The token-based system requires that the JD Edwards Collaborative Portal user ID and the JD Edwards EnterpriseOne user ID are the same or that a mapping be set up for the user IDs on the JD Edwards EnterpriseOne server.

Note. If JD Edwards EnterpriseOne and JD Edwards Collaborative Portal are sharing an LDAP instance, this is not an issue. Since JD Edwards EnterpriseOne only accepts uppercase user IDs in its database, JD Edwards Collaborative Portal will also require uppercase user IDs for the generated token to be validated.

See Also

Chapter 13, "Setting Up JD Edwards EnterpriseOne Single Sign-On," Managing User ID Mapping in JD Edwards EnterpriseOne, page 178

Configuring Single Signon for Collaborative Portal in the *JD Edwards EnterpriseOne Tools 8.97 Collaborative Portal Reference Guide*

Configuring Single Sign-On for Portlets

This section provides information on how to modify the TokenGen.ini file settings for single sign-on and contains single sign-on configuration information for these portlets:

- EnterpriseOne Portlet (JSR168)
- Collaborative Portal EnterpriseOne Menu
- Hosted EnterpriseOne Portlet
- CSS, ESS, SSS
- EnterpriseOne Links
- CRM

Modifying TokenGen.ini File Settings

Single sign-on requires that you change the TokenGen.ini settings for Node Name and Node Password to correspond to the entries in the JD Edwards EnterpriseOne security server. The values shown in the [NODE MANAGER] section are for a default install:

```
[NODE MANAGER]
NodeName=_GLOBALNODE
NodePwd=_GLOBALPWD
```

To modify these settings after the install, locate the TokenGen.ini file in this directory:

<*WebSphere home*>/properties

EnterpriseOne Portlet (JSR168)

With the EnterpriseOne portlet, the JAS server runs as part of the portlet rather than being connected to remotely. This also means that the EnterpriseOne portlet uses the jas.ini and jdbj.ini files that were installed as part of the JD Edwards Collaborative Portal install.

The user IDs must be synchronized between the JD Edwards Collaborative Portal and the JD Edwards EnterpriseOne user database. If the default environment and role are set in the OWWEB section of the jas.ini, these entries will be used for all users. If no default entries are set, the user will be asked to choose from a list of environments and roles when they go to a page with the JD Edwards EnterpriseOne portlet on it.

When multiple JD Edwards EnterpriseOne portlets are placed on a page, only one of the portlets displays the environment and role list. The other portlets display the warning message, "This portlet is waiting for authentication to be completed."

See Also

JD Edwards EnterpriseOne Tools 8.96 HTML Web Server Reference Guide for information about the jas.ini file settings

Collaborative Portal EnterpriseOne Menu

Before release 8.11, EnterpriseOne Menu (then called Task Explorer) used inherited trust for single sign-on. As of 8.11, the portlet uses the authenticate token. The environment and role are configured through the configuration screen of the portlet by the administrator. Alternatively, the default environment and role can be set in the jas.ini of the remote JAS server.

Hosted EnterpriseOne Portlet

Before release 8.11, the Hosted EnterpriseOne Portlet used inherited trust for single sign-on. As of release 8.11, the portlet uses the authenticate token. Environment and role are configured through the edit screen by each user. Alternatively, the administrator can set the default environment and role in the jas.ini of the remote EnterpriseOne JAS server.

CSS, ESS, SSS

Before release 8.11, these portlets used inherited trust for single sign-on. As of release 8.11, these portlets use the authenticate token. The environment and role are set through the portlet configuration screen by the administrator.

EnterpriseOne Links

Before release 8.11, EnterpriseOne Links used inherited trust for single sign-on. As of release 8.11, this portlet uses the authenticate token. The environment and role are still set through the portlet configuration screen by the administrator.

CRM

The CRM portlets, based on the Youcentric technology, continue to use the inherited trust system for single sign-on. CRM portlets included in the 8.11 JD Edwards EnterpriseOne solution are included in the EnterpriseOne portlet.

Configuring Single Sign-On Between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne

This section provides an overview of setting up single sign-on between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne and discusses how to:

- Manage user ID mapping in JD Edwards EnterpriseOne.
- Manage user ID mapping when using LDAP.

- Synchronize user mapping between LDAP and JD Edwards EnterpriseOne while using LDAP authentication.
- View user ID mapping when using LDAP.

Understanding Single Sign-On Between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne

Prior to JD Edwards EnterpriseOne release 8.11, single sign-on between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne was accomplished as follows:

1. PeopleSoft Enterprise Portal generated a token and sent it to JD Edwards EnterpriseOne.
2. JD Edwards EnterpriseOne called back to the PeopleSoft Enterprise Portal application server to validate token and received back a user ID.
3. The system used the user ID to sign on to JD Edwards EnterpriseOne.

Since JD Edwards EnterpriseOne can validate and sign on with a token generated by the PeopleSoft Enterprise Portal, it is no longer necessary to call back to the PeopleSoft Enterprise Portal side to validate the token. This simplification of the single sign-on setup between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne means that the following items are no longer required:

- The psjoa.jar, psft.jar, and PeopleSoft.Generated.CompIntfc.jar files in the JD Edwards EnterpriseOne system. The latest JD Edwards Collaborative Portal installer does not install these files.
- The PeopleSoftAppServer, PeopleSoftAppServerUser, and PeopleSoftAppServerPassword jas.ini entries in the OWWEB section.
- The DBUser and DBPassword entries in the jas.ini are no longer required in the SECURITY section.
- The setup of the component interface (PRTL_SS_CI) on the PeopleSoft Enterprise Portal. Additionally, the admin user for accessing this interface no longer needs to be set up.
- The entry in the PSTRUSTNODES table on the PeopleSoft Enterprise Portal for the local node.

Note. The environment and role entries are still set up the same as in previous releases, as defaults in the jas.ini on the JD Edwards EnterpriseOne HTML Web Server.

See *JD Edwards EnterpriseOne Tools 8.97 HTML Web Server Reference Guide*

Time Zone Adjustment for PeopleSoft Enterprise Portal

When setting up single sign-on between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne, you must properly configure the ENTERPRISE TIMEZONE ADJUSTMENT setting in the JD Edwards EnterpriseOne enterprise server jde.ini file. This setting enables you to enter the difference in time between Greenwich Mean Time (GMT) and PeopleSoft Enterprise Portal Node time. You should change this setting whenever daylight saving time changes to reflect the difference between GMT time and the PeopleSoft Enterprise Portal Node time.

In this example of the ENTERPRISE TIMEZONE ADJUSTMENT setting, the difference between the GMT and PeopleSoft Enterprise Portal Node time is entered in minutes for a PeopleSoft Enterprise Portal that is running in Mountain Standard Time (MST):

```
[ENTERPRISE TIMEZONE ADJUSTMENT]
EntNode=-360
```


User ID Mapping for Single Sign-On

Since PeopleSoft Enterprise and JD Edwards EnterpriseOne systems have different user IDs, you must map the user IDs between the two systems in order for single sign-on to work. If you manage user IDs in a JD Edwards EnterpriseOne database, then you can use a JD Edwards EnterpriseOne application to map users. If you use LDAP to manage user information such as user IDs, passwords, and role relationships, then you must use the third-party LDAP tool to set up user ID mapping.

Managing User ID Mapping in JD Edwards EnterpriseOne

Access the SSO Environment Configuration Tools form. In JD Edwards Solution Explorer, select System Administration Tools (GH9011), Security Maintenance, Security Maintenance Advanced and Technical Operations, SSO Environment Configuration Tools.

1. Click the Configure the UserID Mapping link.
2. On the Work with SSO E/E1 UserID Mapping form, use the Add, Select, and Delete buttons to manage user ID mappings.
3. To add a user ID mapping, click Add.
4. On the SSO E/E1 userID Mapping Revisions form, complete the EnterpriseOne UserID and Enterprise UserID fields.

   The system saves the record in the F00927 table.

Note. If the JD Edwards EnterpriseOne user ID is not in the F0092 table, the system generates an error stating that it cannot add the mapping record.

Managing User ID Mapping when Using LDAP

JD Edwards EnterpriseOne can use LDAP (Lightweight Data Access Protocol) to manage user IDs, password, and role relationships. If the JD Edwards EnterpriseOne system is LDAP-enabled, this setting must be added to the jde.ini file:

```
[SECURITY]
LDAPAuthentication=true
```

See Also

Chapter 11, “Enabling LDAP Support in JD Edwards EnterpriseOne,” page 125

Synchronizing User Mappings Between LDAP and JD Edwards EnterpriseOne While Using LDAP Authentication

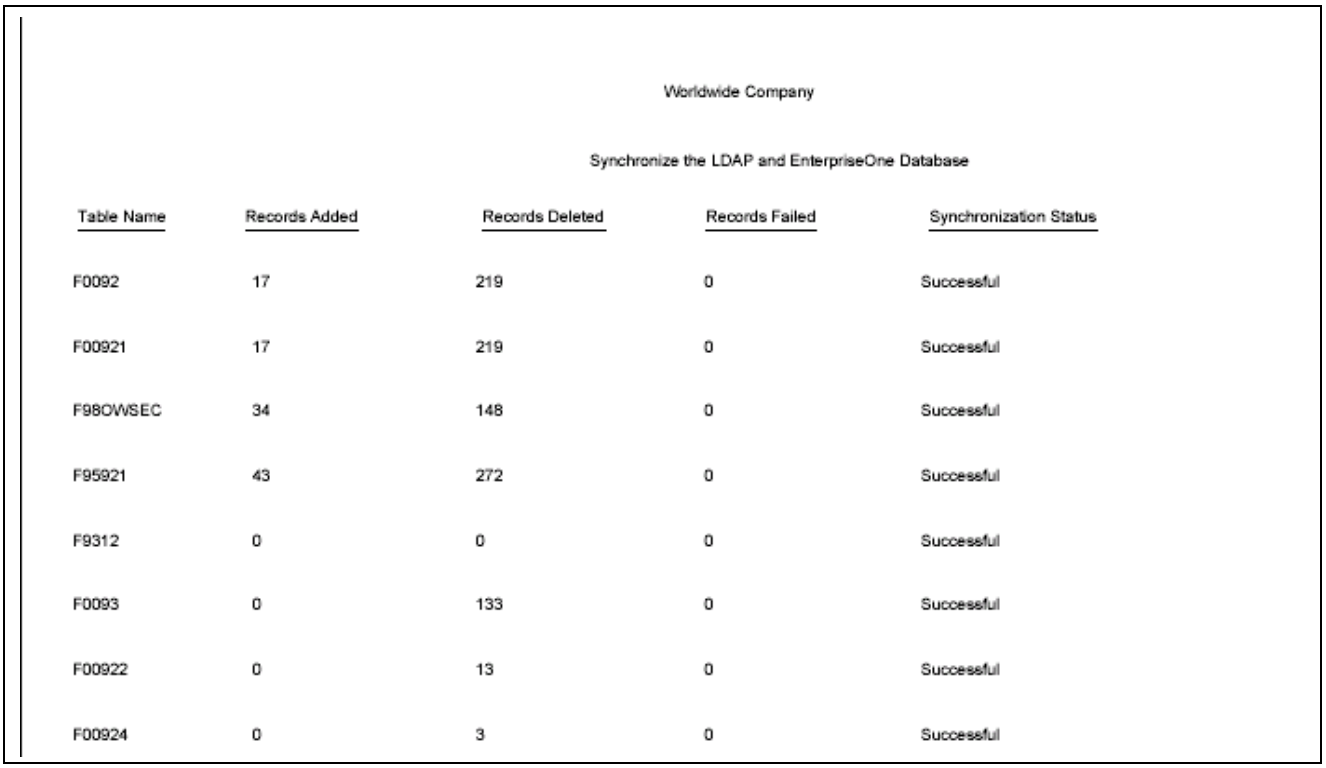
JD Edwards EnterpriseOne provides an optional batch application, Synchronize the LDAP and EnterpriseOne Database (R9200040), that you can run to synchronize all of the user mappings between the LDAP and JD Edwards EnterpriseOne databases. The user mapping synchronization also occurs when a user signs in to JD Edwards EnterpriseOne. However, the synchronization only applies to the user who just signed in. Therefore, you should run R9200040 to:

- Synchronize all users.
- Purge obsolete users (such as the users that have already been removed from LDAP) from the database.

Note. You should be extremely cautious when running this batch application since it not only synchronizes user mappings, but also synchronizes other user profile settings such as user-role relationships. Moreover, it will delete all the users that do not exist in LDAP.

To synchronize all user mappings between the LDAP and JD Edwards EnterpriseOne databases, run the R9200040 batch application:

This is an example of the results of running the R9200040 batch application:



Worldwide Company

Synchronize the LDAP and EnterpriseOne Database

Table Name	Records Added	Records Deleted	Records Failed	Synchronization Status
F0092	17	219	0	Successful
F00921	17	219	0	Successful
F98OWSEC	34	148	0	Successful
F95921	43	272	0	Successful
F9312	0	0	0	Successful
F0093	0	133	0	Successful
F00922	0	13	0	Successful
F00924	0	3	0	Successful

R9200040 output

Viewing User ID Mapping When Using LDAP

When using LDAP to manage user sign-on information, you can still view the user ID mappings for single sign-on through JD Edwards EnterpriseOne.

Access the SSO Environment Configuration Tools form. In JD Edwards Solution Explorer, select System Administration Tools (GH9011), Security Maintenance, SSO Environment Configuration Tools.

1. On the SSO Environment Configuration Tools form, click the View UserID Mapping option.
2. On the Work with SSO E/E1 UserID Mapping form, select a mapping record and then click the Select button to view the mapping.

CHAPTER 14

Understanding Single Sign-On Between JD Edwards EnterpriseOne and Oracle

Single sign-on between JD Edwards EnterpriseOne and Oracle enables users to sign in once to access both JD Edwards EnterpriseOne and Oracle single sign-on enabled applications. This chapter provides a list of prerequisites and discusses:

- Oracle single sign-on components.
- Supported JD Edwards EnterpriseOne and Oracle single sign-on configurations.
- Single sign-on when running JD Edwards EnterpriseOne on Oracle Application Server.
- Single sign-on when running JD Edwards EnterpriseOne on IBM WebSphere.
- Non-web client sign-on in the Oracle single sign-on configuration.

Note. In addition, you can enable support of long user IDs and passwords in a JD Edwards EnterpriseOne single sign-on configuration with Oracle Access Manager or Oracle AS Single Sign-On Server. See "Using Long User IDs and Passwords in JD Edwards EnterpriseOne" in the Red Paper Library on Customer Connection for more information.

Prerequisites

The Oracle Identity Management infrastructure must be installed as part of the Oracle Application Server setup. See the *Oracle Identity Manager Installation Guide for Oracle Application Server* for more information.

When installing JD Edwards EnterpriseOne HTML Web Server on Oracle Application Server, the OracleAS Single Sign-On option must be enabled.

See *JD Edwards EnterpriseOne Tools 8.97 Server Manager Guide*

If you are running JD Edwards EnterpriseOne web applications on IBM WebSphere Application Server instead of Oracle Application Server, the PeopleSoft SSO Plug-In must be installed on the OracleAS Single Sign-On server.

See the Customer Connection web site for information on how to install this plug-in.

Oracle Single Sign-On Components

Configuring single sign-on between JD Edwards EnterpriseOne and Oracle applications requires a thorough understanding of the Oracle Identity Management infrastructure within Oracle Application Server. Oracle Identity Management provides the framework that supports single sign-on. OracleAS Single Sign-On is the component within Oracle Identity Management that works with these other components to enable single sign-on:

- Single sign-on server.
- Partner applications.
- mod_osso.
- Oracle Internet Directory.
- Oracle Identity Management infrastructure.

Single Sign-On Server

The single sign-on server consists of program logic in the Oracle Application Server database, Oracle HTTP Server, and OC4J server that enables you to sign in securely to applications. The single sign-on server enables access to several applications by authenticating only once.

Partner Applications

OracleAS applications delegate the authentication function to the single sign-on server. For this reason, they are called partner applications. An authentication module called mod_osso enables these applications to accept authenticated user information instead of a user name and password once users have signed in to the single sign-on server. A partner application is responsible for determining whether a user authenticated by OracleAS Single Sign-On is authorized to use the application.

Examples of partner applications include OracleAS Portal, OracleAS Discoverer, and Oracle Delegated Administration Services. When JD Edwards EnterpriseOne is installed on Oracle Application Server, it is also considered a partner application.

mod_osso

mod_osso is an Oracle HTTP Server module that provides authentication to OracleAS applications. Located on the application server, mod_osso simplifies the authentication process by serving as the sole partner application to the single sign-on server. In this way, mod_osso renders authentication transparent to partner applications.

Oracle Internet Directory

Oracle Internet Directory is the repository for all single sign-on user accounts and passwords—administrative and non-administrative. The single sign-on server authenticates users against their entries in the directory. At the same time, it retrieves user attributes form the directory that enable applications to validate users.

Oracle Identity Management Infrastructure

OracleAS Single Sign-On is just one link in an integrated infrastructure that also includes these components:

- Oracle Internet Directory
- Oracle Directory Integration and Provisioning
- Oracle Delegated Administrative Services
- OracleAS Certificate Authority

Working together, these components, called the Oracle Identity Management infrastructure, manage the security life cycle of users and other network entities in an efficient, cost-effective way.

See Also

Oracle Application Server Single Sign-On Administrator's Guide

Oracle Identity Management Integration Guide

Supported JD Edwards EnterpriseOne and Oracle Single Sign-On Configurations

Single sign-on is supported between JD Edwards EnterpriseOne web applications and OracleAS Single Sign-On enabled applications.

Note. JD Edwards EnterpriseOne non-web client applications, such as Windows client, JAVA Connector, and COM Connector, do not use OracleAS Single Sign-On for authentication.

How single sign-on works between JD Edwards EnterpriseOne and Oracle depends upon your implementation:

- JD Edwards EnterpriseOne HTML Web Server installed on Oracle Application Server.

  In this configuration, single sign-on is bi-directional. This means that whichever system users sign in to first, JD Edwards EnterpriseOne or Oracle, they do not have to sign in again to access an application in the other system.

- JD Edwards EnterpriseOne HTML Web Server installed on IBM WebSphere.

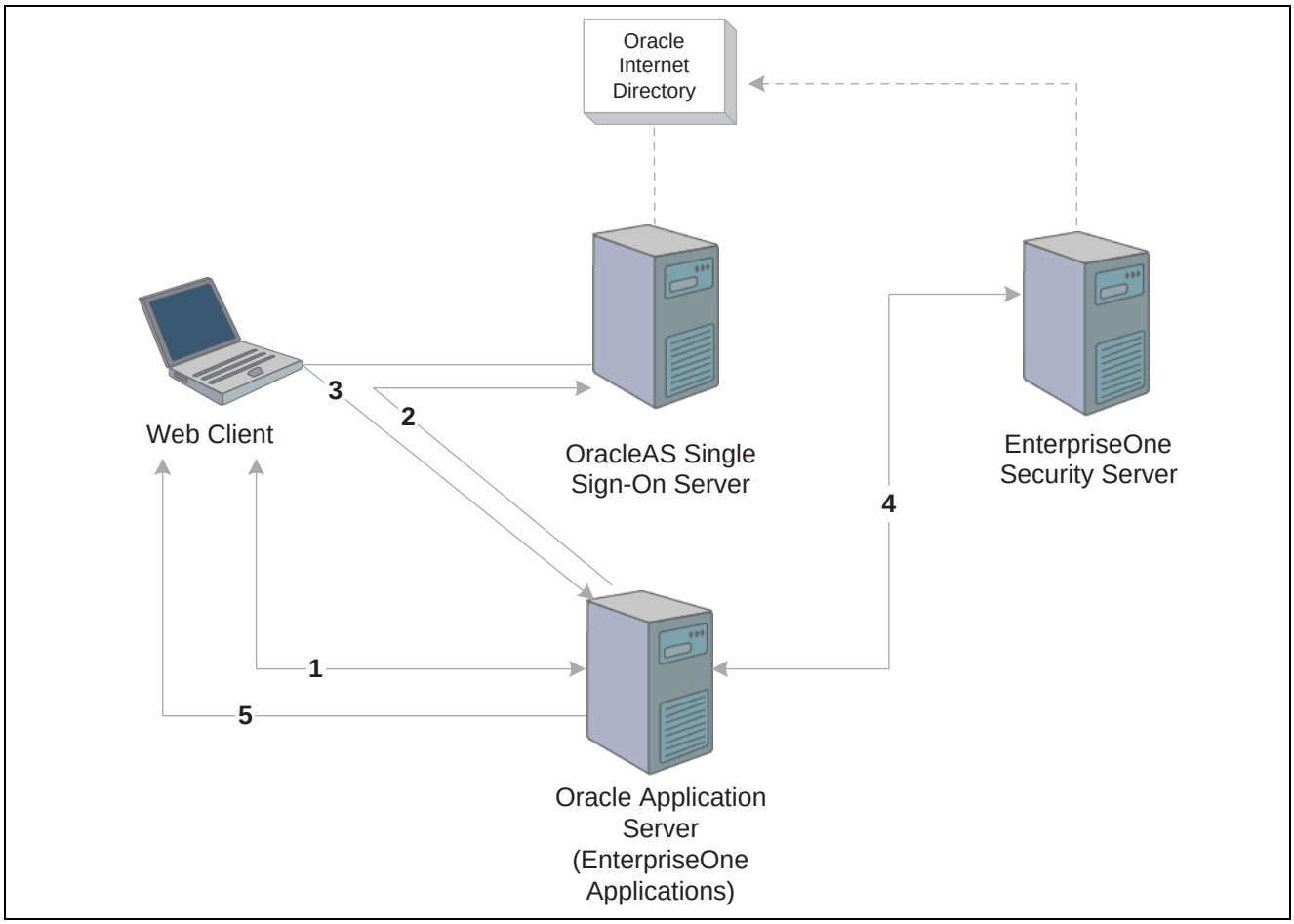
  In this configuration, single sign-on is unidirectional. If users have already signed in to Oracle Application Server, they can access a JD Edwards EnterpriseOne application without having to re-enter a user name and password. However, in this configuration, if users sign in to JD Edwards EnterpriseOne first, they cannot access an Oracle application through single sign-on. They will have to re-enter a user ID and password.

In addition, JD Edwards EnterpriseOne provides single sign-on from Oracle Portal, enabling users to access a JD Edwards EnterpriseOne application inside Oracle Portal. For more information, see the *JD Edwards EnterpriseOne Tools 8.96 Portlet Installation for the Oracle Portal Guide.*

Single Sign-On when Running JD Edwards EnterpriseOne on Oracle Application Server

When JD Edwards EnterpriseOne HTML Web Server is running on Oracle Application Server, JD Edwards EnterpriseOne delegates user authentication to the OracleAS Single Sign-On server. The mod_osso authentication module enables JD Edwards EnterpriseOne applications to accept authenticated user information instead of a user name and password once users have signed in to OracleAS Single Sign-On server. JD Edwards EnterpriseOne determines whether a user authenticated by OracleAS Single Sign-On is authorized to use the application.

This diagram shows the single sign-on process when JD Edwards EnterpriseOne HTML Web Server is running on Oracle Application Server:



JD Edwards EnterpriseOne and OracleAS single sign-on

These steps explain the single sign-on process illustrated in the diagram:

1. A user signs in to an Oracle partner application (either a JD Edwards EnterpriseOne or Oracle web application).
2. Using mod_osso, the partner application redirects the request to the OracleAS Single Sign-On server.
3. The OracleAS Single Sign-On server authenticates the user ID and password, generates an Oracle SSO cookie, and redirects the request to the JD Edwards EnterpriseOne partner application on Oracle Application Server.
4. Based on the Oracle SSO cookie, JD Edwards EnterpriseOne generates an authenticate token (PS_TOKEN) and sends it to the JD Edwards EnterpriseOne security server to validate the token, which enables the user to sign in.
5. A session is established for the web user.

Note. In the diagram, Oracle Internet Directory can be used as an LDAP directory for the JD Edwards EnterpriseOne security server.

Single Sign-Off

Signing off of a JD Edwards EnterpriseOne application terminates the single sign-on session, which in turn signs off all active Oracle partner applications. When you click Sign Out in a JD Edwards EnterpriseOne application, the system takes you to the single sign-off page, where sign-off occurs. If you signed off successfully, each of the applications listed on the single sign-off page has a check mark next to the application name. A broken image next to an application name denotes an unsuccessful sign-off.

Once all of the application names activated in a session have a check mark, you can click Return to go to the application from which you initiated sign-off.

Signing off an Oracle application takes you to the single sign-off page as well. This closes any Oracle applications that are running. However, any JD Edwards EnterpriseOne applications that are open remain active. Only when a user accesses the JD Edwards EnterpriseOne application does JD Edwards EnterpriseOne check if the Oracle SSO cookie is present. If it is not, the system ends the JD Edwards EnterpriseOne session and redirects the user to the Oracle Single Sign-On page for sign-in.

JD Edwards EnterpriseOne Single Sign-On Settings when Running on Oracle Application Server

Part of configuring single sign-on between JD Edwards EnterpriseOne and Oracle involves enabling the Oracle single sign-on option during the JD Edwards EnterpriseOne HTML Web Server installation. This section contains the Oracle single sign-on settings that are configured during the install, as well as additional settings that can be configured after the install.

See *JD Edwards EnterpriseOne Tools 8.97 Server Manager Guide* and the *JD Edwards EnterpriseOne Tools 8.97 HTML Web Server Reference Guide*

JD Edwards EnterpriseOne jas.ini Settings

When the Oracle single sign-on option is selected in the JD Edwards EnterpriseOne HTML Web Server installation, the system delegates JD Edwards EnterpriseOne user authentication to OracleAS Single Sign-On. The installer configures this setting in the [SECURITY] section of the jas.ini file:

Setting	Purpose
OracleSSO=	Determines if OracleAS Single Sign-On is used for user authentication. Valid values are: • TRUE • FALSE (default)

Another setting in the [SECURITY] section controls the functionality of the Return link on the Single Sign-Off web page. You can configure this setting *after* the JD Edwards EnterpriseOne HTML Web Server install:

Setting	Purpose
OracleSSOSignOffURL=	Determines the web page that the Return link accesses from the Oracle Single Sign-Off web page when the user signs off from JD Edwards EnterpriseOne. Enter a URL for the web page that you want users to access from the Return link. The default is the URL for accessing the JD Edwards EnterpriseOne web client.

JD Edwards EnterpriseOne TokenGen.ini Settings

JD Edwards EnterpriseOne uses the TokenGen.ini file to generate an authenticate token (PS_TOKEN). A common key is required for the encryption and decryption of the authenticate token. This key is set during the JD Edwards EnterpriseOne HTML Web Server installation and is saved in the TokenGen.ini file. The key consists of the node name and node password, as well as other parameters that *must not* be modified:

Setting	Default Value
NodeName=	*NodeName*
NodePwd=	*NodePassword*
CLIENTTYPE=	1
CODEPAGE	0
VERSION=	700
TOOLSVERSION=	8.10
SIGNATURETYPE=	N
MNRD	0

If you configured single sign-on settings on the JD Edwards EnterpriseOne security server, you can change the NodeName and NodePassword settings during the JD Edwards EnterpriseOne HTML Web Server installation.

When the single sign-on node has not been configured on the JD Edwards EnterpriseOne security server, the installer displays the default values for the Node Name and Node Password.

After the JD Edwards EnterpriseOne HTML Web Server is installed, you can change the values for the node name and node password to correspond to the entries on your JD Edwards EnterpriseOne security server, if necessary. It will require the restart of JD Edwards EnterpriseOne HTML Web Server.

See Also

Chapter 12, “Understanding JD Edwards EnterpriseOne Single Sign-On,” page 159

Settings for Configuring JD Edwards EnterpriseOne Virtual Hosts with Oracle Single Sign-On

Single sign-on partner applications are integrated with mod_osso, which is registered automatically by the OracleAS installer. In essence, partner applications are registered by way of mod_osso. Registering the module creates an entry for it in the identity management infrastructure database as well as on the application computer.

When the JD Edwards EnterpriseOne HTML Web Server is configured with a port other than the default port (which is typically 80), you should register JD Edwards EnterpriseOne HTML Web Server with the other port using mod_osso. Using port 90 as an example, these commands show how to register JD Edwards EnterpriseOne HTML Web Server using mod_osso:

```
SET ORACLE_HOME=C:\OracleAppSrv
%ORACLE_HOME%\sso\bin\ssoreg.bat -oracle_home_path %ORACLE_HOME% -site_name App⇒
Server90.eone.jdedwards.com -config_mod_osso TRUE -mod_osso_url http:⇒
//eone.jdedwards.com:90 -virtualhost -config_file %ORACLE_HOME%\Apache\Apache⇒
```



```
\conf\osso\port90\osso.conf
%ORACLE_HOME%/dcm/bin/dcmctl updateConfig -v -d
```

For additional information on how to configure virtual hosts with Oracle Single Sign-On, see "Configuring mod_osso with Virtual Hosts" in the *Oracle® Application Server Single Sign-On Administrator's Guide.*

Single Sign-On When Running JD Edwards EnterpriseOne on IBM WebSphere

When JD Edwards EnterpriseOne HTML Web Server is running on IBM WebSphere, single sign-on is unidirectional. Users must first sign in to an Oracle application using Oracle Single Sign-On. Only then can they access a JD Edwards EnterpriseOne application in the same session without having to re-enter their user ID and password. If users access a JD Edwards EnterpriseOne web application first, the JD Edwards EnterpriseOne sign-in screen appears; the sign-in request does not redirect users to the Oracle Single Sign-On page.

This solution is similar to JD Edwards EnterpriseOne single sign-on from the PeopleSoft Enterprise Portal, which uses the authenticate token.

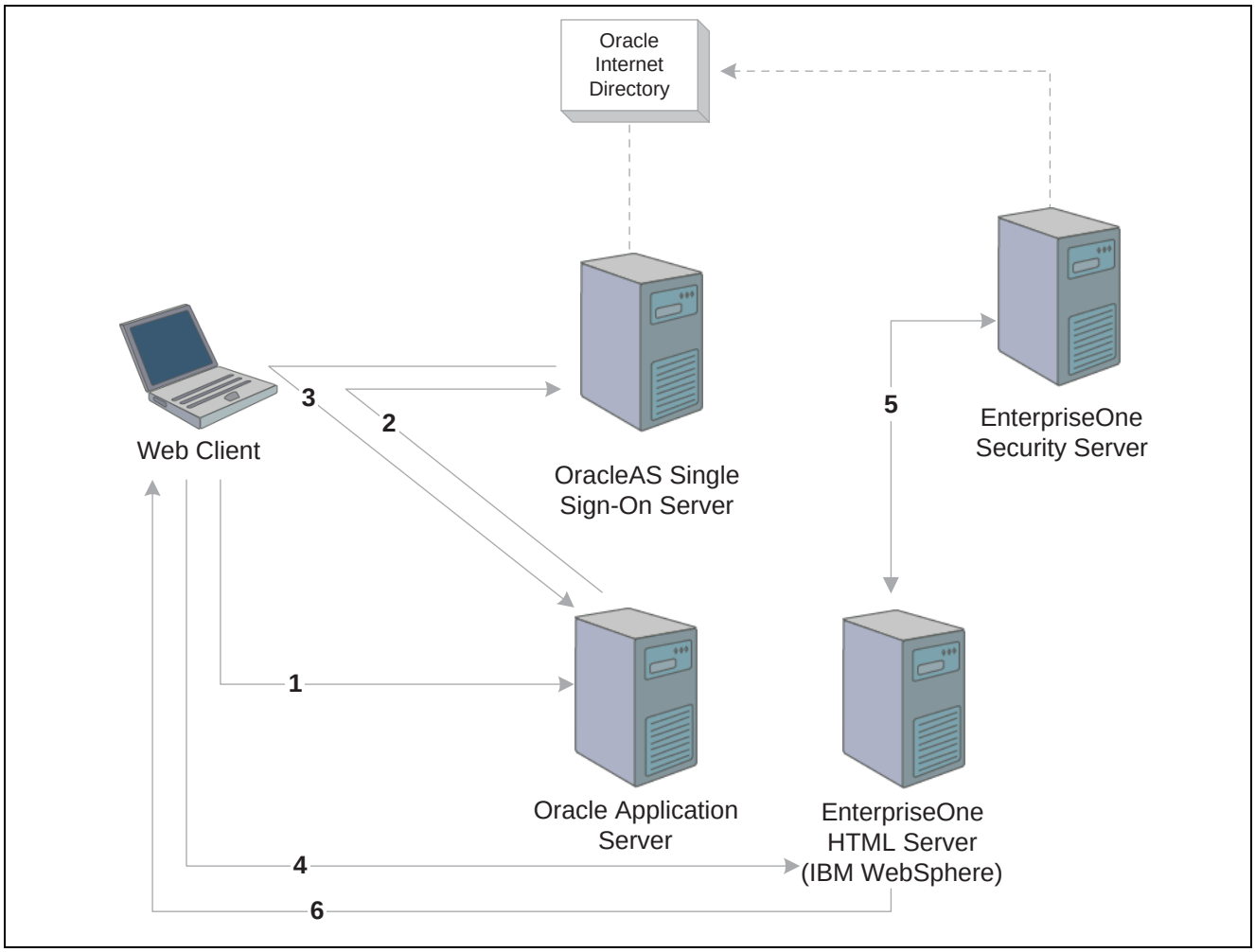
See Chapter 13, "Setting Up JD Edwards EnterpriseOne Single Sign-On," Configuring Single Sign-On Between PeopleSoft Enterprise Portal and JD Edwards EnterpriseOne, page 176.

In this configuration, Oracle AS Single Sign-On uses the PeopleSoft SSO Plug-In to achieve single sign-on with JD Edwards EnterpriseOne. The plug-in, which must be installed on the OracleAS Single Sign-On server, generates an authenticate token that IBM WebSphere uses to achieve single sign-on.

See Customer Connection web site for information on how to download and install this plug-in.

Note. Single sign-off between Oracle and JD Edwards EnterpriseOne is not supported when JD Edwards EnterpriseOne is running on IBM WebSphere. When you sign off of JD Edwards EnterpriseOne, the system ends the JD Edwards EnterpriseOne session, but any Oracle application sessions that are open continue to run. You must close the browser to sign in to JD Edwards EnterpriseOne again. Signing off of an Oracle application ends the OracleAS Single Sign-On session, as well as any other Oracle applications that were active in the session; however, any JD Edwards EnterpriseOne applications that are open will remain active.

This illustration shows the single sign-on process when JD Edwards EnterpriseOne HTML Web Server is running on IBM WebSphere:



JD Edwards EnterpriseOne and OracleAS single sign-on with IBM WebSphere

These steps explain the single sign-on process illustrated in the diagram:

1. A user signs in to an Oracle partner application on Oracle Application Server.
2. Using mod_osso, the partner application redirects the request to the OracleAS Single Sign-On server.
3. OracleAS Single Sign-On authenticates the user ID and password, generates an Oracle SSO cookie and PS_TOKEN cookie, and redirects the request to the partner application on Oracle Application Server.
4. When the same user tries to launch a JD Edwards EnterpriseOne application in the same session, the browser sends the request to the JD Edwards EnterpriseOne HTML Web Server running on IBM WebSphere.
5. The JD Edwards EnterpriseOne HTML Web Server sends the PS_TOKEN to the JD Edwards EnterpriseOne security server to validate the token.
6. Upon validation, IBM WebSphere establishes a session for the web user.

Note. In this diagram, Oracle Internet Directory can be used as an LDAP directory for JD Edwards EnterpriseOne.

Time Zone Setting Adjustment

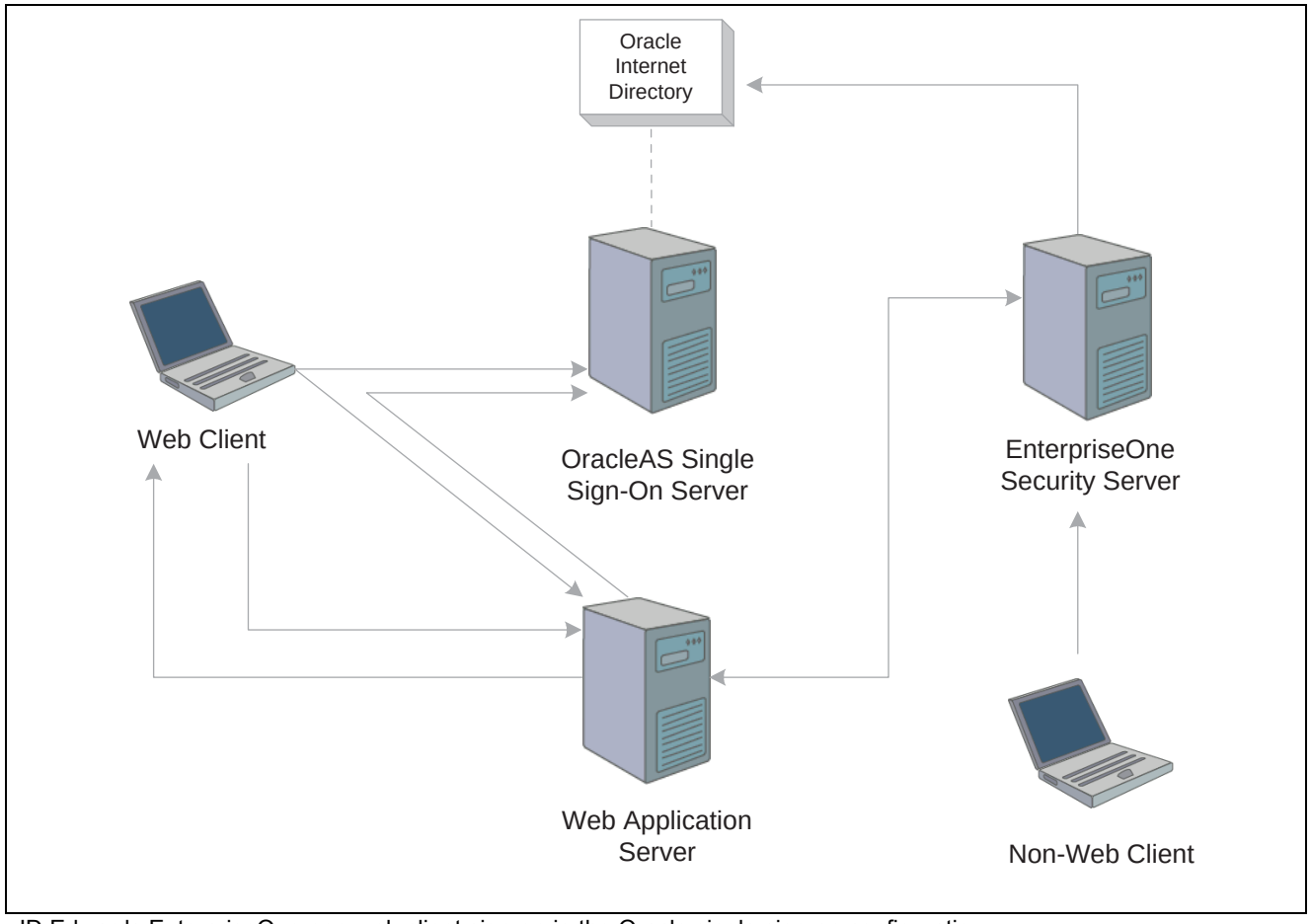
When JD Edwards EnterpriseOne is running on IBM WebSphere, you must configure the ENTERPRISE TIMEZONE ADJUSTMENT setting in the JD Edwards EnterpriseOne enterprise server jde.ini file. This setting enables you to enter the difference in time between Greenwich Mean Time (GMT) and OracleAS Single Sign-On node time. You should change this setting whenever daylight saving time changes to reflect the difference between GMT time and the OracleAS Single Sign-On node time.

In this example of the ENTERPRISE TIMEZONE ADJUSTMENT setting, the difference between the GMT and OracleAS Single Sign-On time is entered in minutes for an OracleAS Single Sign-On server that is running in Mountain Standard Time (MST):

```
[ENTERPRISE TIMEZONE ADJUSTMENT]
OracleSSONode=-360
```

Non-Web Client Sign-On in the Oracle Single Sign-On Configuration

JD Edwards EnterpriseOne non-web clients, such as Windows, JAVA Connector, and COM Connector, cannot use OracleAS Single Sign-On. However, this diagram shows how JD Edwards EnterpriseOne can use Oracle Internet Directory, which is an LDAP compliant directory service, to authorize non-web client users:



JD Edwards EnterpriseOne non-web client sign-on in the Oracle single sign-on configuration

OracleAS Single Sign-On uses the Oracle Internet Directory (OID) to manage user information. If enabled for LDAP, JD Edwards EnterpriseOne security server can validate the user ID and password of the non-web client user from Oracle Internet Directory.

See Also

Chapter 11, “Enabling LDAP Support in JD Edwards EnterpriseOne,” page 125

CHAPTER 15

Setting Up JD Edwards EnterpriseOne Single Sign-On Through Oracle Access Manager

This chapter provides an overview of JD Edwards EnterpriseOne single sign-on through Oracle Access Manager and discusses how to:

- Set up Oracle Access Manager single sign-on for JD Edwards EnterpriseOne.
- Set up JD Edwards EnterpriseOne for single sign-on integration with Oracle Access Manager.
- Set up single sign-off.

Note. You can also set up single sign-on between JD Edwards EnterpriseOne and Oracle applications through the Oracle AS Single Sign-On Server, which is not discussed in this chapter.

In addition, you can enable support of long user IDs and passwords in a JD Edwards EnterpriseOne single sign-on configuration with Oracle Access Manager or Oracle AS Single Sign-On Server. See "Using Long User IDs and Passwords in JD Edwards EnterpriseOne" in the Red Paper Library on Customer Connection for more information.

See Also

Chapter 14, "Understanding Single Sign-On Between JD Edwards EnterpriseOne and Oracle," page 181

Understanding JD Edwards EnterpriseOne Single Sign-On Through Oracle Access Manager

Oracle Access Manager provides single sign-on functionality for Oracle applications, including JD Edwards EnterpriseOne. It provides a secure internet infrastructure for identity management for JD Edwards EnterpriseOne applications and processes. This infrastructure provides:

- Identity and access management across JD Edwards EnterpriseOne applications, enterprise resources, and other domains.
- Foundation for managing the identities of customers, partners, and employees across internet applications. These user identities are protected by security policies for web interaction.

Integration with Oracle Access Manager provides JD Edwards EnterpriseOne implementations with these features:

- Oracle Access Manager authentication, authorization, and auditing services for JD Edwards EnterpriseOne applications.
- Oracle Access Manager single sign-on for JD Edwards EnterpriseOne applications and other Oracle Access Manager-protected resources in a single domain or across domains.

Note. JD Edwards EnterpriseOne single sign-on through Oracle Access Manager is supported only by the JD Edwards EnterpriseOne Web client, not Collaborative Portal.

- Oracle Access Manager authentication schemes that provide single sign-on for JD Edwards EnterpriseOne applications:
  - Basic Over LDAP (Lightweight Directory Access Protocol): Users enter a user name and password in a window supplied by the Web server.

    This method can be redirected to Secure Socket Layer (SSL).
  - Form: Similar to the basic challenge method, users enter information in a custom HTML form.

    You choose the information that users must provide in the form.
  - X509 Certificates: X.509 digital certificates over SSL.

    A user's browser must supply a certificate.
  - Integrated Windows Authentication (IWA): Users will not notice a difference between an Oracle Access Manager authentication and IWA when they log on to the desktop, open an Internet Explorer (IE) browser, request an Oracle Access Manager-protected web resource, and complete single sign-on.
  - Microsoft .NET Passport: NET Passport is a component of the Microsoft .NET framework. The .NET plug-in is a Web-based authentication service that provides single sign-on for Microsoft-protected web resources.
  - Custom: You can use other forms of authentication through the Oracle Access Manager Authentication Plug-in API.
- Session timeout: Oracle Access Manager enables you to set the length of time that a user session is valid.
- Ability to use the Oracle Access ManagerIdentity System for identity management. The Identity System provides identity management features such as portal inserts, delegated administration, workflows, and self-registration to JD Edwards EnterpriseOne applications.

  You can determine how much access to provide to users upon self-registration. Identity System workflows enable a self-registration request to be routed to appropriate personnel before access is granted. Oracle Access Manager also provides self-service, enabling users to update their own identity profiles.

See Also

Oracle Access Manager Integration Guide and the Oracle Identity Manager documentation.

JD Edwards EnterpriseOne Integration Architecture

JD Edwards EnterpriseOne has a configurable authentication mechanism that allows it to authenticate a user against:

- Native tables (through a security kernel).
- Lightweight Data Access Protocol (LDAP).
- Custom plug-ins, including the ability to read HTTP Headers.

JD Edwards EnterpriseOne single sign-on through Oracle Access Manager involves:

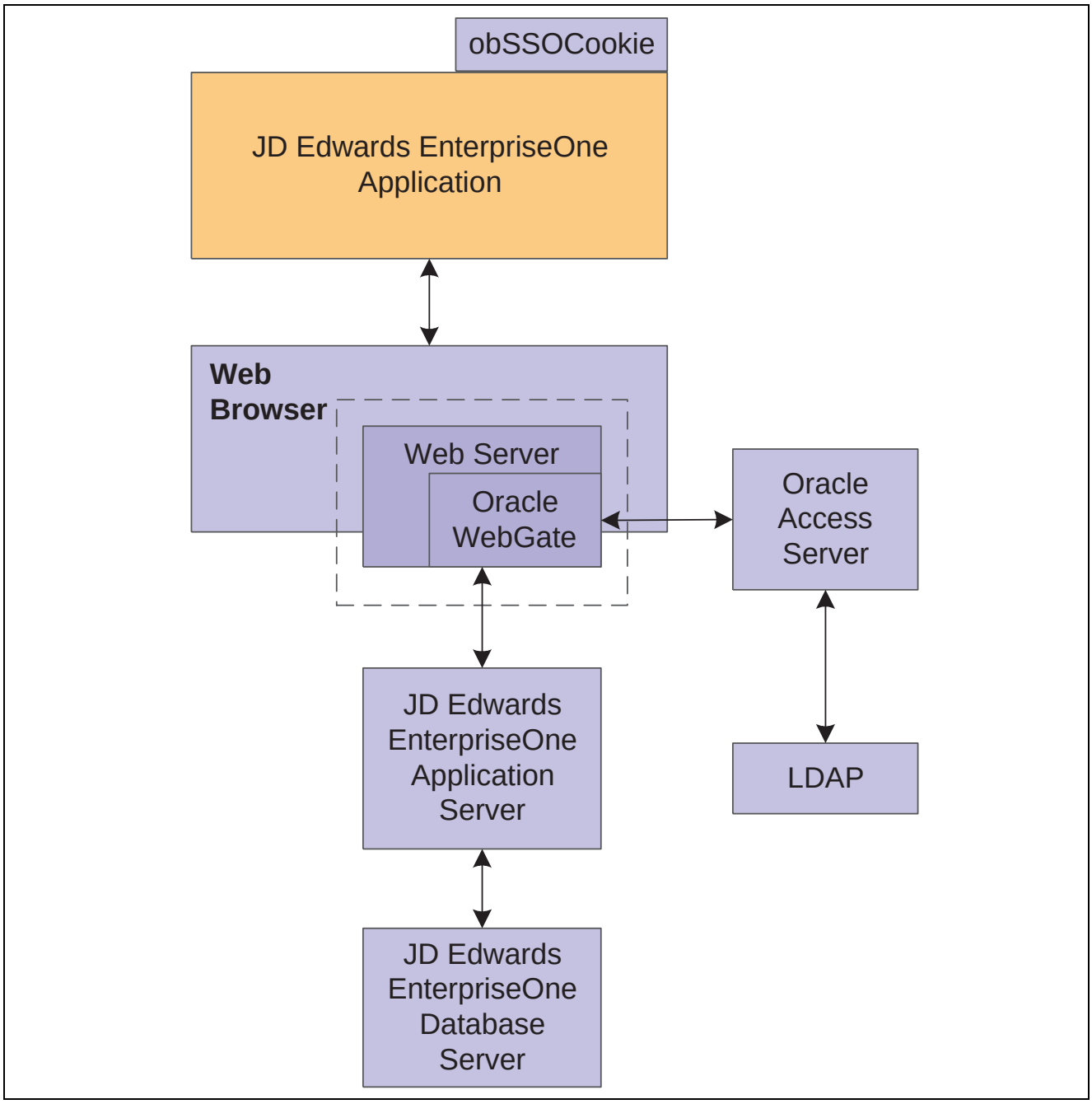
- Protection through a WebGate, which is a plug-in that intercepts Web resource (HTTP) requests and forwards them to the Access Server for authentication and authorization.

- Populating a header variable with an attribute value that is stored in the LDAP directory used by Oracle Access Manager.
- Configuring JD Edwards EnterpriseOne to invoke the Oracle Access Manager authentication process, overriding the default authentication mechanism.

Single Sign-On Architecture

Single sign-on with Oracle Access Manager requires a JD Edwards EnterpriseOne HTML Web Server configuration with an application server, such as Oracle Application Server 10g, that contains an HTTP server and a J2EE container, which is required for the Java servlets and Java code to run. In addition, WebGate must be installed on the HTTP Server, and it must be configured to protect the JD Edwards EnterpriseOne URLs that are used to access the HTML Web Server.

The user accesses a JD Edwards EnterpriseOne application using a web browser. WebGate intercepts the user's HTTP request and checks for an obSSOCookie. The obSSOCookie is an encrypted cookie that the Oracle Access Manager Access System uses to implement single-domain and multi-domain single sign-on. If the cookie does not exist or has expired, the user is prompted to enter credentials. Oracle Access Manager verifies the user credentials, and if the user is authenticated, the WebGate redirects the user to the requested resource and passes the required header variable to JD Edwards EnterpriseOne. The header variable is read by JD Edwards EnterpriseOne and is used to generate the PS_TOKEN. The following illustration shows the integration environment and process flow:



JD Edwards EnterpriseOne Single Sign-On through Oracle Access Manager

The following steps describe the single sign-on process:

1. A user attempts to access a JD Edwards EnterpriseOne program.
2. A WebGate that is deployed on the JD Edwards EnterpriseOne HTTP Server intercepts the request.
3. The WebGate checks the Access Server to determine whether the resource (JD Edwards EnterpriseOne URL) is protected.

   The security policy consists of an authentication scheme, authorization rules, and allowed operations based on an authentication and authorization success or failure.
4. If a valid session does not exist and the resource is protected, WebGate prompts the user for credentials.

5. If the credentials are validated, Oracle Access Manager performs the actions that are defined in the security policy for the JD Edwards EnterpriseOne resource and sets an HTTP header variable that maps to the JD Edwards EnterpriseOne user ID.
6. If a valid session cookie exists and the user is authorized to access the resource, WebGate redirects the user to the requested JD Edwards EnterpriseOne resource.
7. JD Edwards EnterpriseOne receives the request for the JD Edwards EnterpriseOne resource and runs the code that is defined in its authentication configuration.
8. The code reads the HTTP header variable and sets that value as the signed-on JD Edwards EnterpriseOne user. It then generates the PS_TOKEN, which contains the same information.
9. JD Edwards EnterpriseOne generates the applications, subject to further authorization verification within JD Edwards EnterpriseOne.

Supported Versions and Platforms

This chapter describes the integration of Oracle Access Manager 10g (10.1.4.0.1) with Tools 8.97 and JD Edwards EnterpriseOne applications. However, any references to specific versions and platforms in this chapter are for demonstration purposes.

To see the supported versions and platforms for this integration, refer to Metalink, by performing the following steps:

1. Go to the following URL:
2. Select the Certify tab.
3. Click View Certifications by Product.
4. Select the Application Server option, and click Submit.
5. Select Oracle Application Server, and click Submit.

Setting Up Oracle Access Manager Single Sign-On for JD Edwards EnterpriseOne

This section lists prerequisites and discusses how to set up Oracle Access Manager single sign-on for JD Edwards EnterpriseOne, which includes these tasks:

- Create a host identifier for the JD Edwards EnterpriseOne HTTP Server.
- Create a policy domain and policies to restrict access to JD Edwards EnterpriseOne URLs.
- Define a resource that controls the highest-level URL prefix to protect.
- Define two authorization rules.
- Define an authorization action.
- Define an authentication rule.
- Define an access policy and add the JD Edwards EnterpriseOne URL pattern to it.
- Define an authentication rule for the JD Edwards EnterpriseOne resources.
- Define an authentication action that sets a custom HTTP header variable upon successful authentication.

- Define an authentication expression for the JD Edwards EnterpriseOne resources.

Note. JD Edwards EnterpriseOne single sign-on through Oracle Access Manager is supported only with the JD Edwards EnterpriseOne Web client, not Collaborative Portal.

Prerequisites

Before you set up Oracle Access Manager and JD Edwards EnterpriseOne for single sign-on, you must:

- Install a supported directory server according to vendor instructions.
- Install and configure Oracle Access Manager using the directory server as the LDAP repository.

  See *Oracle Access Manager Installation Guide.*
- Configure the HTML Web Server so that JD Edwards EnterpriseOne applications are rendered and accessed through the HTTP Server.
- Install a WebGate on the JD Edwards EnterpriseOne HTTP Server.

  See *Oracle Access Manager Installation Guide*
- Configure the Web browser to allow cookies, according to vendor instructions.

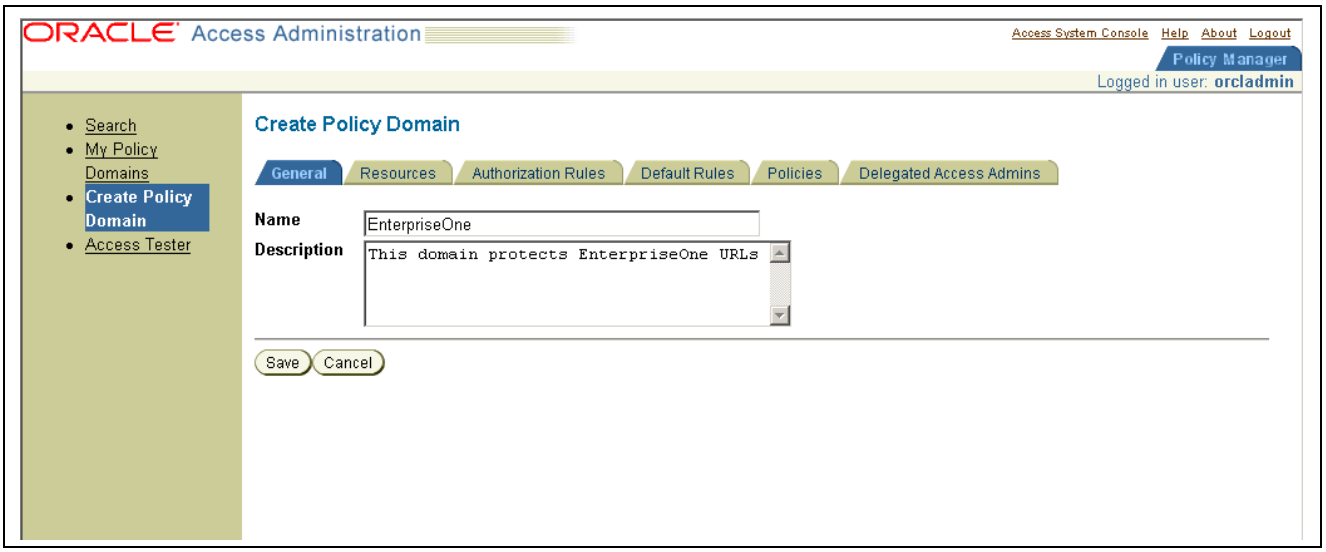
Creating a Host Identifier for the JD Edwards EnterpriseOne HTTP Server

Sign in to Oracle Access Manager.

1. From the Access System Landing page, select the Access System Console.
2. Click Access System Configuration, and then click Host Identifiers.
3. Add information about the server.

Creating a Policy Domain and Policies to Restrict Access to JD Edwards EnterpriseOne URLs

In Oracle Access Manager, access the System Landing page.



Create Policy Domain page: General tab

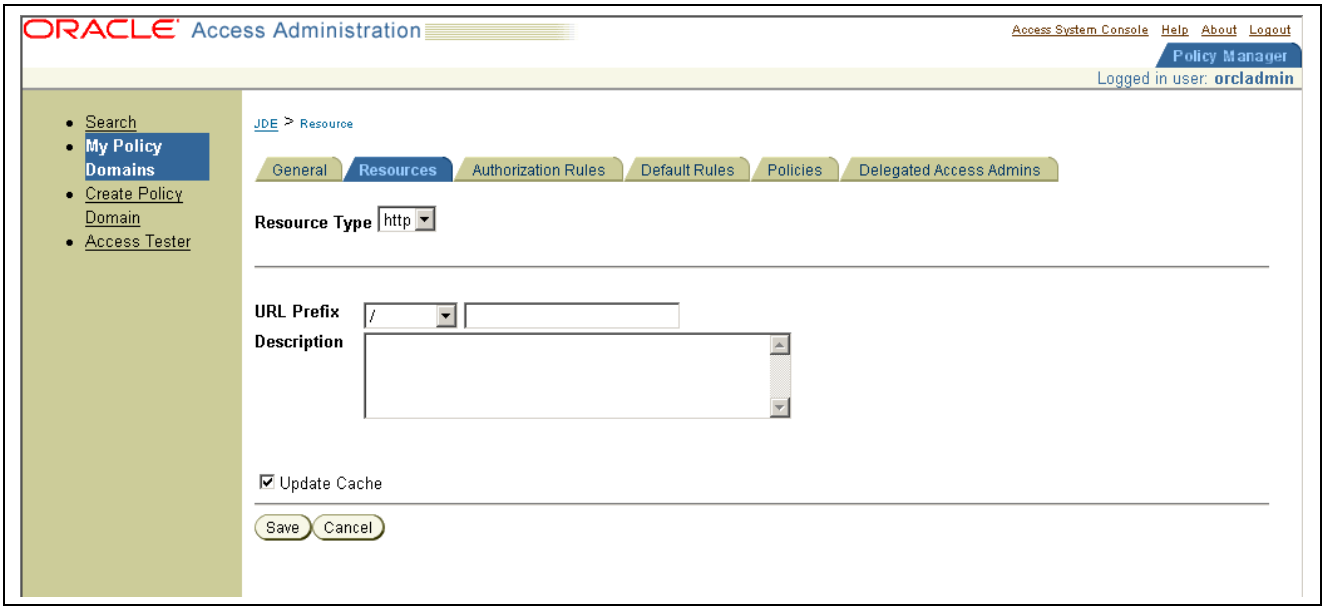
1. From the Access System Landing page, select the Policy Manager, and then click create Policy Domain.
2. Define a policy domain and policies.

   The policy domain should protect all JD Edwards EnterpriseOne URLs that users access. For example, if you use JD Edwards EnterpriseOne Portal to consolidate access to various JD Edwards EnterpriseOne applications, the policy must protect the portal and application URLs.

   URL prefix formats are specific to your JD Edwards EnterpriseOne implementation. For example, the version 8.97 URLs have the format /jde/E1Menu.maf.

Defining a Resource That Controls the Highest-Level URL Prefix to Protect

If you are already viewing the new policy domain, click Resources. Otherwise, click My Policy Domains, the link for the policy domain, and then Resources.

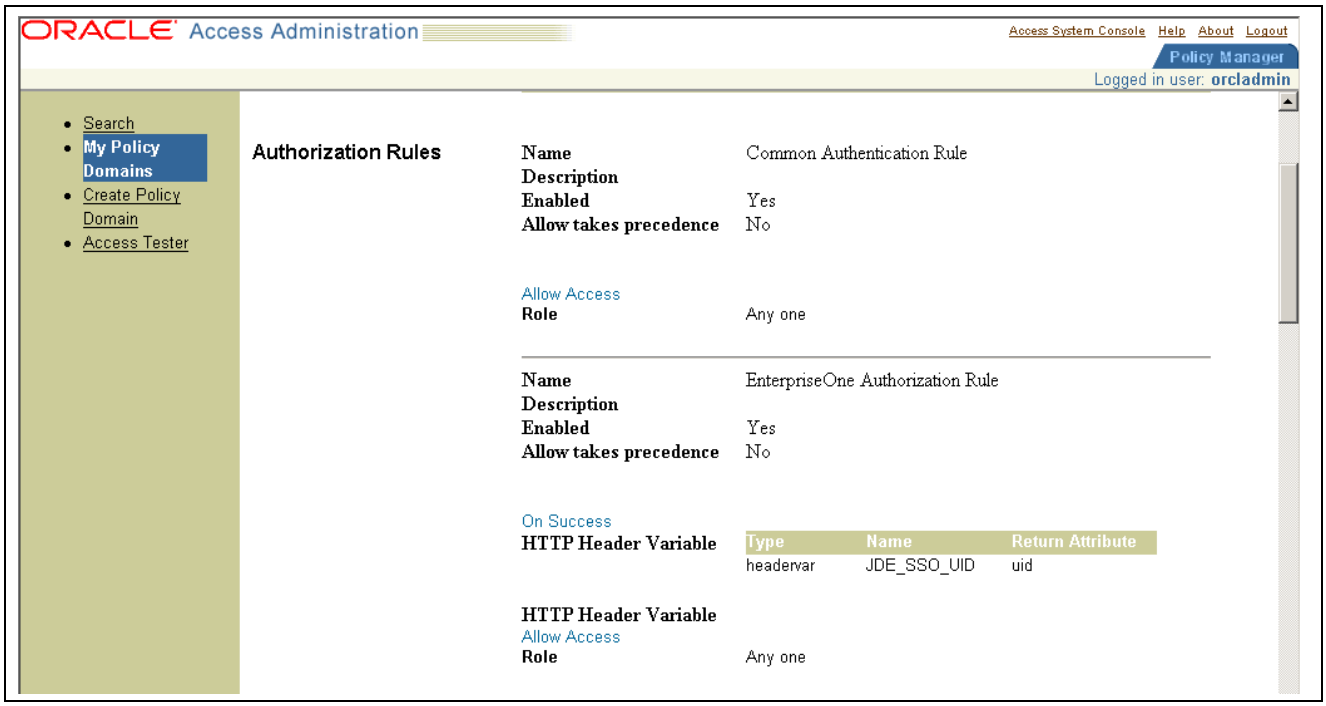


Resources page

Defining Two Authorization Rules

You must define two authorization rules that determine which users have access to all resources, including JD Edwards EnterpriseOne resources.

If you are already viewing the new policy domain, click Authorization Rules. Otherwise, click My Policy Domains, the link for the policy domain, and then Authorization rules.

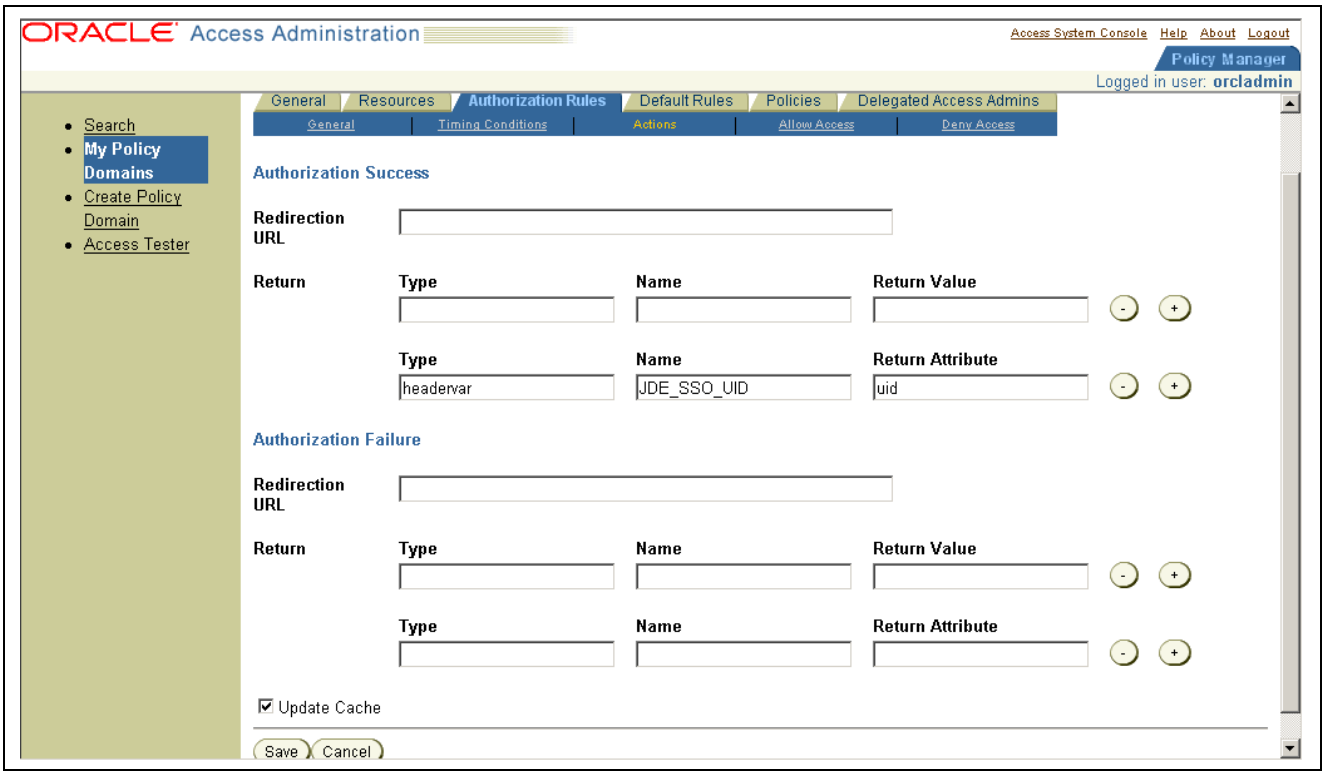


Authorization Rules page

Defining an Authorization Action

You must define an authorization action that sets a custom HTTP header variable upon successful authorization.

If you are already viewing the new policy domain, click Authorization Rules, Actions. Otherwise, click My Policy Domains, the link for the policy domain, Authorization Rules, and then Actions.

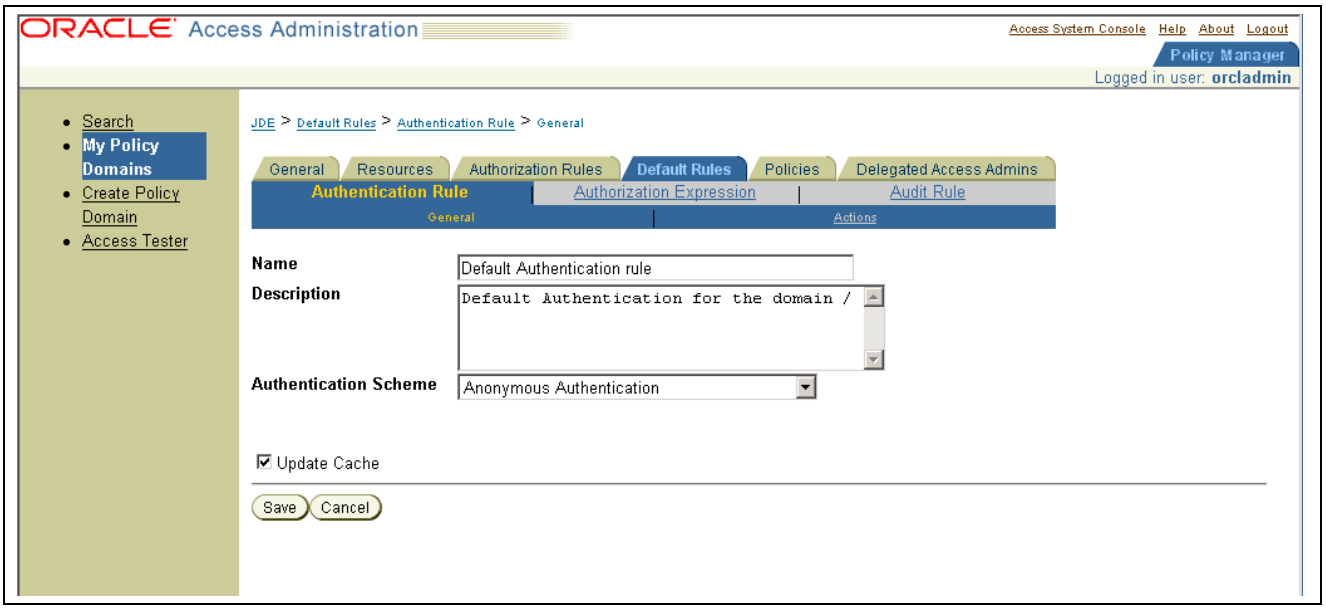


Authorization Rules page

The header variable should contain a value that maps to the JD Edwards EnterpriseOne user ID.

Defining an Authentication Rule

If you are already viewing the new policy domain, click Default Rules, Authentication Rule. Otherwise, click My Policy Domains, the link for the policy domain, Default Rules, and then Authentication Rule.

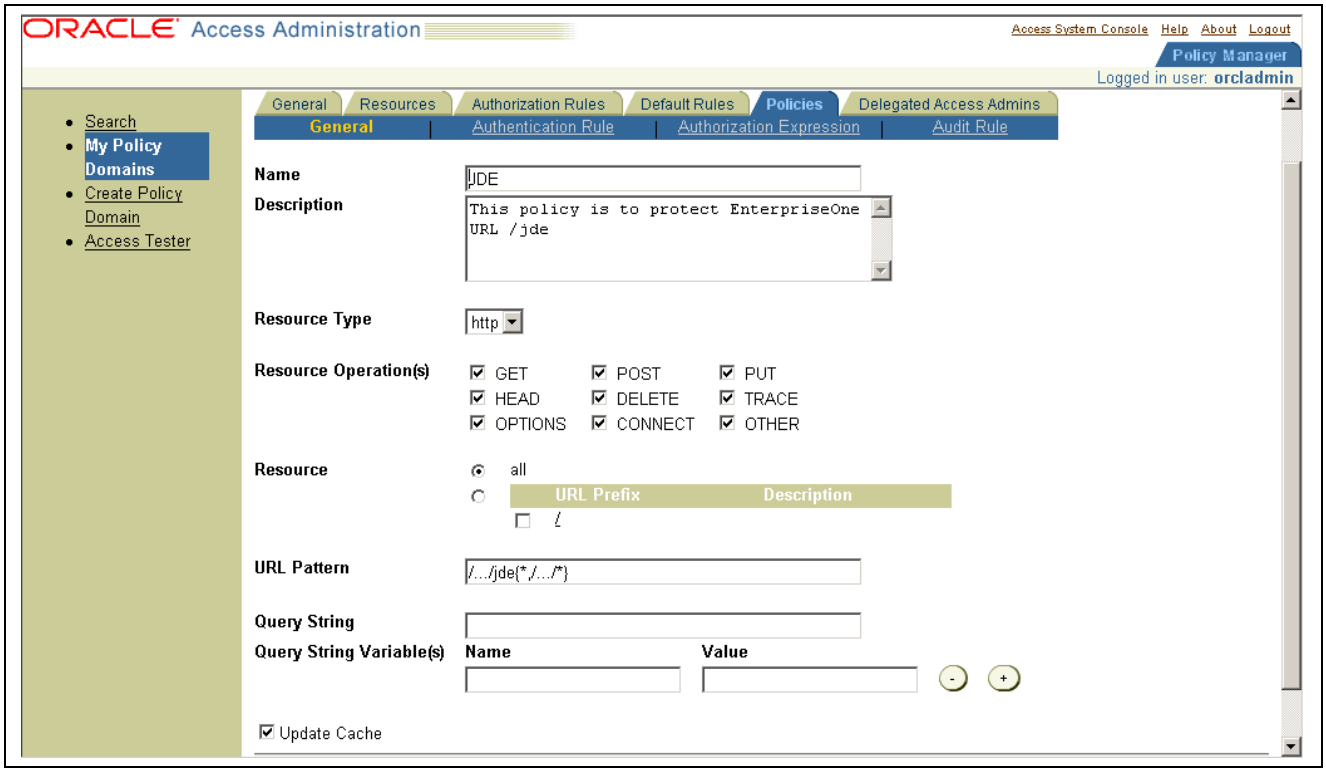


Authentication Rule Configuration page

Note. An authentication rule could be, for example, Oracle Access and Identity Basic Over LDAP, form authentication, and so on.

Defining an Access Policy and Adding the JD Edwards EnterpriseOne URL Pattern to It

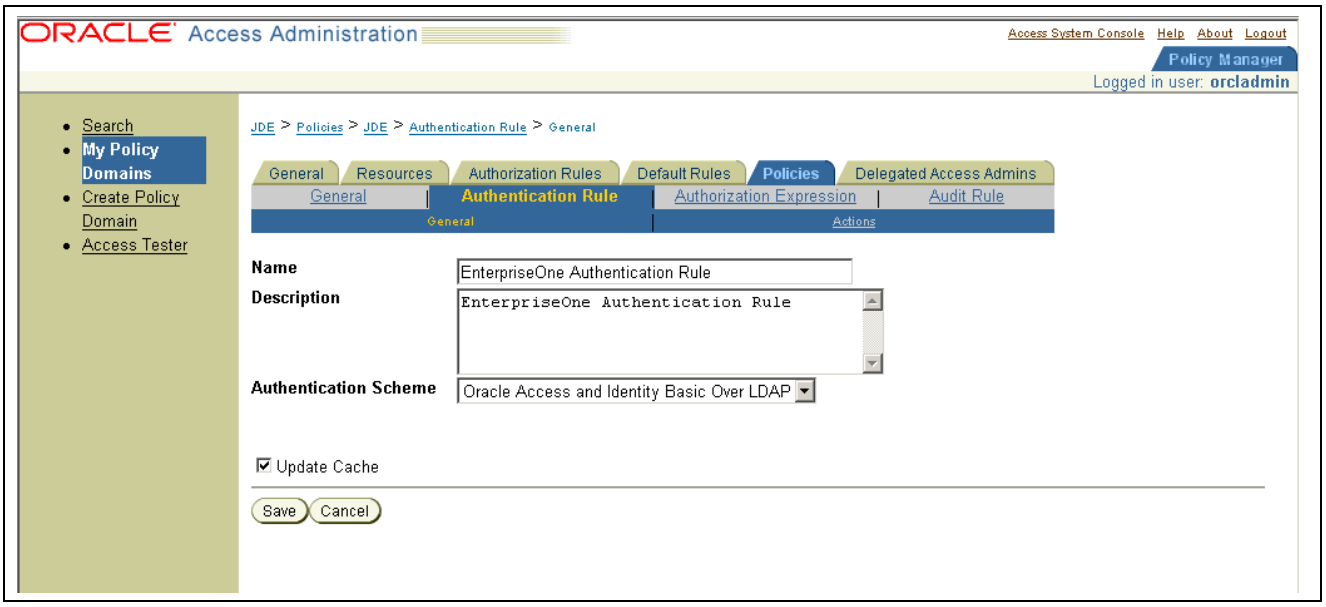
If you are already viewing the new policy domain, click Policies, Add. Otherwise, click My Policy Domains, the link for the policy domain, Policies, and then Add.



Policies page with an example of a saved policy

Defining an Authentication Rule for the JD Edwards EnterpriseOne Resources

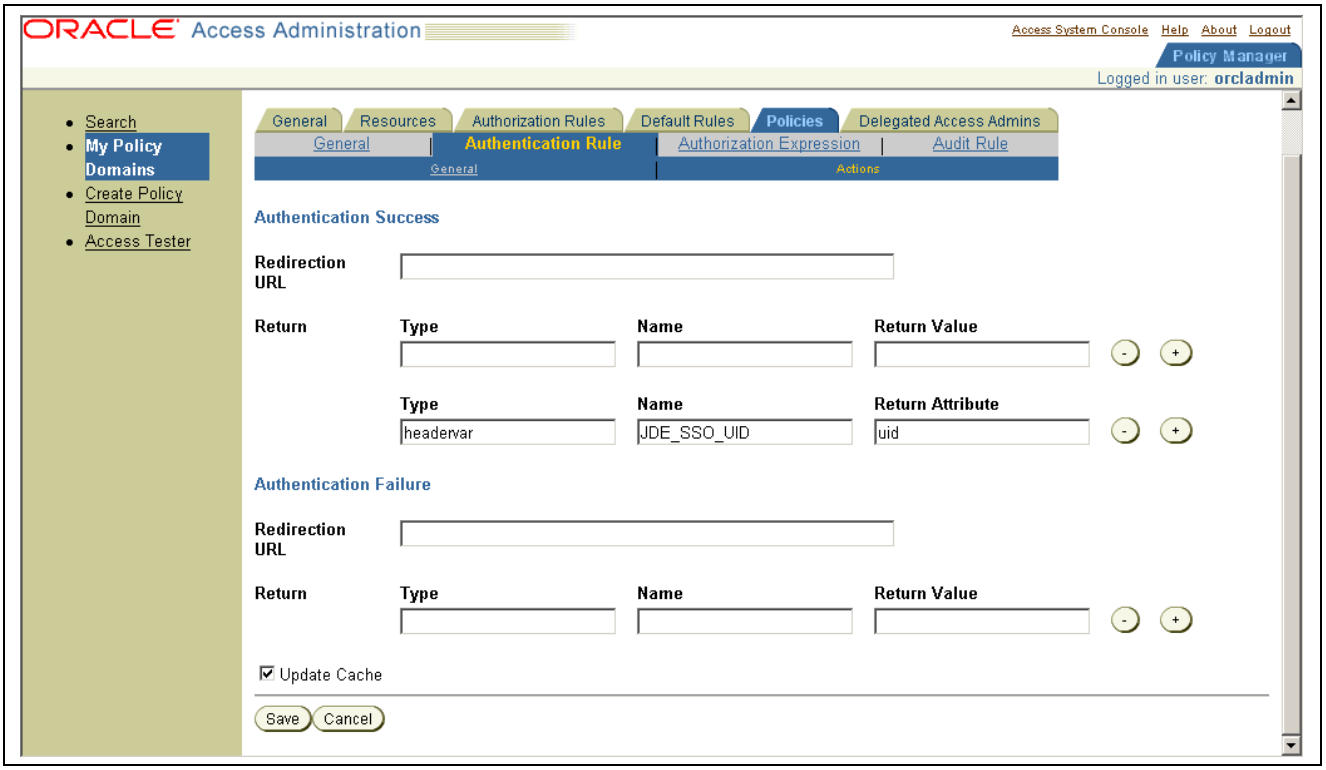
If you are already viewing the new policy domain, click Policies, JDE, and then Authentication Rule. Otherwise, click My Policy Domains, the link for the policy domain, Policies, JDE, and then Authentication Rule.



Authentication Rule page

Defining an Authentication Action That Sets a Custom HTTP Header Variable Upon Successful Authentication

If you are already viewing the new policy domain, click Policies, JDE, Authentication Rule, and then Actions. Otherwise, click My Policy Domains, the link for the policy domain, Policies, JDE, Authentication Rule, and then Actions.

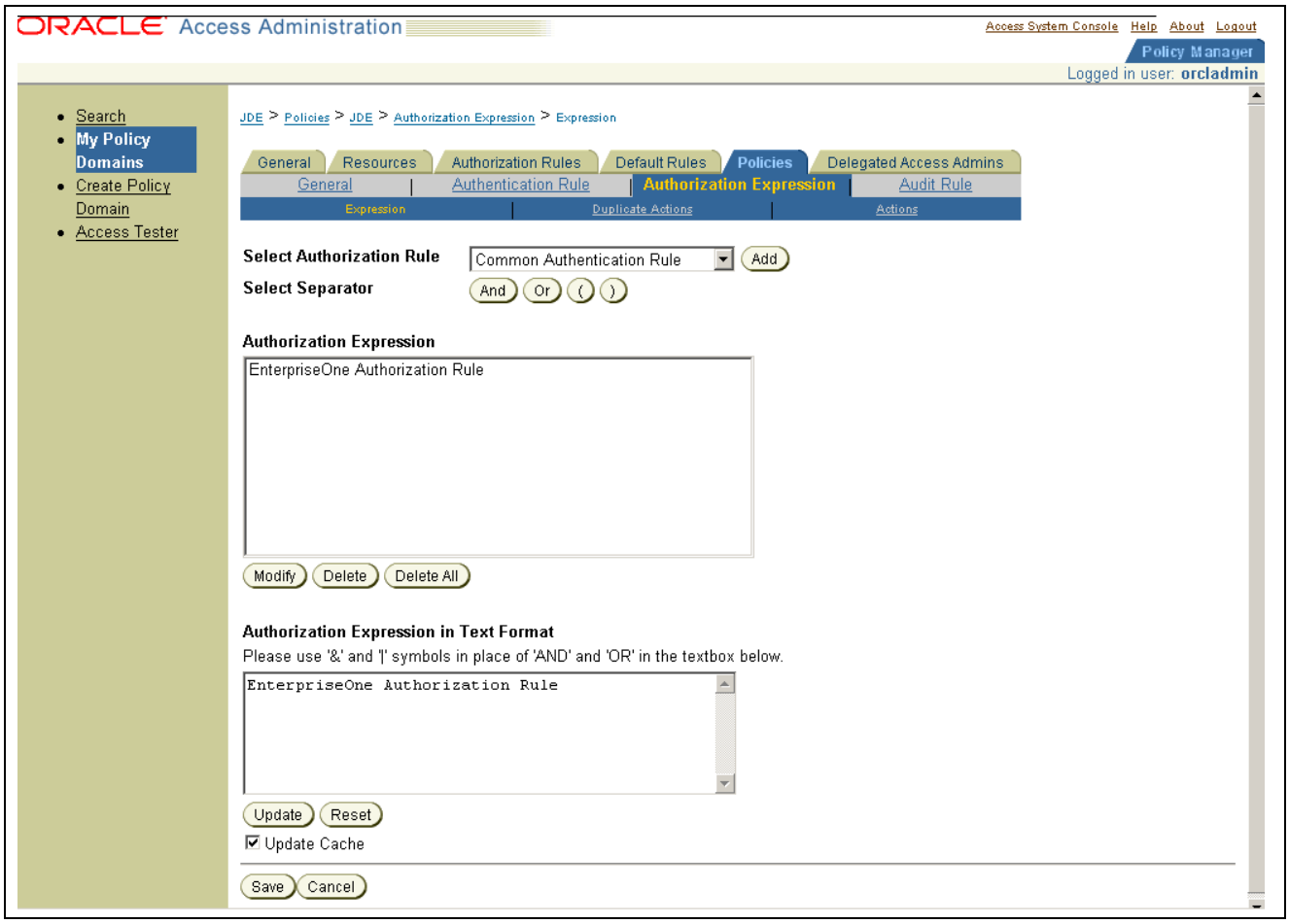


Authentication Rule page

The header variable should contain a value that maps to the JD Edwards EnterpriseOne user ID.

Defining an Authorization Expression for the JD Edwards EnterpriseOne Resources

If you are already viewing the new policy domain, click Policies, JDE, and then Authorization Expression. Otherwise, click My Policy Domains, the link for the policy domain, Policies, JDE, and then Authorization Expression.



Authorization Expression page

Setting Up JD Edwards EnterpriseOne for Single Sign-On Integration with Oracle Access Manager

This section discusses how to set up JD Edwards EnterpriseOne for single sign-on integration with Oracle Access Manager.

1. Access the JD Edwards EnterpriseOne Web client jas.ini file located on the HTML Web Server machine.
2. In the Security section, complete these settings:

Setting	Value
OracleAccessSSO=	TRUE
OracleAccessSSOSignOffURL=	http://*fullyqualifiedhostname*:*port*/access/oblix/lang/en-us/EnterpriseOnelogout.html

3. Make sure that the HMTL Web Server machine is set up as a trusted node.

   In addition, when setting up the trusted node, you might have to change the key for the encryption and decryption of the authenticate token. The settings for this key are set during the installation of the JD Edwards EnterpriseOne HTML Web Server and are stored in the TokenGen.ini file on the security server.

Configuring Single Sign-Off

This section discusses how to configure single sign-off for JD Edwards EnterpriseOne.

Note. If you use the Basic Over LDAP authentication scheme on some versions of Microsoft Internet Explorer, you may get unexpected results with the single sign-off URL. Internet Explorer caches user credentials when a Basic Over LDAP authentication scheme is used. For some versions of Internet Explorer, this means that users can continue to access resources after logging out. If you experience this problem with the single sign-off URL, Oracle recommends that you use a Form over LDAP authentication scheme.

1. Create a new HTML page called EnterpriseOneLogout.html.
2. Open the EnterpriseOneLogout.html file in an editor and add the following information to it:

   Note. You can customize the sign-off page if desired.

```
<!doctype html public "-//w3c//dtd html 4.0 transitional//en">
<html lang="en-US">
 <head>
  <title>Oracle Access Manager</title><link rel="stylesheet" type="text/css" href=⇒
"style2/coreid.css"></link>
  <meta http-equiv="PRAGMA" name="PRAGMA" content="NO-CACHE">
  <meta http-equiv="Expires" name="Expires" content="Mon, 06 Jan 1990 00:00:01⇒
 GMT">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  <meta name="Description" content="Oracle Access Manager">
  <meta name="Robot" content="none">
  <meta name="Copyright" content="Copyright © 1996-2006, Oracle. All Rights⇒
 Reserved.">
  <style type="text/css"> <!--.unnamed1 { font-family: Arial, Helvetica, sans-⇒
serif; font-size: 2pt}
 --></style>
  <script language="JavaScript">
  function delCookie(name,path,domain) {
   var today = new Date();
   var deleteDate = new Date(today.getTime() - 48 * 60 * 60 * 1000); // minus 2⇒
```

```
 days
   var cookie = name + "="
    + ((path == null) ? "" : "; path=" + path)
    + ((domain == null) ? "" : "; domain=" + domain)
    + "; expires=" + deleteDate;
   document.cookie = cookie;
  }

  function delOblixCookie() {
   // set focus to ok button
   var isNetscape = (document.layers);
   if (isNetscape == false || navigator.appVersion.charAt(0) >= 5) {
    for (var i=0; i<document.links.length; i++) {
     if (document.links[i].href == "javascript:top.close()") {
      document.links[i].focus();
      break;
     }
    }
   }
   delCookie('ObTEMC', '/');
   delCookie('ObSSOCookie', '/');
   delCookie('ObSSOCookie', '/');
   delCookie('OBBasicAuth', '/');
   delCookie('JSESSIONID', '/jde');
   // in case cookieDomain is configured
   // delete same cookie to all of subdomain
   var subdomain;
   var domain = new String(document.domain);
   var index = domain.indexOf(".");
   while (index > 0) {
    subdomain = domain.substring(index, domain.length);
    if (subdomain.indexOf(".", 1) > 0) {
     delCookie('ObTEMC', '/', subdomain);
     delCookie('ObSSOCookie', '/', subdomain);
     delCookie('OBBasicAuth', '/', subdomain);
     delCookie('JSESSIONID', '/jde', subdomain);
    }
    domain = subdomain;
    index = domain.indexOf(".", 1);
   }
  }
  </script>
 </head>
<link rel="stylesheet" type="text/css" href="/css/webguistylesheet.jsp">

 <body bgcolor="#ffffff" marginwidth="0" marginheight="0" topmargin="0" leftmargin=⇒
⇒
⇒
⇒
"0"
```



```
 onload="delOblixCookie();">
 <table width="100%" height="100%" cellpadding="0" cellspacing="0">
  <tr>
   <td height="148" valign="middle">
    <p align="center">
     <img src="./images/Oracle_JDEE1.gif" alt="Oracle JD Edwards EnterpriseOne⇒
Logo">
    </p>
   </td>
  </tr>
  <tr>
   <td height="250" align="center" valign="middle">
    <h3><font size="5">Oracle Access Manager Applications</font></h3>
    <h3>You have been logged out.</h3>
    <h3>For security reasons, please close the browser window </h3>
    <h3>by clicking the OK button.</h3>
    <a href="javascript:top.close()" onmouseover="self.status='Close the browser⇒
window.'; return true">
     <img border="0" alt="Close the browser window." src="style2/NAVok.gif"></a>
    <script language="JavaScript1.2">
       var jdeLegalInfo = "The Programs (which include both the software and⇒
documentation) contain proprietary information; they are provided under a license⇒
agreement containing restrictions on use and disclosure and are also protected by⇒
copyright, patent, and other intellectual and industrial property laws. Reverse⇒
engineering, disassembly, or decompilation of the Programs, except to the extent⇒
required to obtain interoperability with other independently created software or⇒
as specified by law, is prohibited.\nThe information contained in this document⇒
is subject to change without notice. If you find any problems in the⇒
documentation, please report them to us in writing. This document is not⇒
warranted to be error-free. Except as may be expressly permitted in your license⇒
agreement for these Programs, no part of these Programs may be reproduced or⇒
transmitted in any form or by any means, electronic or mechanical, for any⇒
purpose.\nSubject to patent protection under one or more of the following U.S.⇒
patents:  5,781,908; 5,828,376; 5,950,010; 5,960,204; 5,987,497; 5,995,972;⇒
5,987,497; and 6,223,345.  Other patents pending.\nContains GNU libgmp library;⇒
Copyright © 1991 Free Software Foundation, Inc. This library is free software⇒
which can be modified and redistributed under the terms of the GNU Library⇒
General Public License.\nIncludes Adobe® PDF Library, Copyright 1993-2001 Adobe⇒
Systems, Inc. and DL Interface, Copyright 1998-2001 Datalogics Inc.  All rights⇒
reserved.  Adobe® is a trademark of Adobe Systems Incorporated.\nPortions of this⇒
program contain information proprietary to Microsoft Corporation.  Copyright 1985-⇒
⇒
⇒
⇒
1999 Microsoft Corporation.\nPortions of this program contain information⇒
proprietary to Tenberry Software, Inc. Copyright 1992-1995 Tenberry Software,⇒
Inc.\nPortions of this program contain information proprietary to Premia⇒
Corporation. Copyright 1993 Premia Corporation.\nThis product includes code⇒
licensed from RSA Data Security.\nAll rights reserved.\nThis product includes⇒
software developed by the OpenSSL Project for use in the OpenSSL Toolkit http:⇒
```

```
//www.openssl.org/).\nThis product includes cryptographic software written by Eric⇒
 Young (eay@cryptsoft.com).\nThis product includes software written by Tim Hudson ⇒
(tjh@cryptsoft.com).All rights reserved.";
     </script>
    </td>
   </tr>
   <tr>
    <td valign="bottom">
     <table width="100%" border="0" cellspacing="0" cellpadding="5">
      <tr>
       <td width="325"><div class="fineprint">
         <script>
            jdeLegalInfo = "The Programs (which include both the software and⇒
 documentation) contain proprietary information; they are provided under a license⇒
 agreement containing restrictions on use and disclosure and are also protected by⇒
 copyright, patent, and other intellectual and industrial property laws. Reverse⇒
 engineering, disassembly, or decompilation of the Programs, except to the extent⇒
 required to obtain interoperability with other independently created software or⇒
 as specified by law, is prohibited.\nThe information contained in this document⇒
 is subject to change without notice. If you find any problems in the⇒
 documentation, please report them to us in writing. This document is not⇒
 warranted to be error-free. Except as may be expressly permitted in your license⇒
 agreement for these Programs, no part of these Programs may be reproduced or⇒
 transmitted in any form or by any means, electronic or mechanical, for any⇒
 purpose.\nSubject to patent protection under one or more of the following U.S.⇒
 patents:  5,781,908; 5,828,376; 5,950,010; 5,960,204; 5,987,497; 5,995,972;⇒
 5,987,497; and 6,223,345.  Other patents pending.\nContains GNU libgmp library;⇒
 Copyright © 1991 Free Software Foundation, Inc. This library is free software⇒
 which can be modified and redistributed under the terms of the GNU Library⇒
 General Public License.\nIncludes Adobe® PDF Library, Copyright 1993-2001 Adobe⇒
 Systems, Inc. and DL Interface, Copyright 1998-2001 Datalogics Inc.  All rights⇒
 reserved.  Adobe® is a trademark of Adobe Systems Incorporated.\nPortions of this⇒
 program contain information proprietary to Microsoft Corporation.  Copyright 1985-⇒
⇒
⇒
⇒
1999 Microsoft Corporation.\nPortions of this program contain information⇒
 proprietary to Tenberry Software, Inc. Copyright 1992-1995 Tenberry Software,⇒
 Inc.\nPortions of this program contain information proprietary to Premia⇒
 Corporation. Copyright 1993 Premia Corporation.\nThis product includes code⇒
 licensed from RSA Data Security.\nAll rights reserved.\nThis product includes⇒
 software developed by the OpenSSL Project for use in the OpenSSL Toolkit http:⇒
//www.openssl.org/).\nThis product includes cryptographic software written by Eric⇒
 Young (eay@cryptsoft.com).\nThis product includes software written by Tim Hudson ⇒
(tjh@cryptsoft.com).All rights reserved.";
         </script>
         <a href="#content"><img src="./images/1pix_shim.gif" border="0" alt="Skip⇒
 navigation links"></a><a class="fineprint" style="COLOR: black" href="javascript:⇒
alert(jdeLegalInfo);">Legal
          Terms</a><br>
```



```
         Copyright © 2003-2005, Oracle. All rights reserved. Oracle, JD Edwards,
         PeopleSoft, and Retek are registered trademarks of Oracle Corporation and⇒
/or
         its affiliates. Other names may be trademarks of their respective⇒
 owners.</div>
       </td>
       <td><a name="content"></a></td>
      </tr>
     </table>
    </td>
   </tr>
   <noscript>A script enabled browser is required for this page to function
    properly</noscript>
   </td>
  </table>
 </body>
</html>
```

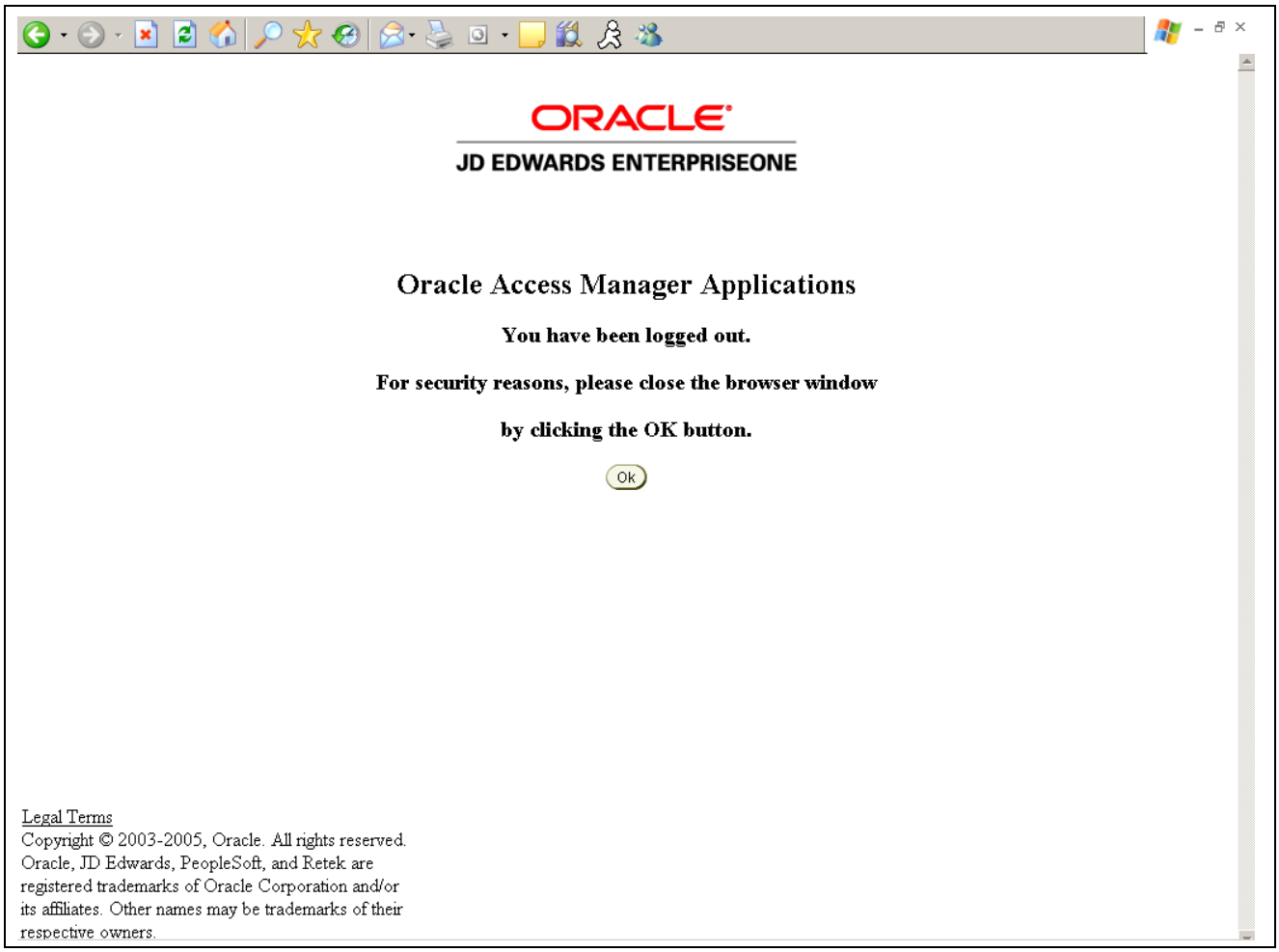
3. Place the EnterpriseOneLogout.html file in a path that is not protected by a WebGate.

   The default path is:

   Policy_Manager_install_dir/access/oblix/lang/en-us/EnterpriseOneLogout.html

   Where *Policy_Manager_install_dir* is the directory where the Policy Manager is installed.

   The file contains Javascript that deletes the ObTEMC, ObSSOCookie, ObBasicAuth, and JSESSIONID cookie. See the appendix on configuring logout in the *Oracle Access Manager Access Administration Guide* for details.



Signoff page

CHAPTER 16

Setting Up Single Sign-On Between JD Edwards EnterpriseOne and Crystal Enterprise

This chapter provides overviews of JD Edwards EnterpriseOne and Crystal Enterprise single sign-on and discusses how to set up each program to enable single sign-on.

Understanding Single Sign-On between JD Edwards EnterpriseOne and Crystal Enterprise

Single sign-on between JD Edwards EnterpriseOne and Crystal Enterprise provides a way for users to access Crystal Enterprise from JD Edwards EnterpriseOne. JD Edwards EnterpriseOne uses a predefined task type to launch Crystal Enterprise from the JD Edwards EnterpriseOne Menu. From the JD Edwards EnterpriseOne Menu, you can select the Crystal Enterprise task to open a new Crystal Enterprise session. This provides a convenient way for JD Edwards EnterpriseOne users to access Crystal Enterprise without having to maintain separate user IDs and passwords for Crystal Enterprise.

Note. A separate Crystal Enterprise license is used each time a user opens a new Crystal Enterprise session from JD Edwards EnterpriseOne. Therefore, you should remind users to sign off of Crystal Enterprise when finished to ensure that there are enough licenses available for users. Although, if a user forgets to sign off, the Crystal Enterprise web server will eventually time out and release the license.

Prerequisite

You must install Crystal Enterprise with JD Edwards EnterpriseOne HTML Web Server in one of two supported configurations before setting up JD Edwards EnterpriseOne and Crystal Enterprise for single sign-on.

See JD Edwards EnterpriseOne Tools Release 8.97 Business Objects XI R2 Guide

Configuring Single Sign-On Between JD Edwards EnterpriseOne and Crystal Enterprise

This section discusses how to:

- Verify the UDC for the Crystal Enterprise task type.
- Add the Crystal Enterprise task to the JD Edwards EnterpriseOne Menu.
- Set up the default domain in Crystal Management Console.

- Verify the Crystal Enterprise web server definition.

Verifying the UDC for the Crystal Enterprise Task Type

Access the Work with User Defined Codes form. In JD Edwards Solution Explorer, type *UDC* in the Fast Path.

1. Complete these fields and click Find:
   - Product Code

     Enter *H90*.
   - User Defined Code

     Enter *TT*.
   - Codes (in the QBE line)

     Enter *20*.

   The system should display 20, which is the UDC for Crystal Enterprise.
2. If no entries are found, click the Add button to create the UDC for Crystal Enterprise.
3. On User Defined Codes, tab to the blank row at the bottom of the list of UDCs and complete these fields:
   - Codes

     Enter *20*.
   - Description 1

     Enter *Crystal Enterprise*.
   - Hard Coded

     Enter *Y*.
4. Click OK.

Add the Crystal Enterprise Task to the JD Edwards EnterpriseOne Menu

In JD Edwards Solution Explorer, click the Menu Design button to access the Menu Design view.

1. Click the Views button and select the menu to which you want to add the task.
2. Expand the appropriate nodes to locate the position in the menu where you want to place the Crystal Enterprise task.
3. Right-click the parent menu node and select Insert New Task.
4. On Task Revisions, complete these fields:
   - Task ID
   - Task Name
   - Product Code (in the Common tab)
5. In the Executable tab, select the Crystal Enterprise option, and then click OK.

Setting Up the Default Domain in Crystal Management Console

In order for the Crystal Enterprise task to correctly launch from JD Edwards EnterpriseOne, you must make sure that the default domain for JD Edwards EnterpriseOne is set up correctly in Crystal Management Console (CMC).

Sign in to CMC.

1. In CMC, click the Authentication button.
2. In the EnterpriseOne tab, complete these fields:
   - EnterpriseOne System User
   - Domain

     Enter the default domain for EnterpriseOne.
   - EnterpriseOne Role
3. Click the Update button.

Verifying the Crystal Enterprise Web Server Definition

In JD Edwards Solution Explorer, enter *P9654A* in the Fast Path to access the Work with Locations and Machines form.

1. Click Find.
2. Expand each node until you see the Crystal Enterprise Web Server node.
3. Click this node and make sure that at least one Crystal Enterprise web server definition is listed.
4. If no entries are listed, select the Crystal Enterprise Web Server node, and then click the Add button to add a definition for the web server.
5. On Crystal Enterprise Web Server Revisions, complete these fields and then click OK:

Field	Description
Machine Name	Enter the name of the machine on the network (server or workstation).
Description	Enter a description for the machine.
Release	Enter the release number as defined in the Release Master.
Host Type	Enter the host machine type.
Primary User	Enter the primary user for the listed machine.
Port Number (Crystal tab)	Enter the port number for the JD Edwards EnterpriseOne instance.

APPENDIX A

Creating a JD Edwards EnterpriseOne LDAP Configuration for OID

This appendix is a supplement to the "Enabling LDAP Support in Oracle JD Edwards EnterpriseOne" chapter in this guide. Use the settings detailed in this appendix as a reference when creating an LDAP configuration for Oracle Internet Directory (OID).

This appendix provides an overview of the JD Edwards EnterpriseOne LDAP configuration for OID and describes how to:

- Add OID to the list of LDAP server types.
- Create an LDAP configuration for OID.
- Configure LDAP server settings for OID.
- Configure LDAP to JD Edwards EnterpriseOne enterprise server mappings for OID.

Understanding JD Edwards EnterpriseOne LDAP Configuration for OID

OID is an LDAP compliant directory service. You can configure JD Edwards EnterpriseOne to use OID as the LDAP server. This enables administrators to use the directory service to manage user information such as user IDs, passwords, and user-role relationships.

Important! This section does not contain all of the steps for creating an LDAP configuration, only specific values that are required for setting up an LDAP configuration for OID.

When you configure OID as the LDAP server, the settings that you configure depend on how you plan to use OID, which can include these scenarios:

- Managing only user IDs and passwords.
- Managing user-role relationships in addition to user IDs and passwords.
- Using Secure Socket Layer (SSL).
- Using the User Profile Self-Service application (P0092SS).

See Also

Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," page 125

Oracle Internet Directory Administrator's Guide

Adding OID to the List of LDAP Server Types

Before you can create an LDAP configuration for OID, you must manually add OID as an option in the LDAP Server Type field of the LDAP Server Configuration Workbench program (P95928). To do so, use the User Defined Code program (P0004A) to add a UDC for OID.

Access the Work With User Defined Codes form. In JD Edwards Solution Explorer, enter *UDC* in the Fast Path.

1. Complete these fields and click Find:

Field	Value
Product Code	*95*
User Defined Codes	*LS*

2. Click Add.
3. On the User Defined Codes form, scroll to the last empty row of the detail area.

Important! Be sure to add the new code on the *last* detail row so that you do not inadvertently overwrite a blank code, which might appear in the first detail row. A blank code might have only a period in the Description field.

4. Complete these fields and click OK:

Field	Value
Codes	*OID*
Description 1	*Oracle Internet Directory*

Creating an LDAP Configuration for OID

Use this section as a reference for creating an LDAP configuration.

See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Creating an LDAP Configuration, page 138.

When you create an LDAP configuration for OID, on the LDAP Server Information form, you must select OID in the LDAP Server Type field.

Configuring the LDAP Server Settings for OID

Use the OID settings in this section as a reference for configuring the LDAP server settings.

See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Configuring the LDAP Server Settings, page 139.

The values in the tables are variables and will differ depending upon your configuration.

Configure these attributes:

Attribute	Value
USRSRCHBAS	*cn=Users,dc=jdedwards,dc=com*
USRSRCHFLT	*objectclass=inetOrgPerson*
USRSRCHSCP	*subtree*

If roles are enabled in LDAP, configure these attributes:

Attribute	Value
ROLSRCHBAS	*cn=Groups,dc=jdedwards,dc=com*
ROLSRCHFLT	*objectclass=groupofUniqueNames*
ROLSRCHSCP	*subtree*

If you are using SSL with LDAP server, configure these attributes as well:

Attribute	Value
SSLPORT	*636*
CERTDBPATH	*c:\certdbdir (Directory path for cert7.db)*

If you are using the user profile self-service application for the Manufacturing Sourcing module , configure these settings:

Attribute	Value
USRADDLOC	cn=Users, dc=jdedwards,dc=com
USRCLSHRCY	*top,person,organizationalperson,inetOrgPerson,orcluser,orcluserv2*
ROLADDLOC	*cn=Groups,dc=jdedwards,dc=com*

Configuring LDAP to JD Edwards EnterpriseOne Enterprise Server Mappings for OID

Use the OID settings in this section as a reference for configuring LDAP to JD Edwards EnterpriseOne enterprise server mappings.

See Chapter 11, "Enabling LDAP Support in JD Edwards EnterpriseOne," Configuring LDAP to JD Edwards EnterpriseOne Enterprise Server Mappings, page 142.

The values in the tables are variables and will differ depending upon your configuration.

Configure these attributes:

Attribute	Value
E1USRIDATR	*uid*
USRSRCHATR	*uid*
EUSRIDATR	*uid*

If roles are enabled in LDAP, configure these attributes:

Attribute	Value
ROLNAMEATR	*cn*
ROLSRCHATR	*uniquemember*

If you are using the user profile self-service application for the Manufacturing Sourcing module, configure these settings:

Attribute	Value
CMNNAME	*cn*
SURNAME	*sn*
PASSWORD	*userPassword*
OBJCLASS	*objectClass*

APPENDIX B

JD Edwards EnterpriseOne Cookies

This appendix discusses the web runtime cookies.

Web Runtime Cookies

This table lists the web runtime cookies that the HTML Web Server sends to a web browser when running JD Edwards EnterpriseOne web applications.

JD Edwards EnterpriseOne Web Runtime Cookie	Purpose	Life Span	Turn ON/OFF
com_jdedwards_ LastLayout	This cookie stores the OneWorld Portal Workspace (WORKSPACEID) that was last accessed by a user (USERID). **Note.** This cookie is only applicable to OneWorld Portal users.	The life span of the cookie is one year.	You cannot turn off this cookie.
com_jdedwards_CSN	This cookie stores the information to implement critical state functionality for the HTML Client Component running inside the OneWorld Portal.	10000 milliseconds.	You cannot turn off this cookie.
advancedState	This cookie stores the information about whether to display the Environment and Role fields on the JD Edwards EnterpriseOne sign-in screen.	Seven days.	This cookie is created only if the DisplayEnvironment property defined in the [LOGIN] section of the JAS.INI is not set to "HIDDEN".
jdeLoginCookie	This cookie stores the username, password, role, language code and rtlLayout information about a user's login in an encrypted format.	The life span of the cookie depends on the value of CookieLifeTime property defined in the [SECURITY] section of the JAS.INI file. If this property is not defined, then by default, this cookie's life span is set to seven days.	This cookie is not created if the UseLogonCookie property defined in the [SECURITY] section of the JAS.INI is set to false. The system does not create this cookie by default.

JD Edwards EnterpriseOne Web Runtime Cookie	Purpose	Life Span	Turn ON/OFF
AutoPopulate	This cookie stores a user's preference of whether to auto populate the grid on a form. A user can turn the autopopulate grid option on/off by using the AutoPopulate option in the Tools menu on a form.	The life span of the cookie one year.	You cannot turn off this cookie.
maxLogLength	This cookie determines the maximum number of javascript debug statements that can be logged using JSMonitor.log() API. The default value for this cookie is 15. A developer can turn on the logging by clicking the Enable JSMonitor button after pressing CTRL+D.	This cookie never expires.	You cannot turn off this cookie.

Glossary of JD Edwards EnterpriseOne Terms

Accessor Methods/Assessors Java methods to "get" and "set" the elements of a value object or other source file.

activity rule The criteria by which an object progresses from one given point to the next in a flow.

add mode A condition of a form that enables users to input data.

Advanced Planning Agent (APAg) A JD Edwards EnterpriseOne tool that can be used to extract, transform, and load enterprise data. APAg supports access to data sources in the form of rational databases, flat file format, and other data or message encoding, such as XML.

alternate currency A currency that is different from the domestic currency (when dealing with a domestic-only transaction) or the domestic and foreign currency of a transaction.

In JD Edwards EnterpriseOne Financial Management, alternate currency processing enables you to enter receipts and payments in a currency other than the one in which they were issued.

Application Server Software that provides the business logic for an application program in a distributed environment. The servers can be Oracle Application Server (OAS) or WebSphere Application Server (WAS).

as if processing A process that enables you to view currency amounts as if they were entered in a currency different from the domestic and foreign currency of the transaction.

as of processing A process that is run as of a specific point in time to summarize transactions up to that date. For example, you can run various JD Edwards EnterpriseOne reports as of a specific date to determine balances and amounts of accounts, units, and so on as of that date.

Auto Commit Transaction A database connection through which all database operations are immediately written to the database.

back-to-back process A process in JD Edwards EnterpriseOne Supply Management that contains the same keys that are used in another process.

batch processing A process of transferring records from a third-party system to JD Edwards EnterpriseOne.

In JD Edwards EnterpriseOne Financial Management, batch processing enables you to transfer invoices and vouchers that are entered in a system other than JD Edwards EnterpriseOne to JD Edwards EnterpriseOne Accounts Receivable and JD Edwards EnterpriseOne Accounts Payable, respectively. In addition, you can transfer address book information, including customer and supplier records, to JD Edwards EnterpriseOne.

batch server A server that is designated for running batch processing requests. A batch server typically does not contain a database nor does it run interactive applications.

batch-of-one immediate A transaction method that enables a client application to perform work on a client workstation, then submit the work all at once to a server application for further processing. As a batch process is running on the server, the client application can continue performing other tasks.

See also direct connect and store-and-forward.

best practices Non-mandatory guidelines that help the developer make better design decisions.

BPEL	Abbreviation for Business Process Execution Language, a standard web services orchestration language, which enables you to assemble discrete services into an end-to-end process flow.
BPEL PM	Abbreviation for Business Process Execution Language Process Manager, a comprehensive infrastructure for creating, deploying, and managing BPEL business processes.
Build Configuration File	Configurable settings in a text file that are used by a build program to generate ANT scripts. ANT is a software tool used for automating build processes. These scripts build published business services.
build engineer	An actor that is responsible for building, mastering, and packaging artifacts. Some build engineers are responsible for building application artifacts, and some are responsible for building foundation artifacts.
Build Program	A WIN32 executable that reads build configuration files and generates an ANT script for building published business services.
business analyst	An actor that determines if and why an EnterpriseOne business service needs to be developed.
business function	A named set of user-created, reusable business rules and logs that can be called through event rules. Business functions can run a transaction or a subset of a transaction (check inventory, issue work orders, and so on). Business functions also contain the application programming interfaces (APIs) that enable them to be called from a form, a database trigger, or a non-JD Edwards EnterpriseOne application. Business functions can be combined with other business functions, forms, event rules, and other components to make up an application. Business functions can be created through event rules or third-generation languages, such as C. Examples of business functions include Credit Check and Item Availability.
business function event rule	See named event rule (NER).
business service	EnterpriseOne business logic written in Java. A business service is a collection of one or more artifacts. Unless specified otherwise, a business service implies both a published business service and business service.
business service artifacts	Source files, descriptors, and so on that are managed for business service development and are needed for the business service build process.
business service class method	A method that accesses resources provided by the business service framework.
business service configuration files	Configuration files include, but are not limited to, interop.ini, JDBj.ini, and jdelog.properties.
business service cross reference	A key and value data pair used during orchestration. Collectively refers to both the code and the key cross reference in the WSG/XPI based system.
business service cross-reference utilities	Utility services installed in a BPEL/ESB environment that are used to access JD Edwards EnterpriseOne orchestration cross-reference data.
business service development environment	A framework needed by an integration developer to develop and manage business services.
business services development tool	Otherwise known as JDeveloper.
business service EnterpriseOne object	A collection of artifacts managed by EnterpriseOne LCM tools. Named and represented within EnterpriseOne LCM similarly to other EnterpriseOne objects like tables, views, forms, and so on.

business service framework Parts of the business service foundation that are specifically for supporting business service development.

business service payload An object that is passed between an enterprise server and a business services server. The business service payload contains the input to the business service when passed to the business services server. The business service payload contains the results from the business service when passed to the Enterprise Server. In the case of notifications, the return business service payload contains the acknowledgement.

business service property Key value data pairs used to control the behavior or functionality of business services.

Business Service Property Admin Tool An EnterpriseOne application for developers and administrators to manage business service property records.

business service property business service group A classification for business service property at the business service level. This is generally a business service name. A business service level contains one or more business service property groups. Each business service property group may contain zero or more business service property records.

business service property categorization A way to categorize business service properties. These properties are categorized by business service.

business service property key A unique name that identifies the business service property globally in the system.

business service property utilities A utility API used in business service development to access EnterpriseOne business service property data.

business service property value A value for a business service property.

business service repository A source management system, for example ClearCase, where business service artifacts and build files are stored. Or, a physical directory in network.

business services server The physical machine where the business services are located. Business services are run on an application server instance.

business services source file or business service class One type of business service artifact. A text file with the .java file type written to be compiled by a Java compiler.

business service value object template The structural representation of a business service value object used in a C-business function.

Business Service Value Object Template Utility A utility used to create a business service value object template from a business service value object.

business services server artifact The object to be deployed to the business services server.

business view A means for selecting specific columns from one or more JD Edwards EnterpriseOne application tables whose data is used in an application or report. A business view does not select specific rows, nor does it contain any actual data. It is strictly a view through which you can manipulate data.

central objects merge A process that blends a customer's modifications to the objects in a current release with objects in a new release.

central server A server that has been designated to contain the originally installed version of the software (central objects) for deployment to client computers. In a typical JD Edwards EnterpriseOne installation, the software is loaded on to one machine—the central server. Then, copies of the software are pushed out or downloaded to various workstations attached to it. That way, if the software is altered or corrupted through its use on workstations, an original set of objects (central objects) is always available on the central server.

charts Tables of information in JD Edwards EnterpriseOne that appear on forms in the software.

check-in repository A repository for developers to check in and check out business service artifacts. There are multiple check-in repositories. Each can be used for a different purpose (for example, development, production, testing, and so on).

connector Component-based interoperability model that enables third-party applications and JD Edwards EnterpriseOne to share logic and data. The JD Edwards EnterpriseOne connector architecture includes Java and COM connectors.

contra/clearing account A general ledger account in JD Edwards EnterpriseOne Financial Management that is used by the system to offset (balance) journal entries. For example, you can use a contra/clearing account to balance the entries created by allocations in JD Edwards EnterpriseOne Financial Management.

Control Table Workbench An application that, during the Installation Workbench processing, runs the batch applications for the planned merges that update the data dictionary, user-defined codes, menus, and user override tables.

control tables merge A process that blends a customer's modifications to the control tables with the data that accompanies a new release.

correlation data The data used to tie HTTP responses with requests that consist of business service name and method.

cost assignment The process in JD Edwards EnterpriseOne Advanced Cost Accounting of tracing or allocating resources to activities or cost objects.

cost component In JD Edwards EnterpriseOne Manufacturing, an element of an item's cost (for example, material, labor, or overhead).

credentials A valid set of JD Edwards EnterpriseOne username/password/environment/role, EnterpriseOne session, or EnterpriseOne token.

Cross-reference utility services Utility services installed in a BPEL/ESB environment that access EnterpriseOne cross-reference data.

cross segment edit A logic statement that establishes the relationship between configured item segments. Cross segment edits are used to prevent ordering of configurations that cannot be produced.

currency restatement The process of converting amounts from one currency into another currency, generally for reporting purposes. You can use the currency restatement process, for example, when many currencies must be restated into a single currency for consolidated reporting.

cXML A protocol used to facilitate communication between business documents and procurement applications, and between e-commerce hubs and suppliers.

database credentials A valid database username/password.

database server A server in a local area network that maintains a database and performs searches for client computers.

Data Source Workbench An application that, during the Installation Workbench process, copies all data sources that are defined in the installation plan from the Data Source Master and Table and Data Source Sizing tables in the Planner data source to the system-release number data source. It also updates the Data Source Plan detail record to reflect completion.

date pattern A calendar that represents the beginning date for the fiscal year and the ending date for each period in that year in standard and 52-period accounting.

denominated-in currency The company currency in which financial reports are based.

deployment artifacts Artifacts that are needed for the deployment process, such as servers, ports, and such.

deployment server A server that is used to install, maintain, and distribute software to one or more enterprise servers and client workstations.

detail information Information that relates to individual lines in JD Edwards EnterpriseOne transactions (for example, voucher pay items and sales order detail lines).

direct connect A transaction method in which a client application communicates interactively and directly with a server application.

See also batch-of-one immediate and store-and-forward.

Do Not Translate (DNT) A type of data source that must exist on the iSeries because of BLOB restrictions.

dual pricing The process of providing prices for goods and services in two currencies.

duplicate published business services authorization records Two published business services authorization records with the same user identification information and published business services identification information.

embedded application server instance An OC4J instance started by and running wholly within JDeveloper.

edit code A code that indicates how a specific value for a report or a form should appear or be formatted. The default edit codes that pertain to reporting require particular attention because they account for a substantial amount of information.

edit mode A condition of a form that enables users to change data.

edit rule A method used for formatting and validating user entries against a predefined rule or set of rules.

Electronic Data Interchange (EDI) An interoperability model that enables paperless computer-to-computer exchange of business transactions between JD Edwards EnterpriseOne and third-party systems. Companies that use EDI must have translator software to convert data from the EDI standard format to the formats of their computer systems.

embedded event rule An event rule that is specific to a particular table or application. Examples include form-to-form calls, hiding a field based on a processing option value, and calling a business function. Contrast with the business function event rule.

Employee Work Center A central location for sending and receiving all JD Edwards EnterpriseOne messages (system and user generated), regardless of the originating application or user. Each user has a mailbox that contains workflow and other messages, including Active Messages.

enterprise server A server that contains the database and the logic for JD Edwards EnterpriseOne.

Enterprise Service Bus (ESB) Middleware infrastructure products or technologies based on web services standards that enable a service-oriented architecture using an event-driven and XML-based messaging framework (the bus).

EnterpriseOne administrator An actor responsible for the EnterpriseOne administration system.

EnterpriseOne credentials A user ID, password, environment, and role used to validate a user of EnterpriseOne.

EnterpriseOne object A reusable piece of code that is used to build applications. Object types include tables, forms, business functions, data dictionary items, batch processes, business views, event rules, versions, data structures, and media objects.

EnterpriseOne development client Historically called "fat client," a collection of installed EnterpriseOne components required to develop EnterpriseOne artifacts, including the Microsoft Windows client and design tools.

EnterpriseOne extension A JDeveloper component (plug-in) specific to EnterpriseOne. A JDeveloper wizard is a specific example of an extension.

EnterpriseOne process A software process that enables JD Edwards EnterpriseOne clients and servers to handle processing requests and run transactions. A client runs one process, and servers can have multiple instances of a process. JD Edwards EnterpriseOne processes can also be dedicated to specific tasks (for example, workflow messages and data replication) to ensure that critical processes don't have to wait if the server is particularly busy.

EnterpriseOne resource Any EnterpriseOne table, metadata, business function, dictionary information, or other information restricted to authorized users.

Environment Workbench An application that, during the Installation Workbench process, copies the environment information and Object Configuration Manager tables for each environment from the Planner data source to the system-release number data source. It also updates the Environment Plan detail record to reflect completion.

escalation monitor A batch process that monitors pending requests or activities and restarts or forwards them to the next step or user after they have been inactive for a specified amount of time.

event rule A logic statement that instructs the system to perform one or more operations based on an activity that can occur in a specific application, such as entering a form or exiting a field.

explicit transaction Transaction used by a business service developer to explicitly control the type (auto or manual) and the scope of transaction boundaries within a business service.

exposed method or value object Published business service source files or parts of published business service source files that are part of the published interface. These are part of the contract with the customer.

facility An entity within a business for which you want to track costs. For example, a facility might be a warehouse location, job, project, work center, or branch/plant. A facility is sometimes referred to as a "business unit."

fast path A command prompt that enables the user to move quickly among menus and applications by using specific commands.

file server A server that stores files to be accessed by other computers on the network. Unlike a disk server, which appears to the user as a remote disk drive, a file server is a sophisticated device that not only stores files, but also manages them and maintains order as network users request files and make changes to these files.

final mode The report processing mode of a processing mode of a program that updates or creates data records.

foundation A framework that must be accessible for execution of business services at runtime. This includes, but is not limited to, the Java Connector and JDBj.

FTP server A server that responds to requests for files via file transfer protocol.

header information Information at the beginning of a table or form. Header information is used to identify or provide control information for the group of records that follows.

HTTP Adapter A generic set of services that are used to do the basic HTTP operations, such as GET, POST, PUT, DELETE, TRACE, HEAD, and OPTIONS with the provided URL.

instantiate A Java term meaning "to create." When a class is instantiated, a new instance is created.

integration developer The user of the system who develops, runs, and debugs the EnterpriseOne business services. The integration developer uses the EnterpriseOne business services to develop these components.

integration point (IP) The business logic in previous implementations of EnterpriseOne that exposes a document level interface. This type of logic used to be called XBPs. In EnterpriseOne 8.11, IPs are implemented in Web Services Gateway powered by webMethods.

integration server A server that facilitates interaction between diverse operating systems and applications across internal and external networked computer systems.

integrity test A process used to supplement a company's internal balancing procedures by locating and reporting balancing problems and data inconsistencies.

interface table See Z table.

internal method or value object Business service source files or parts of business service source files that are not part of the published interface. These could be private or protected methods. These could be value objects not used in published methods.

interoperability model A method for third-party systems to connect to or access JD Edwards EnterpriseOne.

in-your-face-error In JD Edwards EnterpriseOne, a form-level property which, when enabled, causes the text of application errors to appear on the form.

IServer service This internet server service resides on the web server and is used to speed up delivery of the Java class files from the database to the client.

jargon An alternative data dictionary item description that JD Edwards EnterpriseOne appears based on the product code of the current object.

Java application server A component-based server that resides in the middle-tier of a server-centric architecture. This server provides middleware services for security and state maintenance, along with data access and persistence.

JDBNET A database driver that enables heterogeneous servers to access each other's data.

JDEBASE Database Middleware A JD Edwards EnterpriseOne proprietary database middleware package that provides platform-independent APIs, along with client-to-server access.

JDECallObject An API used by business functions to invoke other business functions.

jde.ini A JD Edwards EnterpriseOne file (or member for iSeries) that provides the runtime settings required for JD Edwards EnterpriseOne initialization. Specific versions of the file or member must reside on every machine running JD Edwards EnterpriseOne. This includes workstations and servers.

JDEIPC Communications programming tools used by server code to regulate access to the same data in multiprocess environments, communicate and coordinate between processes, and create new processes.

jde.log The main diagnostic log file of JD Edwards EnterpriseOne. This file is always located in the root directory on the primary drive and contains status and error messages from the startup and operation of JD Edwards EnterpriseOne.

JDENET A JD Edwards EnterpriseOne proprietary communications middleware package. This package is a peer-to-peer, message-based, socket-based, multiprocess communications middleware solution. It handles client-to-server and server-to-server communications for all JD Edwards EnterpriseOne supported platforms.

JDeveloper Project An artifact that JDeveloper uses to categorize and compile source files.

JDeveloper Workspace An artifact that JDeveloper uses to organize project files. It contains one or more project files.

JMS Queue A Java Messaging service queue used for point-to-point messaging.

listener service A listener that listens for XML messages over HTTP.

local repository A developer's local development environment that is used to store business service artifacts.

local standalone BPEL/ESB server A standalone BPEL/ESB server that is not installed within an application server.

Location Workbench An application that, during the Installation Workbench process, copies all locations that are defined in the installation plan from the Location Master table in the Planner data source to the system data source.

logic server A server in a distributed network that provides the business logic for an application program. In a typical configuration, pristine objects are replicated on to the logic server from the central server. The logic server, in conjunction with workstations, actually performs the processing required when JD Edwards EnterpriseOne software runs.

MailMerge Workbench An application that merges Microsoft Word 6.0 (or higher) word-processing documents with JD Edwards EnterpriseOne records to automatically print business documents. You can use MailMerge Workbench to print documents, such as form letters about verification of employment.

Manual Commit transaction A database connection where all database operations delay writing to the database until a call to commit is made.

master business function (MBF) An interactive master file that serves as a central location for adding, changing, and updating information in a database. Master business functions pass information between data entry forms and the appropriate tables. These master functions provide a common set of functions that contain all of the necessary default and editing rules for related programs. MBFs contain logic that ensures the integrity of adding, updating, and deleting information from databases.

master table See published table.

matching document A document associated with an original document to complete or change a transaction. For example, in JD Edwards EnterpriseOne Financial Management, a receipt is the matching document of an invoice, and a payment is the matching document of a voucher.

media storage object Files that use one of the following naming conventions that are not organized into table format: Gxxx, xxxGT, or GTxxx.

message center A central location for sending and receiving all JD Edwards EnterpriseOne messages (system and user generated), regardless of the originating application or user.

messaging adapter An interoperability model that enables third-party systems to connect to JD Edwards EnterpriseOne to exchange information through the use of messaging queues.

messaging server A server that handles messages that are sent for use by other programs using a messaging API. Messaging servers typically employ a middleware program to perform their functions.

Middle-Tier BPEL/ESB Server A BPEL/ESB server that is installed within an application server.

Monitoring Application An EnterpriseOne tool provided for an administrator to get statistical information for various EntepriseOne servers, reset statistics, and set notifications.

named event rule (NER) Encapsulated, reusable business logic created using event rules, rather that C programming. NERs are also called business function event rules. NERs can be reused in multiple places by multiple programs. This modularity lends itself to streamlining, reusability of code, and less work.

nota fiscal In Brazil, a legal document that must accompany all commercial transactions for tax purposes and that must contain information required by tax regulations.

nota fiscal factura In Brazil, a nota fiscal with invoice information.

See also *nota fiscal.*

Object Configuration Manager (OCM) In JD Edwards EnterpriseOne, the object request broker and control center for the runtime environment. OCM keeps track of the runtime locations for business functions, data, and batch applications. When one of these objects is called, OCM directs access to it using defaults and overrides for a given environment and user.

Object Librarian A repository of all versions, applications, and business functions reusable in building applications. Object Librarian provides check-out and check-in capabilities for developers, and it controls the creation, modification, and use of JD Edwards EnterpriseOne objects. Object Librarian supports multiple environments (such as production and development) and enables objects to be easily moved from one environment to another.

Object Librarian merge A process that blends any modifications to the Object Librarian in a previous release into the Object Librarian in a new release.

Open Data Access (ODA) An interoperability model that enables you to use SQL statements to extract JD Edwards EnterpriseOne data for summarization and report generation.

Output Stream Access (OSA) An interoperability model that enables you to set up an interface for JD Edwards EnterpriseOne to pass data to another software package, such as Microsoft Excel, for processing.

package JD Edwards EnterpriseOne objects are installed to workstations in packages from the deployment server. A package can be compared to a bill of material or kit that indicates the necessary objects for that workstation and where on the deployment server the installation program can find them. It is point-in-time snapshot of the central objects on the deployment server.

package build A software application that facilitates the deployment of software changes and new applications to existing users. Additionally, in JD Edwards EnterpriseOne, a package build can be a compiled version of the software. When you upgrade your version of the ERP software, for example, you are said to take a package build.

Consider the following context: “Also, do not transfer business functions into the production path code until you are ready to deploy, because a global build of business functions done during a package build will automatically include the new functions.” The process of creating a package build is often referred to, as it is in this example, simply as “a package build.”

package location The directory structure location for the package and its set of replicated objects. This is usually \\deployment server\release\path_code\package\package name. The subdirectories under this path are where the replicated objects for the package are placed. This is also referred to as where the package is built or stored.

Package Workbench An application that, during the Installation Workbench process, transfers the package information tables from the Planner data source to the system-release number data source. It also updates the Package Plan detail record to reflect completion.

Pathcode Directory The specific portion of the file system on the EnterpriseOne development client where EnterpriseOne development artifacts are stored.

patterns General repeatable solutions to a commonly occurring problem in software design. For business service development, the focus is on the object relationships and interactions. For orchestrations, the focus is on the integration patterns (for example, synchronous and asynchronous request/response, publish, notify, and receive/reply).

planning family A means of grouping end items whose similarity of design and manufacture facilitates being planned in aggregate.

preference profile The ability to define default values for specified fields for a user-defined hierarchy of items, item groups, customers, and customer groups.

print server The interface between a printer and a network that enables network clients to connect to the printer and send their print jobs to it. A print server can be a computer, separate hardware device, or even hardware that resides inside of the printer itself.

pristine environment A JD Edwards EnterpriseOne environment used to test unaltered objects with JD Edwards EnterpriseOne demonstration data or for training classes. You must have this environment so that you can compare pristine objects that you modify.

processing option A data structure that enables users to supply parameters that regulate the running of a batch program or report. For example, you can use processing options to specify default values for certain fields, to determine how information appears or is printed, to specify date ranges, to supply runtime values that regulate program execution, and so on.

production environment A JD Edwards EnterpriseOne environment in which users operate EnterpriseOne software.

production-grade file server A file server that has been quality assurance tested and commercialized and that is usually provided in conjunction with user support services.

Production Published Business Services Web Service Published business services web service deployed to a production application server.

program temporary fix (PTF) A representation of changes to JD Edwards EnterpriseOne software that your organization receives on magnetic tapes or disks.

project In JD Edwards EnterpriseOne, a virtual container for objects being developed in Object Management Workbench.

promotion path The designated path for advancing objects or projects in a workflow. The following is the normal promotion cycle (path):

11>21>26>28>38>01

In this path, *11* equals new project pending review, *21* equals programming, *26* equals QA test/review, *28* equals QA test/review complete, *38* equals in production, *01* equals complete. During the normal project promotion cycle, developers check objects out of and into the development path code and then promote them to the prototype path code. The objects are then moved to the productions path code before declaring them complete.

proxy server A server that acts as a barrier between a workstation and the internet so that the enterprise can ensure security, administrative control, and caching service.

published business service EnterpriseOne service level logic and interface. A classification of a published business service indicating the intention to be exposed to external (non-EnterpriseOne) systems.

published business service identification information Information about a published business service used to determine relevant authorization records. Published business services + method name, published business services, or *ALL.

published business service web service — Published business services components packaged as J2EE Web Service (namely, a J2EE EAR file that contains business service classes, business service foundation, configuration files, and web service artifacts).

published table — Also called a master table, this is the central copy to be replicated to other machines. Residing on the publisher machine, the F98DRPUB table identifies all of the published tables and their associated publishers in the enterprise.

publisher — The server that is responsible for the published table. The F98DRPUB table identifies all of the published tables and their associated publishers in the enterprise.

pull replication — One of the JD Edwards EnterpriseOne methods for replicating data to individual workstations. Such machines are set up as pull subscribers using JD Edwards EnterpriseOne data replication tools. The only time that pull subscribers are notified of changes, updates, and deletions is when they request such information. The request is in the form of a message that is sent, usually at startup, from the pull subscriber to the server machine that stores the F98DRPCN table.

QBE — An abbreviation for query by example. In JD Edwards EnterpriseOne, the QBE line is the top line on a detail area that is used for filtering data.

real-time event — A message triggered from EnterpriseOne application logic that is intended for external systems to consume.

refresh — A function used to modify JD Edwards EnterpriseOne software, or subset of it, such as a table or business data, so that it functions at a new release or cumulative update level, such as B73.2 or B73.2.1.

replication server — A server that is responsible for replicating central objects to client machines.

Rt-Addressing — Unique data identifying a browser session that initiates the business services call request host/port user session.

rules — Mandatory guidelines that are not enforced by tooling, but must be followed in order to accomplish the desired results and to meet specified standards.

quote order — In JD Edwards Procurement and Subcontract Management, a request from a supplier for item and price information from which you can create a purchase order.

In JD Edwards Sales Order Management, item and price information for a customer who has not yet committed to a sales order.

secure by default — A security model that assumes that a user does not have permission to execute an object unless there is a specific record indicating such permissions.

Secure Socket Layer (SSL) — A security protocol that provides communication privacy. SSL enables client and server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

SEI implementation — A Java class that implements the methods that declare in a Service Endpoint Interface (SEI).

selection — Found on JD Edwards EnterpriseOne menus, a selection represents functions that you can access from a menu. To make a selection, type the associated number in the Selection field and press Enter.

serialize — The process of converting an object or data into a format for storage or transmission across a network connection link with the ability to reconstruct the original data or objects when needed.

Server Workbench — An application that, during the Installation Workbench process, copies the server configuration files from the Planner data source to the system-release number

	data source. The application also updates the Server Plan detail record to reflect completion.
Service Endpoint Interface (SEI)	A Java interface that declares the methods that a client can invoke on the service.
SOA	Abbreviation for Service Oriented Architecture.
soft coding	A coding technique that enables an administrator to manipulate site-specific variables that affect the execution of a given process.
source repository	A repository for HTTP adapter and listener service development environment artifacts.
spot rate	An exchange rate entered at the transaction level. This rate overrides the exchange rate that is set up between two currencies.
Specification merge	A merge that comprises three merges: Object Librarian merge, Versions List merge, and Central Objects merge. The merges blend customer modifications with data that accompanies a new release.
specification	A complete description of a JD Edwards EnterpriseOne object. Each object has its own specification, or name, which is used to build applications.
Specification Table Merge Workbench	An application that, during the Installation Workbench process, runs the batch applications that update the specification tables.
SSL Certificate	A special message signed by a certificate authority that contains the name of a user and that user's public key in such a way that anyone can "verify" that the message was signed by no one other than the certification authority and thereby develop trust in the user's public key.
store-and-forward	The mode of processing that enables users who are disconnected from a server to enter transactions and then later connect to the server to upload those transactions.
subscriber table	Table F98DRSUB, which is stored on the publisher server with the F98DRPUB table and identifies all of the subscriber machines for each published table.
superclass	An inheritance concept of the Java language where a class is an instance of something, but is also more specific. "Tree" might be the superclass of "Oak" and "Elm," for example.
supplemental data	Any type of information that is not maintained in a master file. Supplemental data is usually additional information about employees, applicants, requisitions, and jobs (such as an employee's job skills, degrees, or foreign languages spoken). You can track virtually any type of information that your organization needs. For example, in addition to the data in the standard master tables (the Address Book Master, Customer Master, and Supplier Master tables), you can maintain other kinds of data in separate, generic databases. These generic databases enable a standard approach to entering and maintaining supplemental data across JD Edwards EnterpriseOne systems.
table access management (TAM)	The JD Edwards EnterpriseOne component that handles the storage and retrieval of use-defined data. TAM stores information, such as data dictionary definitions; application and report specifications; event rules; table definitions; business function input parameters and library information; and data structure definitions for running applications, reports, and business functions.
Table Conversion Workbench	An interoperability model that enables the exchange of information between JD Edwards EnterpriseOne and third-party systems using non-JD Edwards EnterpriseOne tables.

table conversion An interoperability model that enables the exchange of information between JD Edwards EnterpriseOne and third-party systems using non-JD Edwards EnterpriseOne tables.

table event rules Logic that is attached to database triggers that runs whenever the action specified by the trigger occurs against the table. Although JD Edwards EnterpriseOne enables event rules to be attached to application events, this functionality is application specific. Table event rules provide embedded logic at the table level.

terminal server A server that enables terminals, microcomputers, and other devices to connect to a network or host computer or to devices attached to that particular computer.

three-tier processing The task of entering, reviewing and approving, and posting batches of transactions in JD Edwards EnterpriseOne.

three-way voucher match In JD Edwards Procurement and Subcontract Management, the process of comparing receipt information to supplier's invoices to create vouchers. In a three-way match, you use the receipt records to create vouchers.

transaction processing (TP) monitor A monitor that controls data transfer between local and remote terminals and the applications that originated them. TP monitors also protect data integrity in the distributed environment and may include programs that validate data and format terminal screens.

transaction processing method A method related to the management of a manual commit transaction boundary (for example, start, commit, rollback, and cancel).

transaction set An electronic business transaction (electronic data interchange standard document) made up of segments.

trigger One of several events specific to data dictionary items. You can attach logic to a data dictionary item that the system processes automatically when the event occurs.

triggering event A specific workflow event that requires special action or has defined consequences or resulting actions.

two-way authentication An authentication mechanism in which both client and server authenticate themselves by providing the SSL certificates to each other.

two-way voucher match In JD Edwards Procurement and Subcontract Management, the process of comparing purchase order detail lines to the suppliers' invoices to create vouchers. You do not record receipt information.

user identification information User ID, role, or *public.

User Overrides merge Adds new user override records into a customer's user override table.

value object A specific type of source file that holds input or output data, much like a data structure passes data. Value objects can be exposed (used in a published business service) or internal, and input or output. They are comprised of simple and complex elements and accessories to those elements.

variance In JD Edwards Capital Asset Management, the difference between revenue generated by a piece of equipment and costs incurred by the equipment.

In JD Edwards EnterpriseOne Project Costing and JD Edwards EnterpriseOne Manufacturing, the difference between two methods of costing the same item (for example, the difference between the frozen standard cost and the current cost is an engineering variance). Frozen standard costs come from the Cost Components table, and the current costs are calculated using the current bill of material, routing, and overhead rates.

versioning a published business service Adding additional functionality/interfaces to the published business services without modifying the existing functionality/interfaces.

Version List merge The Versions List merge preserves any non-XJDE and non-ZJDE version specifications for objects that are valid in the new release, as well as their processing options data.

visual assist Forms that can be invoked from a control via a trigger to assist the user in determining what data belongs in the control.

vocabulary override An alternate description for a data dictionary item that appears on a specific JD Edwards EnterpriseOne form or report.

wchar_t An internal type of a wide character. It is used for writing portable programs for international markets.

web application server A web server that enables web applications to exchange data with the back-end systems and databases used in eBusiness transactions.

web server A server that sends information as requested by a browser, using the TCP/IP set of protocols. A web server can do more than just coordination of requests from browsers; it can do anything a normal server can do, such as house applications or data. Any computer can be turned into a web server by installing server software and connecting the machine to the internet.

Web Service Description Language (WSDL) An XML format for describing network services.

Web Service Inspection Language (WSIL) An XML format for assisting in the inspection of a site for available services and a set of rules for how inspection-related information should be made.

web service proxy foundation Foundation classes for web service proxy that must be included in a business service server artifact for web service consumption on WAS.

web service softcoding record An XML document that contains values that are used to configure a web service proxy. This document identifies the endpoint and conditionally includes security information.

web service softcoding template An XML document that provides the structure for a soft coded record.

Where clause The portion of a database operation that specifies which records the database operation will affect.

Windows terminal server A multiuser server that enables terminals and minimally configured computers to display Windows applications even if they are not capable of running Windows software themselves. All client processing is performed centrally at the Windows terminal server and only display, keystroke, and mouse commands are transmitted over the network to the client terminal device.

wizard A type of JDeveloper extension used to walk the user through a series of steps.

workbench A program that enables users to access a group of related programs from a single entry point. Typically, the programs that you access from a workbench are used to complete a large business process. For example, you use the JD Edwards EnterpriseOne Payroll Cycle Workbench (P07210) to access all of the programs that the system uses to process payroll, print payments, create payroll reports, create journal entries, and update payroll history. Examples of JD Edwards EnterpriseOne workbenches include Service Management Workbench (P90CD020), Line Scheduling Workbench (P3153), Planning Workbench (P13700), Auditor's Workbench (P09E115), and Payroll Cycle Workbench.

work day calendar In JD Edwards EnterpriseOne Manufacturing, a calendar that is used in planning functions that consecutively lists only working days so that component and work order scheduling can be done based on the actual number of work days available. A work

	day calendar is sometimes referred to as planning calendar, manufacturing calendar, or shop floor calendar.
workflow	The automation of a business process, in whole or in part, during which documents, information, or tasks are passed from one participant to another for action, according to a set of procedural rules.
workgroup server	A server that usually contains subsets of data replicated from a master network server. A workgroup server does not perform application or batch processing.
XAPI events	A service that uses system calls to capture JD Edwards EnterpriseOne transactions as they occur and then calls third-party software, end users, and other JD Edwards EnterpriseOne systems that have requested notification when the specified transactions occur to return a response.
XML CallObject	An interoperability capability that enables you to call business functions.
XML Dispatch	An interoperability capability that provides a single point of entry for all XML documents coming into JD Edwards EnterpriseOne for responses.
XML List	An interoperability capability that enables you to request and receive JD Edwards EnterpriseOne database information in chunks.
XML Service	An interoperability capability that enables you to request events from one JD Edwards EnterpriseOne system and receive a response from another JD Edwards EnterpriseOne system.
XML Transaction	An interoperability capability that enables you to use a predefined transaction type to send information to or request information from JD Edwards EnterpriseOne. XML transaction uses interface table functionality.
XML Transaction Service (XTS)	Transforms an XML document that is not in the JD Edwards EnterpriseOne format into an XML document that can be processed by JD Edwards EnterpriseOne. XTS then transforms the response back to the request originator XML format.
Z event	A service that uses interface table functionality to capture JD Edwards EnterpriseOne transactions and provide notification to third-party software, end users, and other JD Edwards EnterpriseOne systems that have requested to be notified when certain transactions occur.
Z table	A working table where non-JD Edwards EnterpriseOne information can be stored and then processed into JD Edwards EnterpriseOne. Z tables also can be used to retrieve JD Edwards EnterpriseOne data. Z tables are also known as interface tables.
Z transaction	Third-party data that is properly formatted in interface tables for updating to the JD Edwards EnterpriseOne database.

Index

D

E

F

H

I

J

R

S

T

U

V

W