JD Edwards World

Security Administration Guide

Release A9.4

E50782-03

December 2015

Describes pre- and post installation security considerations, as well as describes how to use JD Edwards World security applications to ensure only authorized individuals have access to JD Edwards World applications, features, and data.

ORACLE

JD Edwards World Security Administration Guide, Release A9.4

E50782-03

Contents

Preface ix

Audience ix
Documentation Accessibility ix
Related Information ix
Conventions ix

Part I JD Edwards World Security Overview

1 Introduction to JD Edwards World Security

1.1 Understand JD Edwards World Security 1-1
1.2 JD Edwards World Security Overview 1-1

2 General Principles of Security

2.1 Keep Software Up to Date 2-1
2.2 Restrict Network Access to Critical Services 2-1
2.3 Minimize the Attack Surface 2-1
2.4 Follow the Principle of Least Privilege 2-2
2.5 Define and Report Separation of Duties 2-2
2.6 Construct an In-depth Defense 2-2
2.7 Monitor System Activity 2-2
2.8 Configure User Accounts Securely 2-2
2.9 Set Up a Change Management Process 2-2

Part II JD Edwards World Authentication Security

3 Installation Overview

3.1 Understand Your Environment 3-1
3.2 Common Deployment Topologies 3-2
3.2.1 Single-Server Deployment 3-2
3.2.2 Deployment Using DMZ 3-2

4 Installing JD Edwards World Components

4.1 Downloading Software from the Oracle Software Delivery Cloud 4-1
4.2 Installing JD Edwards World Base 4-1

4.3 Installing JD Edwards World Web Enablement 4-2
4.4 Installing JD Edwards World Service Enablement 4-2
4.5 Installing the JD Edwards World JDBC Driver 4-2

5 Configuring IBM i Security

5.1 IBM i Network Security 5-1
5.2 Configure the IBM i Security Level 5-1
5.3 IBM i User Security 5-2
5.4 IBM i Resource Security 5-2

Part III JD Edwards World Authorization Security

6 Overview to JD Edwards World User Security

6.1 Objectives 6-1
6.2 About JD Edwards World User Security 6-1

7 Set Up User and Group Security

7.1 Setting Up User Security 7-1
7.2 Securing Command Entry 7-2
7.3 Setting Up Group Security 7-3

8 Work with Menu Security

8.1 Understanding Advanced Menu Security 8-1
8.1.1 Set Up Advanced Security Records 8-2
8.1.2 Activate Advanced Menu Security at the User Level 8-4
8.1.3 Advanced Menu Security - Functional Details 8-5
8.1.4 Advanced Menu Security - Examples 8-6
8.1.5 Wildcard Search 8-8
8.1.5.1 Wildcard Search Examples 8-8
8.2 Menu Masking Security 8-9
8.3 What are the Types of Comparisons in Menu Masking? 8-9
8.4 An Example of Menu Masking 8-10
8.5 Using Group Profile or *PUBLIC with Menu Masking 8-10
8.6 Verifying Menu Security Setup 8-11
8.7 Securing Hidden Selections 8-12
8.7.1 Securing Hidden Selection 60 (HS60) 8-12
8.7.2 Preventing Users from Receiving a Send Window Message 8-12
8.7.3 Securing Hidden Selection 33 (HS33) 8-13
8.8 Considerations for Menu Masking 8-14

9 Set Up Action Code, Fast Path, Generic Text, and Search Type Security

9.1 Setting Up Action Code Security 9-1
9.1.1 General Guidelines 9-4
9.2 Setting Up Fast Path Security 9-5
9.3 Setting Up Generic Text Security 9-7

9.3.1 Setup Guidelines 9-10
9.3.1.1 No Role or Group Setup 9-10
9.3.1.2 No Role Setup, User Belongs to a Group 9-10
9.3.1.3 User Signs on with a Security Role 9-11
9.3.2 Security Setup Examples 9-11
9.3.2.1 Example 1 9-11
9.3.2.2 Example 2 9-12
9.3.3 Wildcard Search 9-12
9.3.3.1 Wildcard Search Examples 9-13
9.4 Setting Up Search Type Security 9-13
9.4.1 Activating Search Type Security 9-14
9.4.2 General Guidelines 9-16
9.4.3 Check Sequence for Action Type and Search Type Security 9-16
9.4.3.1 Examples 9-17

10 Work with Business Unit Security

10.1 About Business Unit Security 10-1
10.1.1 Setting up Business Unit Security 10-2
10.2 Considerations for Business Unit Security 10-3
10.2.1 Files Secured Using Business Unit Security 10-4
10.2.2 Alphanumeric and Numeric Characters for Business Unit Setup 10-4
10.2.2.1 Alphanumeric Business Unit Definition 10-4
10.2.2.2 Numeric Business Unit Definition 10-4
10.2.2.3 Planning Business Unit Setup 10-5
10.2.3 Business Unit Ranges 10-5
10.3 Checking Business Unit Security 10-6
10.4 Technical Considerations for Business Unit Security 10-6

11 Work with Function Key Security

11.1 About Function Key Security 11-1
11.2 Working with Function Key Security 11-2
11.2.1 General Guidelines 11-3
11.2.2 Function Code Security - Helpful Hints 11-4
11.3 Standard Function Keys 11-4
11.3.1 Examples 11-5
11.3.1.1 Example 1 11-5
11.3.1.2 Example 2 11-5
11.3.1.3 Example 1 11-5

12 Work with Field Level Masking

12.1 Understanding Field Level Masking 12-1
12.2 Reviewing the Field Level Masking Flow 12-2
12.3 Tasks to Set up Field Level Masking 12-4
12.4 Field Masking Inclusions 12-4
12.4.1 File Name Selection Window (P941SLW) 12-6
12.5 Setting up Data Item Masking Definitions 12-6

12.5.1 Examples of Data Item Masking Definitions 12-7
12.5.2 Data Item Selection window (P941SLW) 12-11
12.6 Setting up Database Field Level Masking 12-11
12.6.1 File Name Selection window (P941SLW) 12-14
12.7 Working with Field Level Masking Workbench 12-14
12.8 Setting Field Level Masking 12-15
12.9 Dropping Field Level Masking 12-16

13 Set Up User Defined Codes Security

13.1 Setting Up User Defined Codes Security 13-1
13.1.1 General Guidelines 13-2
13.1.2 User Defined Codes Security - Helpful Hints 13-3

14 Set Up Batch Approval/Post Security

14.1 Setting Up Batch Approval/Post Security 14-1

15 Set Up Report Writer Security

15.1 Setting up Report Writer Form Security 15-1
15.1.1 General Guidelines 15-4
15.2 Updating Report Writer Version Security 15-5
15.3 Masking DREAM Writer Processing Options 15-7

16 Change User Profile Ownership

16.1 Changing User Profile Ownership 16-1

17 Work With the Security Workbench

17.1 Understanding the Security Workbench 17-1
17.2 Using the Security Workbench 17-2
17.2.1 Security Workbench Options 17-4
17.2.2 Security Workbench Function Keys 17-5
17.2.3 DREAM Writer Considerations 17-5
17.2.4 Security Workbench Examples 17-6
17.2.4.1 Example 1 17-6
17.2.4.2 Example 2 17-6
17.2.5 Exporting Security Data from the Security Workbench 17-7
17.3 Working With the Security Tester 17-7
17.3.1 Security Tester Options 17-9
17.3.2 Security Tester Examples 17-9
17.3.2.1 Example 1 17-9
17.3.2.2 Example 2 17-10
17.3.3 Wildcard Search 17-10
17.3.3.1 Wildcard Search Examples 17-11
17.3.4 Detail Column 17-11
17.4 Understanding the Security Detail Report 17-14
17.4.1 DREAM Writer Considerations 17-15

17.4.2 Exporting Security Data from the Security Detail Report 17-16

18 Work with Configuration Master Records

18.1 Working with Configuration Master Records 18-1

19 Security Reporting

19.1 General Guidelines 19-1
19.2 Configuring and Using User Activity Reporting 19-2
19.3 Configuring and Using Database Audit Manager 19-2
19.4 Configuring and Using Segregation of Duties Reports 19-3

Part IV JD Edwards World Developer Security

20 Development Environments

20.1 Developer Access 20-1
20.2 Libraries 20-1
20.3 Program Source 20-1

21 Application Security Policies

21.1 Menu Security 21-1
21.2 Action Code Security 21-1
21.3 Function Key Security 21-1
21.4 Video Design 21-2
21.5 DREAM Writer 21-2
21.6 Data Dictionary and User Defined Codes 21-2
21.7 File Audit Fields 21-2
21.8 User Authentication 21-2

22 Object Security Policies

22.1 File Objects 22-1
22.2 Program Objects 22-1
22.3 Adopted Authority 22-1

Part V Appendices

A.1 About Secure Deployment Checklist A-1
B.1 Proof of Field Level Masking Set B-10
B.2 Test the Masking Field on a Screen and a Report B-12
C.1 Object Authority - Help C-1
C.2 Field Level Masking – Authority Rights C-1

Index

Preface

Welcome to the *JD Edwards World Security Administration Guide*.

Audience

This guide is intended for system administrators and technical consultants who are responsible for setting up user, role, and application security, as well as LDAP and single sign-on configurations for JD Edwards World.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Information

For additional information about JD Edwards World applications, features, content, and training, visit the JD Edwards World pages on the JD Edwards Resource Library located at:

http://learnjde.com

Conventions

This document uses the following text conventions:

Convention	Explanation
boldface	Indicates cautionary information or terms defined in the glossary.
Italics	Indicates book titles or emphasis.

Part I

JD Edwards World Security Overview

This part contains the following chapters:

- Chapter 1, "Introduction to JD Edwards World Security"
- Chapter 2, "General Principles of Security"

1

Introduction to JD Edwards World Security

This chapter contains the following topics:

- Understand JD Edwards World Security
- JD Edwards World Security Overview

1.1 Understand JD Edwards World Security

JD Edwards World is a full-featured, reliable Enterprise Resource Planning (ERP) software product with a long track record of efficient transaction processing capability and low Total Cost of Ownership (TCO).

JD Edwards World is written mainly in IBM RPG, CL, and SQL languages and runs exclusively on IBM hardware, currently the Power Systems line of computers with the IBM i for Business operating system. The computing model is centralized, with all programs running on the IBM i server. Client applications communicate via the native 5250 interface, whether through Windows clients or through a Web browser. The JD Edwards World product operates within the IBM i environment, and it depends on a secure configuration at the operating system level.

In recent releases, the JD Edwards World product has expanded beyond traditional RPG- based, centralized mainframe applications. We have implemented server-side, Java-based applications such as Web Enablement (with the Seagull LegaSuite GUI), Service Enablement (Web services), JD Edwards World JDBC Driver and Electronic Document Delivery (EDD). Each of these features comes with its own set of security considerations.

Note: In this guide, the phrase IBM i refers to the IBM i for Business operating system and the server it runs on. This operating system may be running on hardware servers named iSeries, i5, or Power Systems. The IBM i operating system is the current version of the operating system originating on the IBM AS/400 server.

1.2 JD Edwards World Security Overview

This security guide provides guidelines and recommendations for installing, configuring, and monitoring Oracle's JD Edwards World product to make it more secure in customer environments. This is a practical guide for technical users, installers, and system administrators who implement and maintain the JD Edwards World system. This document discusses guidelines for how to address security at a customer implementation, including hardening of the IBM i operating system

environment, hardening of the JD Edwards World security applications, and other system hardening configuration recommendations.

We cannot address every security scenario that might be applicable to a particular implementation and environment; therefore, this document provides basic recommendations for securing JD Edwards World. We recommend that before implementing your World system you fully test the security setup in a non-production environment to ensure proper functionality and integrity.

In today's environment, a properly secured computing infrastructure is critical. As companies expand, so does the complexity of their business processes. In an internet environment, the risks to valuable and sensitive data are greater than ever before. In addition, a company's computing infrastructure grows as more third-party products are integrated with its enterprise software. As a result, this type of environment can create potential security gaps. This security guide will help you ensure that JD Edwards World and the various components involved in a JD Edwards World setup are properly secured.

You must secure each JD Edwards World environment in alignment with your company's enterprise security policies. Those policies should be created based upon your established security model. When securing a JD Edwards World environment, you should take a comprehensive approach that agrees with your overall corporate security policies, guidelines, and business requirements. This guide covers guidelines and recommendations for securing a JD Edwards World environment based on security features available as of JD Edwards World Release A9.3.

This guide is not intended to replace the JD Edwards World technical documentation delivered with the product. It provides references to relevant information in JD Edwards World technical documentation guides. Readers of this guide should have a good understanding of the JD Edwards World system. Implementing JD Edwards World security requires an in-depth understanding of many disciplines, including IBM i security administration, JD Edwards World security administration, and network security administration.

2

General Principles of Security

The following principles are fundamental to using any application securely. These principles will be referenced throughout this guide.

This chapter contains the following topics:

- Section 2.1, "Keep Software Up to Date"
- Section 2.2, "Restrict Network Access to Critical Services"
- Section 2.3, "Minimize the Attack Surface"
- Section 2.4, "Follow the Principle of Least Privilege"
- Section 2.5, "Define and Report Separation of Duties"
- Section 2.6, "Construct an In-depth Defense"
- Section 2.7, "Monitor System Activity"
- Section 2.8, "Configure User Accounts Securely"
- Section 2.9, "Set Up a Change Management Process"

2.1 Keep Software Up to Date

One of the principles of good security practice is to keep all software versions and updates current, to take advantage of improvements in new releases. Throughout this document, we assume a JD Edwards World Release level of A9.3 and A9.4.

2.2 Restrict Network Access to Critical Services

Keep the IBM i behind a firewall. In addition, if you are using Web Enablement, consider placing a firewall between the LegaSuite GUI server and the System i. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

2.3 Minimize the Attack Surface

This principle encourages the security administrator to reduce the number of possible security vulnerabilities by removing unused or unnecessary system objects and security capabilities. This action may include removing unused IBM User Profiles and JD Edwards User records. It may also include the use of IBM's Adopted Authority feature on the IBM i.

2.4 Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege necessary to perform their jobs. Overambitious granting of authorities, especially early on in an organization's life cycle, when people are few and work needs to be done quickly, often leaves a system open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities. Previously, the common security practice was to grant all access to all users and to restrict authority on a selected basis. In today's security environment, all authorities should be denied as a general rule and selected authority granted where needed. The security modifications beginning in World release A9.3 support this principle by using "no access" as the authorization default.

2.5 Define and Report Separation of Duties

To minimize possible system abuse by otherwise authorized users, the security administrator must define conflicts of responsibility and take steps to ensure that users are not allowed capabilities that conflict from a security standpoint. For example, the user responsible for printing Accounts Payable checks should not be the same person who is responsible for setting up suppliers and approving invoices.

2.6 Construct an In-depth Defense

Your overall security strategy should not rely on one security layer. If one security defense is defeated, you should have reasonable redundancies. For example, you may want to set up Menu Security to restrict unauthorized users from a particular module (such as Payroll), but also set up Action Code Security on critical Payroll programs and secure the Payroll files using IBM i Resource Security.

2.7 Monitor System Activity

One of the main requirements of system security is monitoring. Auditing and reviewing audit records address this requirement. Each component within a system has some degree of monitoring capability. Establish a policy to check and monitor activities in your system regularly. Refer to the IBM i database and operating system documentation for audit functionality. For JD Edwards World, follow the advice in this document and regularly monitor audit records.

2.8 Configure User Accounts Securely

Good security requires secure accounts. Establish a policy to set up strict password controls for all accounts so that passwords are not easily compromised. In addition, establish a policy that requires users to periodically change passwords, perhaps every 90 days.

2.9 Set Up a Change Management Process

Establish a policy to set up a change management process to keep track of all the changes in your software systems. All changes to software should be approved and audited.

Part II

JD Edwards World Authentication Security

JD Edwards World, working with IBM i, has a number of security features designed to protect your information and prevent abuse, accidental loss, or corruption.

This part contains the following chapters:

- Chapter 3, "Installation Overview"
- Chapter 4, "Installing JD Edwards World Components"
- Chapter 5, "Configuring IBM i Security"

3

Installation Overview

This chapter outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems.

This chapter contains these topics:

- Section 3.1, "Understand Your Environment,"
- Section 3.2, "Common Deployment Topologies,"

3.1 Understand Your Environment

To better understand your security needs, answer the following questions:

Which resources am I protecting?

You can protect many resources in the production environment. The most critical is your JD Edwards World database on the IBM i, which contains information that is both sensitive and critical to the performance of your business. The database information also represents a substantial investment in time and resources to build and maintain. You also must keep your production software secure and reliable. Computing hardware is also a substantial investment, as well as a critical operating resource. Finally, the reputation of your business may rest on the integrity and performance of your computing resources. Consider the resources you want to protect when deciding the level of security you must provide.

From whom am I protecting the resources?

You must protect most of your computing resources from unauthorized access, manipulation, or destruction from both internal and external parties. Employees may represent a security vulnerability as important as an outside hacker. For Web Enablement or Service Enablement, you must protect resources from unauthorized access via the Internet. But should you protect the Web site from the employees on the intranet in your enterprise? Access to highly confidential data or strategic resources should be available to only a few trusted users or system administrators. System administrators may not need access to confidential data. Power users may not need access to some system resources.

What will happen if the protections on strategic resources fail?

In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might lead to great damage to database information, systems, or resources. Understanding the security ramifications of each resource will help you protect it properly.

What is my overall security approach?

Before starting the process of setting up a specific security configuration, you should make an overall plan of your security environment. How does the IBM i fit into the overall corporate computing environment? How does JD Edwards security work within the IBM i security environment? In each area, the security policy should be upheld with a tactical action plan, and each area should complement the security features of the other, creating a synergistic "defense in depth".

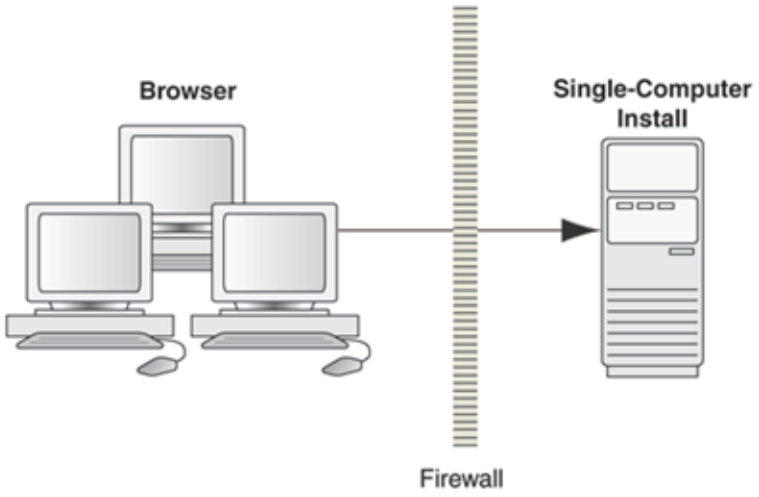
3.2 Common Deployment Topologies

The JD Edwards World system runs only on a centralized IBM i server. The Web Enablement feature, however, brings Internet browser-based access to the World system, so some deployment options must be considered. This section describes common architectures for deploying Oracle JD Edwards World products to secure Internet access.

3.2.1 Single-Server Deployment

The following graphic shows one simple deployment architecture that includes browser-based access. In this scenario, users access JD Edwards World via a browser using World Web Enablement, and the Web Enablement (Seagull LegaSuite GUI) server resides on the same server as the World system. The IBM i server is located behind the corporate firewall.

Figure 3–1 Single-Computer Deployment Architecture



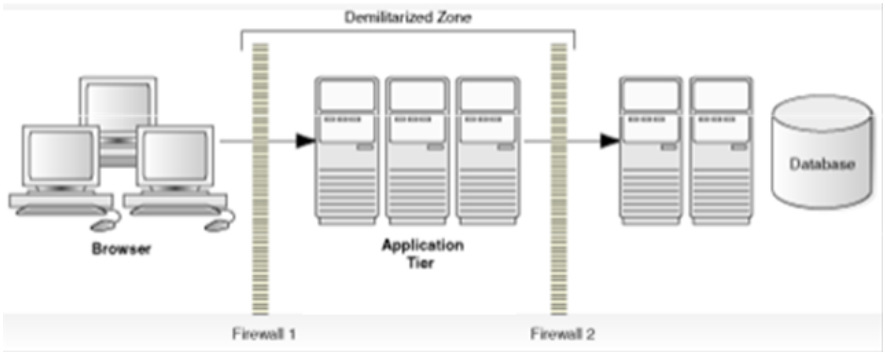
Note: Users may also have access to the IBM i, and thus the World system, using workstation-based software such as 5250 terminal emulation software, communicating to the IBM i via the corporate network (intranet). Some older installations could also have actual 5250 terminals communicating to the IBM i via hard-wired local networks.

3.2.2 Deployment Using DMZ

Another deployment architecture that includes browser-based access is shown in the following graphic. In this scenario, users again access JD Edwards World via a browser

using World Web Enablement, but the Web Enablement server resides on a server in the DMZ and communicates to the IBM i server residing behind a second firewall.

Figure 3–2 Traditional DMZ View



Note: The term demilitarized zone (DMZ) refers to a server that is isolated by firewalls from both the Internet and the intranet, thus forming a buffer between the two.

Firewalls separating DMZ zones provide two essential functions:

- Block any traffic types that are known to be illegal.
- Provide intrusion containment should successful intrusions take over processes or processors.

4

Installing JD Edwards World Components

This chapter contains these topics:

- Section 4.1, "Downloading Software from the Oracle Software Delivery Cloud,"
- Section 4.2, "Installing JD Edwards World Base,"
- Section 4.3, "Installing JD Edwards World Web Enablement,"
- Section 4.4, "Installing JD Edwards World Service Enablement,"
- Section 4.5, "Installing the JD Edwards World JDBC Driver,"

4.1 Downloading Software from the Oracle Software Delivery Cloud

The Oracle Software Delivery Cloud is the preferred delivery mechanism for JD Edwards World software components.

4.2 Installing JD Edwards World Base

For detailed installation instructions, refer to the JD Edwards World Quick Installation Guide.

This section describes how to install and configure the JD Edwards World Base product and additional components securely. Overall recommendations in this guide should be considered when following the Quick Installation Guide.

The base product is written mainly in RPG and processes on the IBM i. Oracle delivers JD Edwards World via download from the Oracle Software Delivery Cloud or DVD. The setup.exe does the transfer, it is not something the customer does manually. After the software is successfully transferred to the IBM i, you must securely archive or remove any Windows-based copies.

Before configuring the JD Edwards World Base product's security configuration, you should determine the overall security approach and be prepared to configure necessary features of IBM i security along with the JD Edwards security.

During the installation, three IBM User Profiles are created or modified for use during the installation: JDE, JDEINSTAL, and JDEPROD. In the past, these profiles were created with passwords that matched the user ID. Beginning with JD Edwards World release A9.3, you must supply a password for each if the profile does not already exist on your machine. These profiles are for the following purposes:

- JDE – This is the user account that will own the installed objects.
- JDEINSTAL – This is the user account to use when configuring the install.

- JDEPROD – This is a sample production JD Edwards User. You may keep it after the install.

After installation and configuration, disposition of these profiles is as follows:

- JDE – This profile typically owns the installed objects and it is used to sign into the pristine environment. Keep it, but disable it from signon.
- JDEINSTAL – Disable it.
- JDEPROD –The IBM Profile will be disabled from signing on by default.

4.3 Installing JD Edwards World Web Enablement

For detailed installation instructions, refer to the JD Edwards World Web Enablement Installation and Configuration Guide.

This section describes how to install and configure the JD Edwards World Web Enablement securely. Overall recommendations in this guide should be considered when following the Web Enablement Installation and Configuration Guide.

JD Edwards World Web Enablement components are installed and run on the IBM i or on a Windows server running an HTTP server such as Apache. Oracle recommends that you install the HTTP server on a computer system that has restricted access, both physically and through the network.

4.4 Installing JD Edwards World Service Enablement

For detailed installation instructions, refer to the JD Edwards World Service Enablement Installation and Configuration Guide. Overall recommendations in this guide should be considered when following the World Service Enablement Installation and Configuration Guide.

JD Edwards World Service Enablement components are installed and run on the Oracle WebLogic Server. Oracle recommends that you install the Oracle WebLogic Server on a computer system that has restricted access, both physically and through the network. Detailed Oracle WebLogic security practices are discussed in the Oracle Fusion Middleware Understanding Security for Oracle WebLogic Server guide.

4.5 Installing the JD Edwards World JDBC Driver

For detailed installation instructions, refer to the JD Edwards World JDBC Driver Guide.

The World JDBC driver components are installed on any Windows platform or on an IBM i system and can be used in support of JD Edwards World Service Enablement, Oracle BI Publisher, or any application that needs to read JD Edwards World business data. The World JDBC driver uses your existing World security setup to secure the files and data that it accesses. In most cases, the existing World security setup is all that is necessary to secure the specific features provided by the JDBC driver. Specifically, the following existing security setup features are leveraged by the World JDBC driver:

- Use IBM i security to identify and secure users and IBM i system objects, such as specific libraries and files.
- Use JD Edwards World users, groups, and environments to control access to specific libraries and files.
- Use business unit security to limit rows to specific business units in all files.

- Use action code security to manage which SQL statements may be used against the database.
- Use column security to manage which specific tables and columns may be queried or updated.

By default, any user who can log into JD Edwards World may use the JD Edwards JDBC driver to read data from JD Edwards data files.

5

Configuring IBM i Security

JD Edwards World operates within the confines of IBM i security and relies upon a secure operating system configuration. This section discusses IBM i security features that are especially relevant to the JD Edwards World product. This guide is not a substitute for fully understanding and configuring the IBM i security environment. Please refer to the IBM i Security Guide for the IBM i release you are running.

This chapter contains these topics:

- Section 5.1, "IBM i Network Security,"
- Section 5.2, "Configure the IBM i Security Level,"
- Section 5.3, "IBM i User Security,"
- Section 5.4, "IBM i Resource Security,"

5.1 IBM i Network Security

Harden the Network Security Environment

The IBM i usually operates in an environment where access to the corporate network and the Internet are available. The IBM i should be protected behind a firewall, and it should be hardened to only allow authorized communications. You should close unnecessary communications ports.

5.2 Configure the IBM i Security Level

The IBM i operating system may be installed to operate at one of four Security Levels:

- Level 20 – Signon security only; minimal security protection.
- Level 30 – Signon and resource security.
- Level 40 – Signon and resource security; integrity protection.
- Level 50 – Signon and resource security; enhanced integrity protection.

Each of these security levels has implications for other security settings in the operating system. You can view your current IBM i Security Level using the following command:

DSPSECA

Oracle recommends that you configure your IBM i Security Level at Level 40 or Level 50.

5.3 IBM i User Security

Lock and Expire Default User Accounts

The IBM i is delivered with many default accounts, such as QSECOFR and QPGMR. Oracle provides three additional user accounts during JD Edwards World installation: JDE, JDEINSTAL, and JDEPROD. You must change the passwords or disable signon for all default accounts. Refer to the appropriate IBM i Security guide for details.

Change Default User Passwords

You must supply a password for each if the profile does not already exist on your machine. After the JD Edwards World software is installed, these default accounts should be dispositioned as described previously. Under no circumstances should you make the passwords for these accounts the same as the User Profile Name.

Note: The most common security vulnerability, and one that is easily avoided, is setting or leaving an insecure password on a default profile.

Enforce Password Management

Your IBM i security guide explains password rules you are able to configure on your IBM i system. Apply basic password management rules, such as password length, reuse, and complexity, to all user passwords.

Limit User Authorities

Typical users should not have powerful authorities such as *SECADMIN, *ALLOBJ, or Command Entry (the Limit Capabilities attribute on the IBM profile should be Yes). Use the Group Profile feature to simplify security administration and to limit special authorities.

5.4 IBM i Resource Security

Object Ownership

All IBM i objects are assigned an owner when they are created. Typically, objects in the World system are owned by user JDE. The JDE IBM profile should be disabled from signing on.

Library Security

IBM i library security is used to simplify the task of setting up and maintaining security, since all objects in a library may be reserved in a few security records versus having to define security for thousands of objects in the library.

Object Authorities

IBM i object authorities are used to define for an object which operational authorities, such as *READ, *CHANGE, or *USE, are allowed to a user or group of users. Files are important objects to secure because they contain your valuable information assets. Object authority should not be left wide open (allowing *PUBLIC all access) on file objects. Since a JD Edwards World environment has thousands of files, it is more practical to set object authorities at the library level. If an individual file requires more restrictive object authority, then you should move it to a separate data library with more restrictive authority or you should set up object authority specific to that file.

Note: The JD Edwards World files that contain security information should be protected from general update access. These files include:

- F0003 - Action Code Security
- F0003T - Action Code Security Tag
- F0103 - Action Code/Search Type Security
- F00823 - Advanced Menu Security Master
- F0024 - Batch Approval/Post Security
- F0001 - Business Unit Security
- F00FP - Fast Path Security
- F9612 - Function Key Security
- F00168 - Generic Text Security
- F9425 - Report Writer Form Security
- F00042 - User Defined Codes Security
- F8201 - Query Group Security File
- F8202 - World Writer File/Field level Security

Field Authorities

IBM i, beginning with the 6.1 operating system release, provides field level encryption. This protects sensitive information "at rest", meaning that the information is secure when copied to tape or other archival formats. Field level encryption does not secure the information from users on the IBM i who are authorized to access the file object.

Authorization List Security

IBM i authorization lists simplify security administration by allowing you to group objects with similar security requirements. An authorization list is used to secure a group of objects, then it is used to define user or groups of users and the authorities each user or group has to those objects.

Adopted Authority

The IBM i adopted authority feature allows users, when running a particular program, to adopt a higher authority for that specific program run. This in turn allows the security administrator to give users less direct authority to objects and to reduce the overall security risk.

Part III

JD Edwards World Authorization Security

This part contains the following chapters:

- Chapter 6, "Overview to JD Edwards World User Security"
- Chapter 7, "Set Up User and Group Security"
- Chapter 8, "Work with Menu Security"
- Chapter 9, "Set Up Action Code, Fast Path, Generic Text, and Search Type Security"
- Chapter 10, "Work with Business Unit Security"
- Chapter 11, "Work with Function Key Security"
- Chapter 12, "Work with Field Level Masking"
- Chapter 13, "Set Up User Defined Codes Security"
- Chapter 14, "Set Up Batch Approval/Post Security"
- Chapter 15, "Set Up Report Writer Security"
- Chapter 16, "Change User Profile Ownership"
- Chapter 17, "Work With the Security Workbench"
- Chapter 18, "Work with Configuration Master Records"
- Chapter 19, "Security Reporting"

6

Overview to JD Edwards World User Security

This chapter contains these topics:

- Section 6.1, "Objectives,"
- Section 6.2, "About JD Edwards World User Security."

6.1 Objectives

- To understand how to set up security
- To understand how to review user security

6.2 About JD Edwards World User Security

There are many types of security within JD Edwards World software. You can use security features to:

- Set up security by user ID
- Create groups based on similar job requirements
- Restrict users to access certain menus or menu selections
- Determine if users can add, change, or delete
- Secure records in master files by business unit
- Disable certain function keys or selection options
- Disable changes to User Defined Codes
- Restrict Address Book records by search type
- Restrict approval and posting of batches to certain users
- Assign report writer version security globally

Complete the following tasks:

- Set up user and group security
- Work with menu security
- Set up Action Code, Fast Path, Generic Text, and Search Type security
- Work with Business Unit security
- Work with Function Key security
- Set up User Defined Codes security

- Set up Batch Approval / Post security
- Set up Report Writer security
- Change user profile ownership
- Work with the Security Workbench
- Work with configuration master records.

7

Set Up User and Group Security

This chapter contains these topics:

- Section 7.1, "Setting Up User Security,"
- Section 7.2, "Securing Command Entry,"
- Section 7.3, "Setting Up Group Security."

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose Security Officer

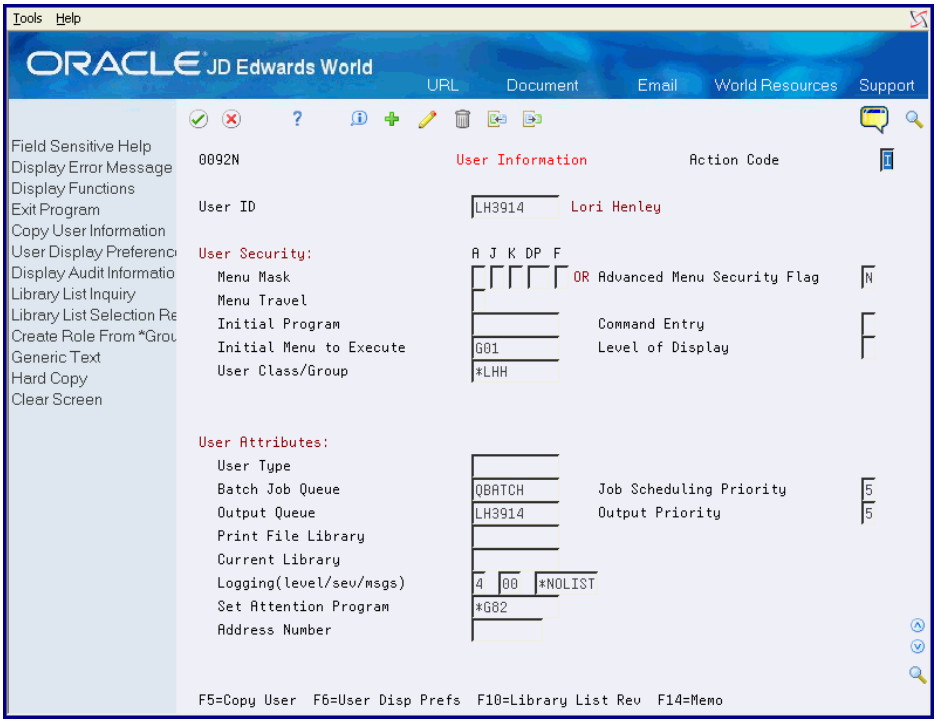
From Security Officer (G9401), choose User Information

7.1 Setting Up User Security

Set up user security to restrict users from certain features. For example, an AP clerk might access an initial custom menu, but cannot use command entry, menu traveling, or fast path. User security offers the following:

- Advanced menu Security OR User keys used in conjunction with menu locks for menu masking
- Initial menu to execute
- Menu traveling
- Command entry
- User class/group

Figure 7–1 User Information screen



See:

- Work with User Profiles in the JD Edwards World Technical Foundation Guide for more information about user profiles.

7.2 Securing Command Entry

Securing command entry on the User Information screen changes your display on JD Edwards World screens. The Command line changes to the Selection line.

Note: This does not secure Command Entry on IBM screens.

To secure Command Entry on IBM screens

1. Use Advanced Menu security or Menu masking to hide Hidden Selection 36 - Command Entry.
2. Set the Allow Command Entry field to 'N' on the User Information screen.
3. Set the Limit capabilities to *YES in the IBM user profile.

Note: When the Limit Capabilities field is set to *YES on the IBM User Profile it overrides a Y setting in the Allow Command Entry field in the User Information program (P0092) on the Security Office menu (G9401). This restricts the use of commands on the Command Line, Group Jobs, and Software Versions Repository (SVR) (F2 in SVR). It is recommended that you review all IBM user profiles that access JD Edwards World software. Set the Limit Capabilities field to *NO or *PARTIAL to allow the user to run commands from these options. If some user's profiles have the Limit Capabilities field set to *YES, then you can set up the system to allow them to execute certain commands by entering CHGCMD on the Command Line. For example, to allow users to execute the CHGOBJ command, enter CHGCMD CHGOBJ on the Command Line and then set the Allow Limit Users (ALWLMTUSR) field to *YES.

7.3 Setting Up Group Security

Group security is the ability to group users so that each individual takes on the characteristics of the group. Create groups based on similar job requirements. The name of the group must begin with an asterisk (*). For example: If the group is *AP assign each Accounts Payable clerk the group *AP.

When you set up groups, certain security features are available that you can place on the group as a whole. You secure each member through the group.

*PUBLIC is considered a group profile. *PUBLIC is not delivered with the system. Add *PUBLIC to activate it. Once added, all users automatically are included.

Roles may also be set up, in order to allow users access to security defined for multiple groups. Roles may comprise users and/or groups.

See Also:

- Work with Roles in the JD Edwards World Technical Foundation Guide for more information about roles.

To set up group security

1. On User Information, add a group user profile with the following:
   - User class/group field must be blank
   - Name of group must begin with *

     The system does not require a corresponding IBM profile.
2. Add the group profile name to the User Class/Group field for each user ID in the group.

8

Work with Menu Security

This chapter contains these topics:

- Section 8.1, "Understanding Advanced Menu Security,"
- Section 8.2, "Menu Masking Security,"
- Section 8.3, "What are the Types of Comparisons in Menu Masking?"
- Section 8.4, "An Example of Menu Masking,"
- Section 8.5, "Using Group Profile or *PUBLIC with Menu Masking,"
- Section 8.6, "Verifying Menu Security Setup,"
- Section 8.7, "Securing Hidden Selections,"
- Section 8.8, "Considerations for Menu Masking."

8.1 Understanding Advanced Menu Security

Beginning with JD Edwards World release A9.3, a new type of menu security called advanced menu security is available. Advanced menu security allows the security administrator to define access to individual users, groups, and *PUBLIC profiles for all menus or for system codes, individual menus, and menu selections. Advanced menu security accommodates role-based security. The default access for advanced menu security is “no access.”

> **Note:** To facilitate a gradual transition to advanced menu security, this security mechanism is not in effect for any user until a switch (flag) is set to Y on the user’s JD Edwards user profile. If the switch to enable advanced menu security has not been set for a particular user, the menu masking feature is still in effect.

The advanced menu security utility is available as an alternative to classic menu masking security, to control user access to menus and menu selections. You can activate the advanced menu security utility by user. It is controlled by a flag in the JD Edwards User Profile file (F0092).

Advanced menu security feature allows easy entry and maintenance of advanced menu security records. To use advanced menu security, complete the following steps:

- Set up records in the Advanced Menu Security file (F00823).
- Activate advanced menu security at the user level on the User Information screen (V0092N)

8.1.1 Set Up Advanced Security Records

Navigation

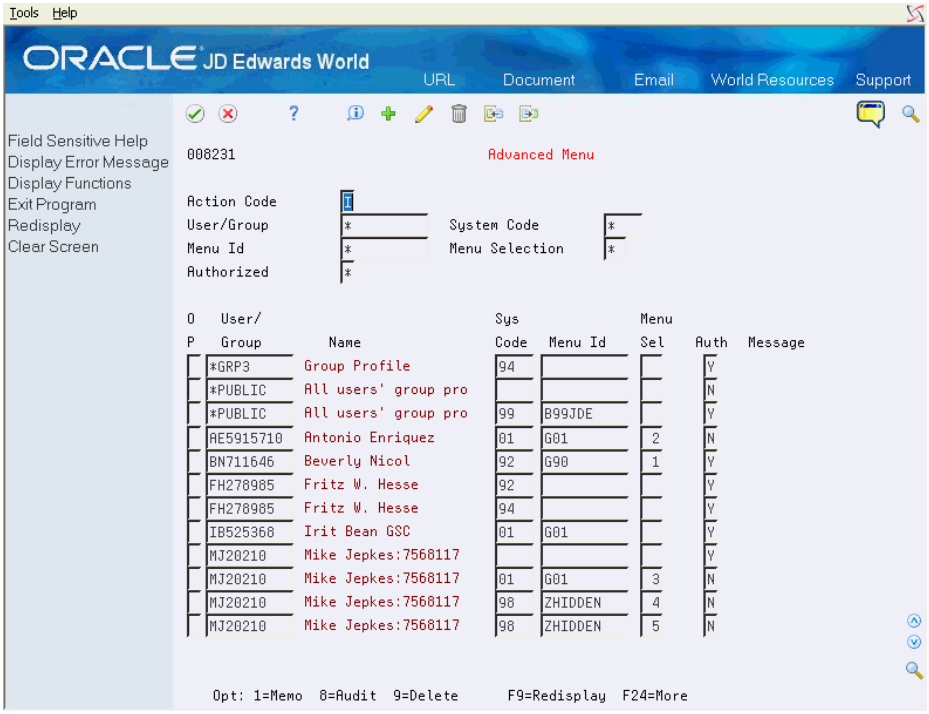
From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose Security Officer

From Security Officer (G9401), choose Advanced Menu.

Figure 8–1 Advanced Menu screen



Field	Explanation
User/Group	Use this field to enter Advanced Menu Security records for a particular user, group, or *PUBLIC. This is the only required field. A record entered without a System Code or Menu ID/Selection will apply to all menus in the system. You may press F1 on the User/Group field to bring up the V0092US - User Search Window. NOTE: Records will appear hierarchically unless the wildcard search is used (see Section 8.1.5, "Wildcard Search" below for specific information).

Field	Explanation
System Code	Use this field to enter the system code the security record applies to. This field is optional. If left blank and a menu ID is specified, the system will default the menu's system code. If system code and menu ID are entered, the menu's system code must match the system code entered. If a menu ID/selection is not specified, this record will apply to all menus in this system code. If a blank is entered for system code, the Menu ID and Menu Selection fields must also be blank. You may press F1 on the System Code field to bring up the V0081Q - User Defined Codes Window. A security record at the system code level will override a security record with blank system code for a user/group. NOTE: Records will appear hierarchically unless the wildcard search is used (see Section 8.1.5, "Wildcard Search" below for specific information).
Menu ID	Use this field to enter the menu ID the record applies to. This field is optional. A security record at the menu level will override one at the system code level. If a blank is entered for menu ID, the Menu Selection field must also be blank. You may press F1 on the Menu ID field to bring up the V0090Q - Index of Menus Window.
Menu Selection	Use this field to enter the menu selection the record applies to. This field is optional. A security record at the menu selection level will override one at the menu level. You may press F1 on the Menu Selection field to bring up the V0090QS Menu Selections Window.
Authorized	Use this field to tell the system if the user, group, or *PUBLIC has access to the system code, menu or menu selection. This data field allows the values of blank, Y or N. Blank: User has access Y: User has access N: User does NOT have access You may limit the subfile display by entering Y or N in the Authorized filtering field. When the Menu level record in the detail is displayed, and there are menu selection level records which override the authorization at the menu level, the message "Mixed" will appear.

Use the fields in the header portion of the screen to search for existing records in the Advanced Menu Security file (F00823). The header fields can be used to filter the subfile inquiry or position the subfile to a specific point. These fields are enabled for use with wildcard search characters. See Section 8.1.5, "Wildcard Search" for further instructions on how to select with these fields.

The system checks the Advanced Menu Security file for a record with the Authorized field set to Y. If a record is found, the user or group or role they are a part of may be authorized for a system code, a menu, or a menu selection. The more detailed records override the more general records.

Advanced menu security accommodates role-based security. In addition to user and group level security, users may be assigned to a security role. When users sign on with a security role, all the groups tied to that security role will be considered when determining authorization to menus.

Note that the default is "No Access," so if a record is not found, authorization is not granted.

The following options are available on the screen:

- Option 1 - Memo: Use this option to enter free-form text with any notes, comments or explanations about the security record. If a memo exists for a record, the selection option field will display in reverse image.
- Option 8 - Audit Information Window: Use this option to retrieve audit information for a security record.
- Option 9 - Delete Line: Use this option to delete a security record.

If you specify a 'D' in the Action Code field to delete all records currently displayed in a subfile, the program will display the V00DWW - Delete Warning Window. When you press F6, the selected records will be deleted.

You may press F9 to display an inquiry again after an update

See Also:

- Work With Import/Export in the *JD Edwards World Technical Tools Guide*.

8.1.2 Activate Advanced Menu Security at the User Level

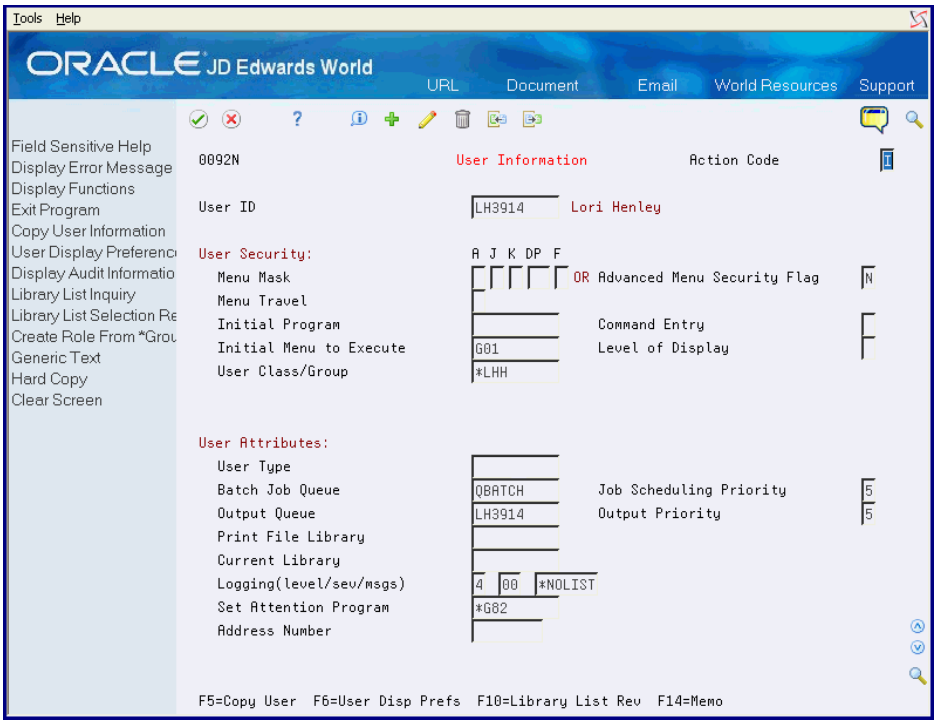
From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose Security Officer

From Security Officer (G9401), choose User Information

Figure 8–2 User Information screen



Field	Explanation
Advanced Menu Security Flag	The Advanced Menu Security flag is used to specify whether the user is using the Advanced Menu Security feature. This data field allows the values of Y or N but not blank. The default value is Y. Blank: User is NOT using Advanced Menu Security Y: User is using Advanced Menu Security N: User is NOT using Advanced Menu Security

Activating advanced menu security for a user overrides any menu masking that was previously set up for the user.

8.1.3 Advanced Menu Security - Functional Details

This section discusses how advanced menu security works in the context of different security setup scenarios:

- No role or group set up: The system checks the Advanced Menu Security file using a hierarchical approach. If the user logs on without selecting a role and is not in a group, the system checks the Menu file in the following order. The system stops checking security records once it finds a record which applies to a specific menu selection, menu or system code, or a record which grants or denies authority to all menus/selections. Authorization is granted or denied to the menu/selection based on the Allow Usage field:

  - Current User, Menu System Code, Menu ID, Menu Selection
  - Current User, Menu System Code, Menu ID
  - Current User, Menu System Code
  - Current User
  - *PUBLIC, Menu System Code, Menu ID, Menu Selection
  - *PUBLIC, Menu System Code, Menu ID
  - *PUBLIC, Menu System Code
  - *PUBLIC

- No role but user belongs to a group: If the user logs on without selecting a role but belongs to a group (specified on the JD Edwards User Profile record in F0092), the system checks the menu file in the following order. The system stops checking once it finds an applicable record and grants access to the Menu ID/Selection based on the Allow Usage field:
  - Current User, Menu System Code, Menu ID, Menu Selection
  - Current User, Menu System Code, Menu ID
  - Current User, Menu System Code
  - Current User
  - Group, Menu System Code, Menu ID, Menu Selection
  - Group, Menu System Code, Menu ID
  - Group, Menu System Code
  - Group
  - *PUBLIC, Menu System Code, Menu ID, Menu Selection
  - *PUBLIC, Menu System Code, Menu ID
  - *PUBLIC, Menu System Code
  - *PUBLIC
- the User signs on with a security role: If the user logs on by selecting a role, the system checks the Menu file as described in the previous section. However, if the role selected has multiple groups attached, the system looks in all groups for a record with the Allow Usage flag set to 'Y'. In other words, if a group is found with the Allow Usage flag set to 'N', the system continues looking in the remaining groups for a record with Allow Usage flag set to 'Y'.

8.1.4 Advanced Menu Security - Examples

The following table (example 1) illustrates the sequence in which the system checks advanced menu security:

User/ Group	System Code	Menu ID	Menu Selection	Allow Usage
ACN001122	00		Advanced Menu Security Flag	Y
ACN001122	00	G00A		N
ACN001122	00	G00A	2	Y
ACN001122	00	G00A	3	Y

User/ Group	System Code	Menu ID	Menu Selection	Allow Usage
ACN001122	00	G00A	4	Y
*GROUP1	00			N
*GROUP1	00	G00A		Y
*GROUP1	43			Y
*PUBLIC				N

In this example user ACN001122 is in group *GROUP1. The system starts by checking for records at the user (ACN001122) level, group level, then *PUBLIC. Records at the user level supersede records at the group level. Records at the group level supersede records at the *PUBLIC level. User ACN001122 Menu access can be described as follows:

- Access allowed to all menus in system code 00 except for Menu G00A
- Access denied to menu G00A except for menu Selections 2, 3, and 4
- Access allowed to all menus in system code 43
- Access denied to remaining menus

The following table (example21) illustrates the sequence in which the system checks advanced menu security:

User/ Group	System Code	Menu ID	Menu Selection	Allow Usage
ACN001122	00			Y
ACN001122	00	G00A		N
ACN001122	00	G00A	2	Y
*GROUP1	00			N
*GROUP1	00	G00A		Y
*GROUP1	43			Y
*GROUP2	00			N
*GROUP2	01	G01		N
*GROUP2	42			Y
*GROUP3	00			N
*GROUP3	01	G01		Y
*GROUP3	43			Y
*PUBLIC				N

In this example, user ACN001122 logs on selecting a role containing groups *GROUP2 and *GROUP3. The system reads through all group records searching for a record allowing access to the menu. For example, *GROUP2 restricts access to menu G01, but *GROUP3 allows access to menu G01. The record that allows access supersedes the record that denies access. Thus ACN001122 is granted access to G01. User ACN001122 menu access can be describes as follows:

- Access allowed to all menus in system code 00 except for menu G00A
- Access denied to menu G00A except for menu selection 2

- Access allowed to menu G01
- Access allowed system code 42 and 43
- Access denied to remaining menus

8.1.5 Wildcard Search

Wildcard search characters can substitute for one or more characters when searching for data in the subfile. Use Configuration Master Setup (P00CFG) on menu G944 option 19 to set up wildcard characters.

For more information, see Chapter 18, "Work with Configuration Master Records" in this guide.

Using wildcards in a search tells the system to search for characters relative to their position in the field. Using wildcard characters will result in an exclusive search as opposed to a subfile reposition.

Wildcard search options include:

- * = Default wildcard search character for zero or many characters
- _ = Default wildcard search character for one and only one character
- | = Default escape wildcard search character. Use the escape wildcard search character to override the wildcard search character to the literal character value.

8.1.5.1 Wildcard Search Examples

These examples illustrate wildcard search options and the records they return:

-
- User/Group = A*: This entry will return all users beginning with A.
- Using 'AN' in the User/Group field repositions the User/Group subfile in alphabetical order starting with AN.
- Using 'AN*' in the User/Group field returns only the User/Group subfile values with A in the first position, N in the second position, then any number of characters after that.
- User/Group = *8: This entry returns all users ending with 8.
- User/Group = *88: This entry returns all users ending with 88.
- User/Group = *8*: This entry returns all user records containing an 8 anywhere in the user ID.
- User/Group = T__1: This entry returns all users beginning with T, then any two characters, then 1 (and no characters after that).
- User/Group = I__253*: This entry returns all users beginning with I, then any two characters, then 253, then any number of characters.
- User/Group = _N*: This entry will return all users beginning with any single character, then N, then any number of characters.
- User/Group = |*AN: This entry repositions the subfile to all users greater than *AN.
- User/Group = PO|_ENTRY: This entry repositions the subfile to all users beginning with or greater than PO_ENTRY.

8.2 Menu Masking Security

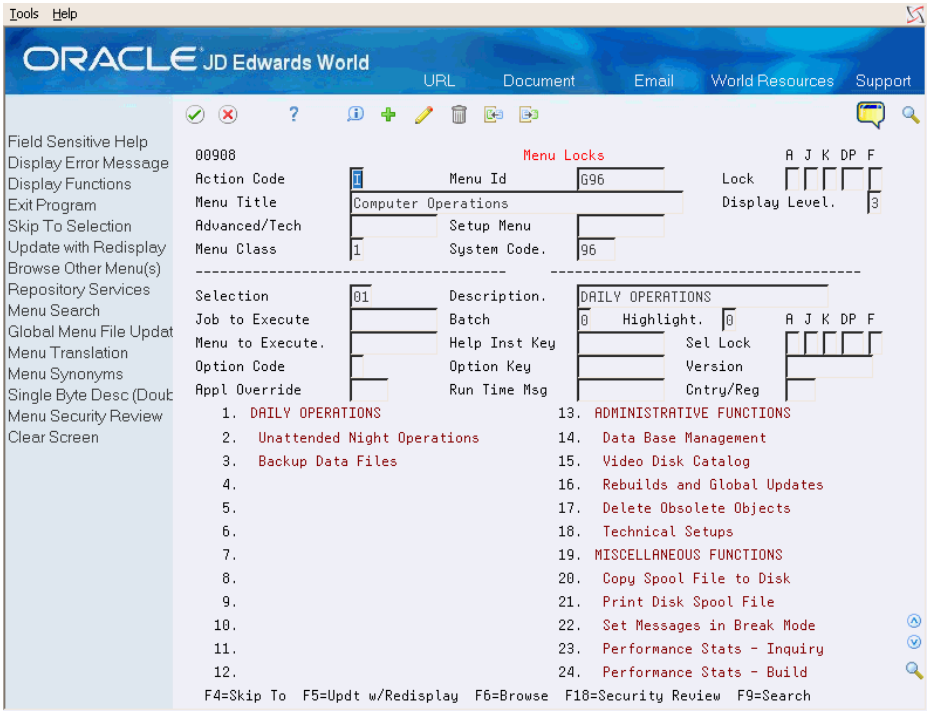
Menu masking is a method of securing entire menus or individual menu selections on a menu by user, group, or *PUBLIC. Menu masking is also used to secure hidden selections. Menu security is determined by the combination of user keys and menu locks based on the following fields:

- A (Authority)
- J (Job)
- K (Knowledge)
- DP (Department)
- F (Future use)

All five fields are active.

Note: Classic Menu Masking Security does not support role-based security

Figure 8–3 Menu Locks screen



The Lock fields secure the entire menu.

The Sel Lock fields secure a specific menu selection.

8.3 What are the Types of Comparisons in Menu Masking?

There are two types of comparison in menu masking, they are:

Comparisons	Description
Direct comparison	This requires an exact match between the J, DP, or F fields both on the menu and in the user profile.
Hierarchical comparison	This applies to the A and K fields. The comparison between the menu and user profile is based on the hierarchy of Blank, A-Z, and 0-9. The system evaluates the Blank being greater than A, which is greater than Z, which is greater than 0, which is greater than 9. 9 has the least authority. ■ Blank in menu locks = no security on that menu or selection ■ Blank in user key = all authority for the user

The system compares each menu lock and user key field beginning with A, then J, K, DP, and F. The comparison must pass all five fields to allow access. If the system finds an instance that disallows access, the system stops the search and locks out the user.

When using fast path, the system checks both the menu and the menu selection for authority.

8.4 An Example of Menu Masking

User/Menu Selection	A	J	K	DP	F
Student (user)	B			AR	
Menu Selection #1	B			AR	(Allowed)
Menu Selection #2	B	A			(Allowed)
Menu Selection #3	C		C		(Allowed)
Menu Selection #4	A				(Disallow)
Menu Selection #5	B			AP	(Disallow)
Menu Selection #6	D			AP	(Disallow)

8.5 Using Group Profile or *PUBLIC with Menu Masking

To use group profile or *PUBLIC with menu masking

1. Add a *PUBLIC profile to the User Information file. Enter user keys for the profile.
2. Place user keys in the appropriate group profile record.
3. Place any user keys in each individual user profile.

   When using individual keys, group profile, or *PUBLIC, the system creates a composite key. This key is a summary of all three user keys. When creating a composite key, the system checks the user keys first, then group, then *PUBLIC for A. Then the system checks all three for J, and so on. As it reads vertically through each key, the first character it reaches becomes the entry for the composite key. In the user, group, *PUBIC scenario, blanks are irrelevant. The system compares the composite key with the menu locks to determine if it will allow access.

Profile	A	J	K	DP	F
User	B				

Profile	A	J	K	DP	F
*JDEGROUP				AR	
*PUBLIC		R	A		
Key Created	B	R	A	AR	

An entry in the User field overrides an entry in the group profile and *PUBLIC. An entry in the group field overrides an entry in the *PUBLIC record.

Profile	A	J	K	DP	F
User	B			PR	
*JDEGROUP		P		AR	
*PUBLIC		R	A		
Key Created	B	P	A	PR	

To maintain blanks as the most authority, use an asterisk in the "key" field. Since the system finds the asterisks first, the asterisks are accepted into the composite key, maintaining the blank. Use an asterisk (*) to override what is in the group profile or in *PUBLIC. Since the DP field is a two-character field, you must use two asterisks (**).

Note: This type of setup can become complicated. If you use this method, create a written plan before implementation.

- Use the *PUBLIC entry as the base.
- Place additional securities needed in group profiles.
- If the user has additional security needs, place entries in the user record.

8.6 Verifying Menu Security Setup

Use any of the following to verify menu security:

- Use the Menu Locks program (P00908) on the Security Advanced and Technical Ops menu (G9431) to determine if the menu contains any locks in the header.
- Use the Menu Locks program (P00908) on the Security Advanced and Technical Ops menu (G9431) to determine if a menu option contains any locks.
- Use the User Information program (P0092) on the Security Officer menu (G9401) to determine if the user profile contains any user keys.
- Use the User Information program (P0092) on the Security Officer menu (G9401) to determine if the user profile contains a group profile. Locate the group profile to determine if it contains any user keys.
- Use the User Information program (P0092) on the Security Officer menu (G9401) to determine if the *PUBLIC profile contains user keys.
- Determine if there is there more than one menu file (F0082).
- In a particular environment, determine if there is there more than one user profile file (F0092).

- Use the User Information program (P0092) on the Security Officer menu (G9401) to determine if the Allow Menu Traveling field is set to Y.

8.7 Securing Hidden Selections

Hidden selections are secured in the same way as menu selections. The Hidden Selection menus are ZHIDDEN, ZHIDDEN002, and ZHIDDEN003.

Hidden selections 27 and 29 allow you to access the Advanced & Technical and Setup Operations menus.

The Hidden Selection Masks screen does not display selections that the user cannot access. You cannot secure the ZHIDDEN menus in their entirety, only the selections.

8.7.1 Securing Hidden Selection 60 (HS60)

HS 60 allows a user to send a message that displays in the Send Window Message on the recipient's screen, to which they either reply or press F3 to exit. HS 60 is also referred to as a break message. HS 60 uses the IBM command SNDMSG.

Following are two different methods to restrict the use of HS 60 and the IBM command SNDMSG. You can:

- Set up the authority you require for the IBM SNDMSG command using GRTOBJAUT.
- Use menu security on ZHIDDEN003 to prevent the use of this selection by those without the correct menu privileges. Alternatively, you can delete the menu entry for HS 60.

8.7.2 Preventing Users from Receiving a Send Window Message

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose System Administration

From System Administration (G944), choose Pre-open Files Setup

You can set up the system to prevent users from receiving a Send Window Message. Users continue to receive messages, but must access their message queue using HS 34 or the IBM command DSPMSG

Before You Begin

Determine whether the user is part of a specific user type by accessing the User Information Revisions program (P0092N) on the Security Officer menu (G9401).

To prevent a user from receiving a Send Window Message

1. On Pre-open Files Setup, if the user is part of a specific User Type, locate that User Type.
2. If the User Type contains the J96SMSGQ or J96SETMSGQ files, delete those files.
3. Locate the *SYS User Type.
4. If the User Type contains the J96SMSGQ or J96SETMSGQ files, delete those files.

8.7.3 Securing Hidden Selection 33 (HS33)

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose run Time Setup

From Run Time Setup (G90), choose Menus Officer

From Menus (G901), choose Revisions

Hidden selection 33 allows a user to access the Work with Submitted Jobs screen and uses the IBM command WRKSBMJOB. On the Work with Submitted Jobs screen, a user can enter the CHGJOB command to move jobs to a different queue or change priorities. You can have the WrkSbmJob Window (V00WSJ) screen display instead of the WRKSBMJOB screen when you use the HS33 command. This allows you to enable Function Keys/Options security.

Before You Begin

Ensure objects J00WSJ, P00WSJ, V00WSJ, and X00WSJ are in your JD Edwards World object library.

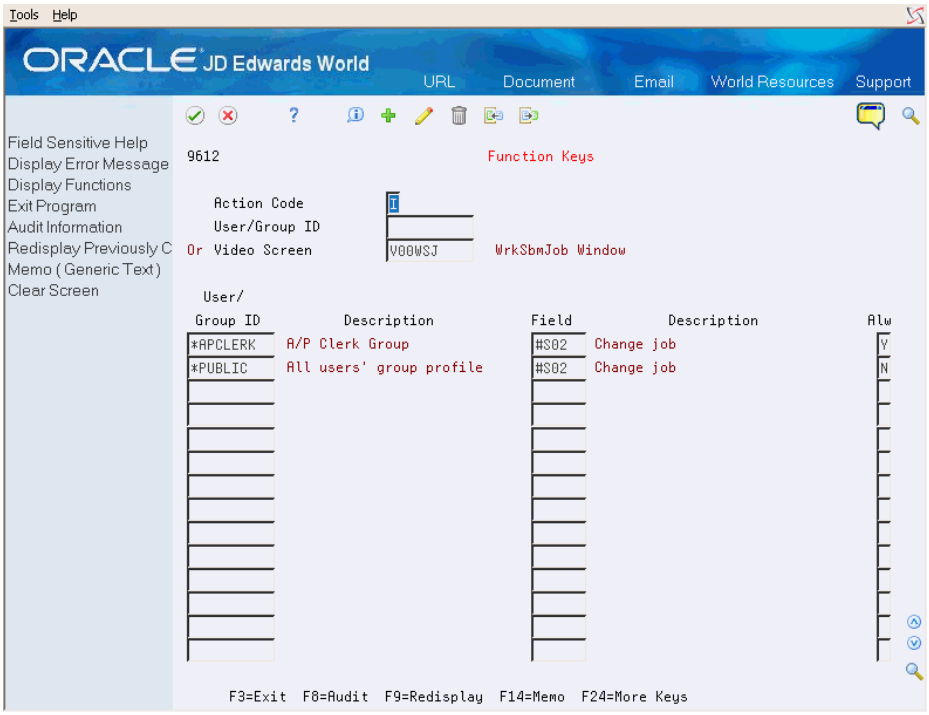
To secure the use of HS 33

1. On Revisions, locate the ZHIDDEN menu ID with SELECT 33 (-Sel 33).
2. Enter J00WSJ in the following field:
   - Option Key
3. Sign out of the environment and sign in.

   HS33 presents the WRKSBMJOB information on V00WSJ.
4. From the Security Officer menu (G9401), choose Function Keys.
5. On Function Keys, locate screen WrkSbmJob Window (V00WSJ) and set up security for the screen per your company requirements.

   In the following example, no users can change jobs except Joe User.

Figure 8–4 Function Keys screen



8.8 Considerations for Menu Masking

- Use menu illustrations as a worksheet.
- Use F8 word search or F18 security review to see menus that have a particular job or menu as a selection.
- Start with one or two fields.
- For users that have very limited access, create your own menu, make your menu the "Initial Menu to Execute" and set Allow Menu Traveling and Allow Fast Path fields to N in User Information.
- Restrict access to User Information, Menu Information and Command Entry.
  - Allow one user to have access: JD Edwards World Security Officer.
  - Where possible, create group profiles for users with similar job requirements.
- Avoid mixing both letters and numbers, particularly in hierarchical fields. Select either letters or numbers until it becomes necessary to use both. Mixing letters and numbers is very confusing.

9

Set Up Action Code, Fast Path, Generic Text, and Search Type Security

This chapter contains these topics:

- Section 9.1, "Setting Up Action Code Security,"
- Section 9.2, "Setting Up Fast Path Security,"
- Section 9.3, "Setting Up Generic Text Security,"
- Section 9.4, "Setting Up Search Type Security."

9.1 Setting Up Action Code Security

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security and System Admin

From Security Administration (G94), choose Security Officer

From Security Officer (G9401), choose Action Code

Action Code Security (P00031) allows you to secure any program ID or any JD Edwards User ID from performing certain actions on programs that have action codes. A user/group ID can be an individual user ID, a group profile ID, or *PUBLIC. The program ID may be an individual program ID or *ALL.

Interactive programs, whether they have an action code or not, may be secured using the Inquiry Action Code field. An 'N' in the Inquiry Action Code field will prevent a user from any access to an interactive program.

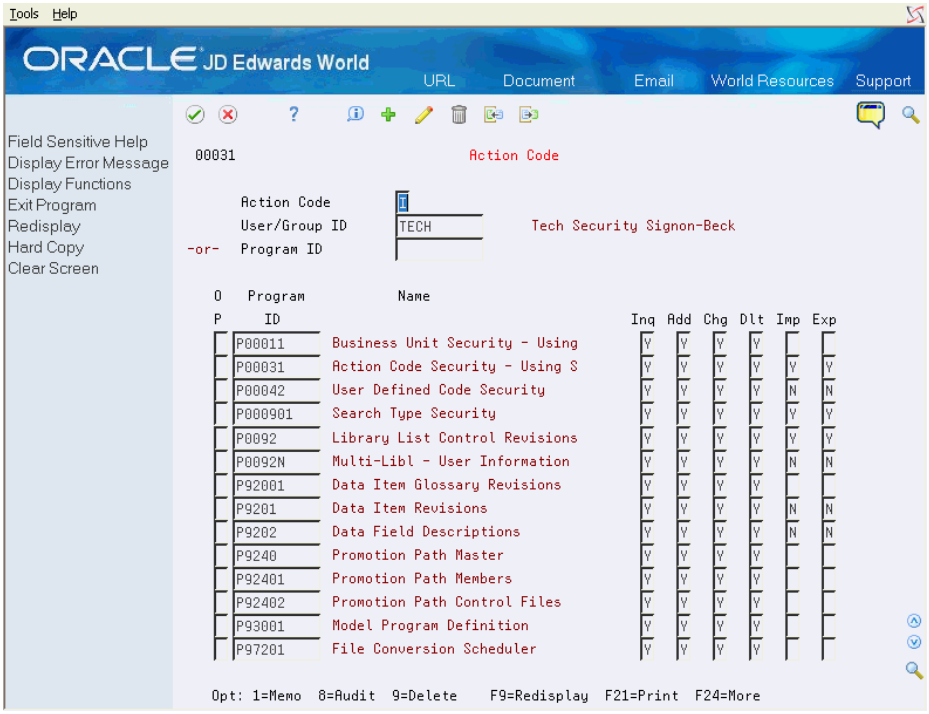
Action code security accommodates role-based security. In addition to user and group level security, Users may be assigned to a security role. When users sign on with a security role, all the groups tied to that security role will be considered when determining authorization to action codes.

Important: The Action Code Security program by default denies access if you have not set up records with the action code types (Inquire, Add, Change, Delete) with the value 'Y'. To allow access to action code security, you must set up records for individual users, groups, or *PUBLIC with the appropriate authorization.

To set up action code security

1. Enter a user ID, group ID, or program ID.
2. Complete the ID field.
3. In the Action Codes fields, enter Y to allow access, or an N to restrict access.

Figure 9–1 Action Code screen



Field	Explanation
User/Group ID	The User/Group ID field is used to enter action code security records for a particular user, group, or *PUBLIC
Program ID	The RPG program name defined in the Software Versions Repository Master file. See also JD Edwards Standards. P SS XXX SS - System number, for example, 01 for Address Book XXX - Specific member ID number
ID	Enter the name of the user, group or program to secure. If a user or group was entered in the top half of the screen, enter a program name to secure for that user or group. If a program name was entered in the top half of the screen, enter a user or group name to secure for that file.
I (Inquire)	This code designates whether an operator has the authority to INQUIRE on records on revision screens that are using action code security. Enter Y or N.
A (Add)	This code designates whether an operator has the authority to ADD records on revision screens that are using Action Code Security. The code is set up in Action Code Security Revisions (F0003). Enter Y or N.

Field	Explanation
C (Change)	This code designates whether an operator has the authority to CHANGE records on revision screens that are using Action Code Security. The code is set up in Action Code Security Revisions (F0003). Enter Y or N.
D (Delete)	This code designates whether an operator has the authority to 'DELETE' records on revision screens that are using Action Code Security. The code is set up in Action Code Security Revisions (F0003). Enter Y or N.
F (Import)	This code designates whether a user has the authority to import data using the PC Import process. Enter Y or N.
T (Export)	This code designates whether a user has the authority to export data using the PC Export process. Enter Y or N.

In the top half of the screen, you may enter either user or group ID or program ID. When you press Enter, the subfile displays all programs associated with a particular user or group profile, or all profiles associated with a particular program.

The following fields are available on the screen:

- Option 1 - Memo: Use this option to enter free-form text with any notes, comments or explanations about the security record. If a memo exists for a record, the selection option field will display in reverse image.
- Option 8 - Audit Information Window: Use this option to retrieve audit information for a security record.
- Option 9 - Delete Line: Use this option to delete a security record. Alternatively, a record can be deleted by blanking out all the fields on the subfile line.

Press F9 to display an inquiry again after an update.

After you set up a 'model' profile, you may use that model to add new profiles. Use the following steps to add profiles based on a model profile:

1. Inquire on the model
2. Roll to the end of the subfile to be sure all records are included.
3. Enter 'A' in the Action Code field, enter the new profile, and press Enter.
4. Inquire on the new profile that you just added to verify the additions.

Use the same approach for programs.

To add new lines to an existing profile or program, inquire first. You may then enter 'C' in the Action Code field and enter new information on either the first available blank space or over an existing profile. If you enter 'C' in the Action Code field and enter information in the first available blank space, the system adds the record. If there is a 'C' in the Action Code field and you type over an existing record, that record's information is changed, including the key.

Use the 'D' action code cautiously. If you enter 'D' in the Action Code field after you have inquired into a profile or program, the system deletes all records in the subfile. To delete just one record in the subfile, enter 'C' in the Action Code field, scroll down and clear the ID in the line that has to be deleted, and press Enter. You can also delete a record by entering 9 in the subfile selection field of the line that has to be deleted.

If you want to restrict a user profile from performing any specific action in all programs, you can use '*ALL' in the program ID for that profile. You cannot secure a CL program. You must use the RPG program, for example, P01051, P00201.

Import and Export capabilities are available on the Action Code Security screen. For more information, see Action Codes for Import/Export in the *JD Edwards World Technical Tools Guide*.

9.1.1 General Guidelines

If a user does not have a role or group, the Action Code Security program checks for security in the following sequence:

1. User Profile ID and Program ID
2. User Profile ID and Program ID = *ALL
3. *PUBLIC and Program ID
4. *PUBLIC and Program ID = *ALL

When the system locates an appropriate record, the application stops checking and uses the authority on the record it has found.

If you want to secure a profile from performing any specific action in all programs, use '*ALL' in the Program ID field for that profile. The system checks the *ALL record after checking for the specific program. This allows for an override to the general rule.

If a user logs on without selecting a role and belongs to a group (specified on the JD Edwards User Profile record in F0092), the system checks the security file in the following order:

1. User Profile ID and Program ID
2. User Profile ID and Program ID = *ALL
3. Group Profile ID (if any) and Program ID
4. Group Profile ID (if any) and Program ID = *ALL
5. *PUBLIC and Program ID
6. *PUBLIC and Program ID = *ALL

When the system locates an appropriate record, the application stops checking and uses the authority on the record it has found.

If you do not use role based security, the system uses the group profile, if any, from the JD Edwards User Profile.

If you use role- based security, a user signed on using a role has access to the authority for multiple groups. In this case, the checks for group profile check all active groups for the role, and if any group has authority, the role is granted authority. When a user is signed on using a role, the user profile's group, if any, is not checked.

Each action code has a Y/N flag which determines whether the user/group or *PUBLIC has authority to that particular action for a program or *ALL.

If you want to secure a profile from any access to an interactive program, enter 'N' in the Inquiry Action Code field. All other fields must be set to 'N'. This completely locks the profile from the program or *ALL.

To determine which programs action code security affects, you can use the Software Versions Repository program (P9801). To locate all programs, you must locate each of the following objects:

- C0001
- C0001A

- C0001T (A91)
- C0001L (ILE)
- C0001TL (ILE)

For each object, use Where Used Cross Reference (F15) and enter / in the Type field and P in the To Display field to display the programs that use action codes.

9.2 Setting Up Fast Path Security

You use the Fast Path program to enter and maintain security records for use with fast path security. Fast path security allows security administrators to grant or deny access to *ALL or individual fast path commands by user, groups and *PUBLIC. Fast path security also accommodates role-based log-ins, giving users who log in using a role access to the fast path commands available for all groups currently attached to that role.

Navigation

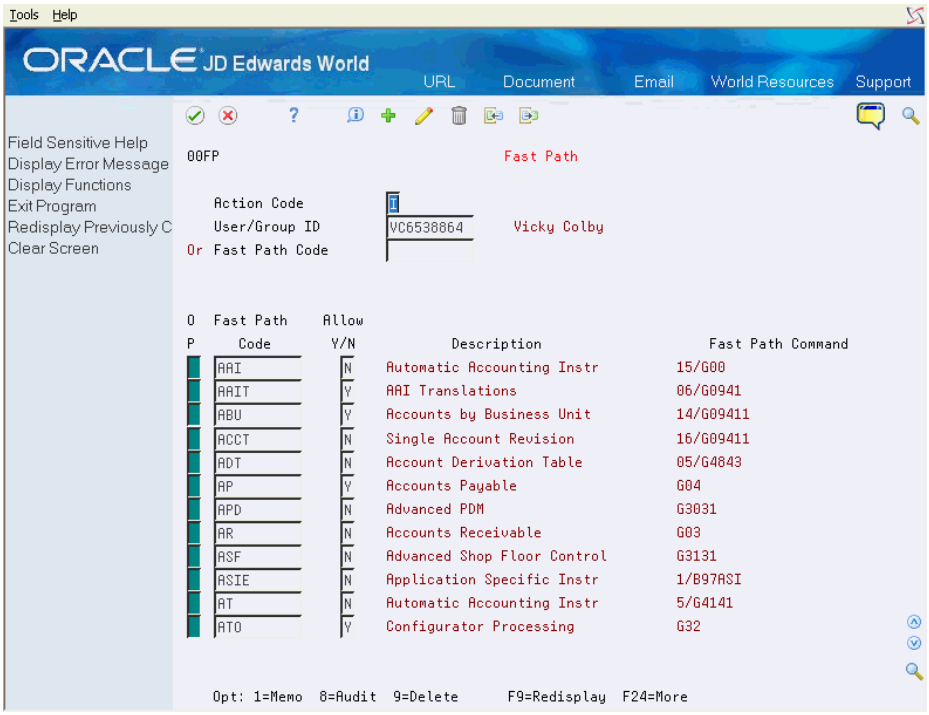
From Security Officer (G9401), choose Fast Path

Use fast path security to set up records for use with fast path authorization. You can set up fast path security at any time.

Note: During your A9.3 upgrade, you executed the Fast Path Conversion program in the Special Application Jobs section. This conversion program created records in the new Fast Path file (F00FP) for all your users, with *ALL fast paths, and either Y=Allow Fast Path or N=Do Not Allow Fast Path, as well as a record for *PUBLIC (if you selected the option to do so). You may add or change existing records using fast path security

The Fast Path Allowed Flag is retained on the JD Edwards user profile record for compatibility with prior World releases. However, as of release A9.3, it is no longer in effect.

Figure 9–2 Fast Path screen



Field	Explanation
User/Group ID (Heading)	Use the User/Group ID field to enter fast path security records for a particular user, group, or for *PUBLIC. When you use this field, you must leave the Fast Path Code field in the header (upper) portion of the screen blank, as the subfile (lower) portion of the screen will display fast path commands.
Fast Path Code (Heading)	Use the Fast Path Code field to enter fast path security records for a particular fast path code or *ALL. When you use this field, you must leave the User/Group ID field in the header (upper) portion of the screen blank, as the subfile (lower) portion of the screen will display user, group or *PUBLIC records.
Fast Path Code (Subfile)	The fast path code is the 'executable' fast path command that a user enters on their session command line. There is a special value, *ALL, to specify Allow Y/N for all fast path commands not specifically defined. This column is displayed when you fill in the User/Group ID field in the header portion of the screen. Only valid fast paths (from UDC 00/FP) and the *ALL value are allowed. Pressing F1 will display the 81QM window, displaying the available fast path codes for selection to be added to subfile.
User/Group ID (Subfile)	User/group ID is the user, group or *PUBLIC that will have Allow Y/N when you fill in the Fast Path Code field in the header portion of the screen. Pressing F1 will display the V0092US window, showing a list of users/groups in the User Information file (F0092).
Allow Y/N	This column is displayed when you fill in the Fast Path Code field in the header portion of the screen. Use the Allow Y/N field to specify whether a fast path command will be allowed or not for the specific combination of fast path or *ALL versus user, group or *PUBLIC.

Field	Explanation
Description	Description is the description of the fast path code, taken from the fast path defined in the 00/FP User Defined Codes file.
Fast Path Command	This column is displayed when you fill in the User/Group ID field in the header portion of the screen. The fast path command is the actual command issued when you enter a fast path code on a command line, taken from the fast path defined in the 00/FP User Defined Codes file. This column is displayed when you fill in the User/Group ID field in the header portion of the screen.
Name	This is the name of a user when you enter a user profile in the subfile (lower) portion of the screen. This column is displayed when you fill in the Fast Path Code field in the header portion of the screen.

The following options are available on the screen:

- Option 1 - Exit to Generic Text: Use this option to enter free-form text with any notes, comments or explanations about the security record. If a memo exists for a record, the selection option field displays in reverse image.
- Option 8 - Audit Information: Use this option to retrieve audit information for a security record.
- Option 9 - Delete User/Fast Path Code: Use this option to delete a security record. Alternatively, a record can be deleted by blanking out both the Fast Path Code or User/Group ID and Allow Y/N fields.

If you specify a 'D' in the Action Code field to delete all records currently displayed in a subfile, the program displays the Delete Warning Window (V00DWW). When you press F6, the selected records are deleted.

It is recommended that you use the Database Audit Manager Tools to set up the Fast Path Security file, F00FP to track details on deleted records.

When the Action Code is 'C' and you type over the fast path code or user/group ID value in the subfile, the record that you typed over is deleted and the new data information will be added to the Fast Path Security file, F00FP.

When the Action Code is 'A' and you type over the fast path code or user/group ID value in the subfile, the new data information is added to file F00FP, but the record data that you typed over are retained. Press F9 to display an inquiry again after an update.

Import and Export capabilities are available on the Fast Path security screen. For more information see Work With Import/Export in the *JD Edwards World Technical Tools Guide*.

9.3 Setting Up Generic Text Security

The Generic Text Security program allows entry and maintenance of security records for use with generic text security. Generic text security allows security administrators to grant or deny users, groups, and *PUBLIC the rights for inquiring on or updating specific generic text applications. Generic text security also accommodates role-based log-ins. When a user chooses a role upon log in, all the groups tied to the specific role will have access to the generic text applications.

When you use generic text security to grant users access to generic text applications, the system checks the Generic Text Security file for a record with access flags for

Inquiry and Update. If a record is found and the requested access flag is set to 'Y', the user has access to the generic text application information.

Important!: The Generic Text security programs automatically lock out all users from accessing all Generic Text Applications. In order to allow access to inquire on and/or update Generic Text Applications, you need to set up records for *PUBLIC, groups, and/or individual users with the appropriate authorization.

Navigation

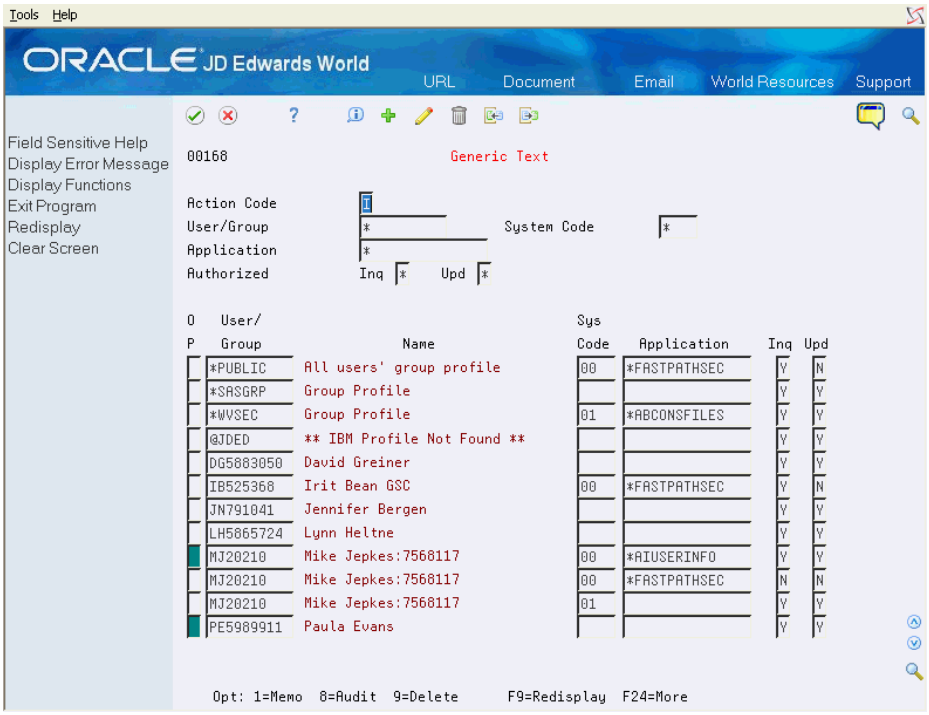
From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security and System Admin

From Security Administration (G94), choose Security Officer

From Security Officer (G9401), choose Generic Text

Figure 9–3 Generic Text screen



Field	Explanation
User/Group	The User/Group field is used to enter generic text security records for a particular user, group, or *PUBLIC. This is the only mandatory field.

Field	Explanation
System Code	The System Code field is used to enter the generic text application system code the security record applies to. This field is optional. You may enter a system code and leave the Application field blank. The security authorization will then apply to all generic text applications with that reporting system code. If you leave the System Code field blank and enter a generic text application, the program will automatically fill in the reporting system code defined in the Generic Text Window Definition File (F00161).
Application	The Application field is used to enter the generic text application this security record applies to. This field is optional. NOTE: A security record entered without a system code or generic text application will apply to all generic text applications. The Inquiry Access Flag field is used to tell the system if the user, group, or *PUBLIC has authority to view messages on the specified generic text application.
Inquiry Access Flag	If you leave the Inquiry Access Flag field blank, the program will automatically fill in 'Y'.
Update Access Flag	The Update Access Flag field is used to tell the system if the user, group, or *PUBLIC has authority to update messages on the specified generic text application. If you leave the Update Access Flag blank, the program will automatically fill in 'Y'.

Use the fields in the header portion of the screen to search for existing records in the Generic Text Security file (F00168). Use the header fields to filter the subfile inquiry or position the subfile to a specific point. These fields are enabled for use with wildcard search characters. See Section 9.3.3, "Wildcard Search" for further instructions on how to use these fields to select records.

The following fields are available on the screen:

- Option 1 - Memo: Use this option to enter free-form text with any notes, comments or explanations about the security record. If a memo exists for a record, the selection option field will display in reverse image.
- Option 8 - Audit Information Window: Use this option to retrieve audit information for a security record.
- Option 9 - Delete Line: Use this option to delete a security record. Alternatively, a record can be deleted by blanking out the User/Group, System Code, Application, Inquiry and Update fields.

If you specify a 'D' in the Action Code field to delete all records currently displayed in a subfile, the program displays the Delete Warning Window (V00DWW). When you press F6, the selected records are deleted.

It is recommended that you use the Database Audit Manager Tools to set up the Generic Text Security file, F00168, to track details on deleted records.

When the Action Code is 'C' and you type over the value in the User/Group field in the subfile, the typed-over record is deleted and the new data information is added to file F00168.

When the Action Code is 'A' and you type over the value in the User/Group field in the subfile, the new data information is added to file F00168, but the typed-over record data is retained. Press F9 to display an inquiry again after an update.

Import and Export capabilities are available on the Generic Text Security screen. For more information see Work With Import/Export in the *JD Edwards World Technical Tools Guide*.

9.3.1 Setup Guidelines

The system checks security using a hierarchical approach, validating the most specific authorities first and moving to more general authorities. The validation stops once a record is found and grants access to the generic text application based on the Inquire and Update access flags.

9.3.1.1 No Role or Group Setup

If users do not have a role or individual group attached to their user ID, the system checks the Generic Text Security file in the following order:

1. Current User, Application System Code, Application
2. Current User, Application System Code
3. Current User
4. *PUBLIC, Application System Code, Application
5. *PUBLIC, Application System Code
6. *PUBLIC

9.3.1.2 No Role Setup, User Belongs to a Group

If users do not have a role attached, but have an individual group attached to their user ID, the system checks the Generic Text Security file in the following order:

1. Current User, Application System Code, Application
2. Current User, Application System Code
3. Current User
4. Group, Application System Code, Application
5. Group, Application System Code
6. Group
7. *PUBLIC, Application System Code, Application
8. *PUBLIC, Application System Code
9. *PUBLIC

In this scenario the group being validated is the group specified in the user's JD Edwards user profile (F0092).

9.3.1.3 User Signs on with a Security Role

If a user logs on selecting a role, the system checks the Generic Text Security file in the following order:

1. Current User, Application System Code, Application
2. Current User, Application System Code
3. Current User
4. Group(s), Application System Code, Application
5. Group(s), Application System Code
6. Group(s)
7. *PUBLIC, Application System Code, Application
8. *PUBLIC, Application System Code
9. *PUBLIC

In this scenario the validation is performed for the group or groups actively associated with the user's log-in role. The authority allowed to any one group is valid for the user's log-in role.

9.3.2 Security Setup Examples

The following examples illustrate security setup scenarios:

9.3.2.1 Example 1

This table illustrates generic text security setup.

User/Group	System Code/Application	Inquiry	Update
ACN001122	00	Y	Y
ACN001122	00 FASTPATHSEC	N	N
ACN001122	01 *ABCONS	Y	Y
ACN001122	01 *ADDNOTE	Y	Y
ACN001122	09 *P0901	Y	N
*GROUP1	00	Y	Y
*GROUP1	00 FASTPATHSEC	Y	Y
*GROUP1	43	Y	Y
*PUBLIC		N	N

In this example, user ACN001122 is in group *GROUP1. The system starts by looking for records at the user (ACN001122) level, group level, then *PUBLIC. Records at the user level supersede records at the group level. Records at the group level supersede records at the *PUBLIC level. User ACN001122 Generic Text Application access can be described as follows:

- Access allowed to all Generic Text applications in system code 00 except for *FASTPATHSEC - Fast Path Security Maintenance
- All access for *ADDNOTE - Additional Address Book Notes in system code 01

- Access denied for all Generic Text applications in system code 01 except *ABCONS and *ADDNOTE
- Access allowed for all Generic Text applications in system code 43.
- Update access denied, but inquiry access is allowed for *P0901 - Accounts by Business Unit in system code 09
- Access denied to the remaining Generic Text applications

9.3.2.2 Example 2

User/Group	System Code/Application	Inquiry	Update
ACN001122	01 *EMAILURL	N	N
ACN001122	04	Y	Y
*GROUP1	00	Y	N
*GROUP1	00 *FASTPATHSEC	Y	Y
*GROUP1	43	N	N
*GROUP2	00 *FASTPATHSEC	N	N
*GROUP2	01	Y	Y
*GROUP2	42	Y	Y
*GROUP3	00 *FASTPATHSEC	Y	Y
*GROUP3	01	Y	N
*GROUP3	43	Y	Y
*PUBLIC		N	N

In this example, user ACN001122 logs on selecting a role containing groups *GROUP2 and *GROUP3. The system reads through all group records searching for a record allowing access to the generic text application. For example, *GROUP2 restricts access to the generic text application *FASTPATHSEC, but *GROUP3 allows full access. The record allowing access supersedes the access denied record, and thus ACN001122 is granted full access to *FASTPATHSEC. User ACN001122 Generic Text Application access can be described as follows:

- Access allowed to all Generic Text applications in system code 04
- All access allowed to all Generic Text applications in system code 01 except *EMAILURL Address - Email / URL
- All access allowed for *FASTPATHSEC in system code 00
- Access denied for all other Generic Text applications in system code 00
- All access allowed for Generic Text applications in system codes 42 and 43
- Access denied to remaining Generic Text applications

9.3.3 Wildcard Search

Wildcard search characters can substitute for one or more characters when searching for data in the subfield. Use Configuration Master Setup (P00CFG) on menu G944 option 19, to set up wildcard characters. For more information, see Chapter 18, "Work with Configuration Master Records" in this guide.

Using wildcards in a search tells the system to search for characters relative to their position in the field. Using wildcard characters will result in an exclusive search as opposed to a subfile reposition.

Wildcard search options include:

- * = default wildcard search character for zero or many characters
- _ = default wildcard search character for one and only one character
- | = default escape wildcard search character. Use the escape wildcard search character to override the wildcard search character to the literal character value.

9.3.3.1 Wildcard Search Examples

These examples illustrates wildcard search options and the records they return:

- User/Group = *A: This entry will return all users beginning with A.
- Using 'AN' subfile in the User/Group field repositions the User/Group in alphabetical order starting with AN.
- Using 'AN*' subfile in the User/Group field returns only the User/Group values with A in the first position, N in the second position, then any number of characters.
- User/Group = *8: This entry will return all users ending with 8.
- User/Group = *88: This entry will return all users ending with 88.
- User/Group = *8*: This entry will return all user records containing an 8 anywhere in the user ID.
- User/Group = T__1: This entry will return all users beginning with T, then any two characters, then 1.
- User/Group = I__253*: This entry will return all users beginning with I, then any two characters, then 253, then any number of characters.
- User/Group = _N*: This entry will return all users beginning with any single character, then N, then any number of characters.
- User/Group = |*AN: This entry will reposition the subfile to all users greater than *AN.
- User/Group = PO|_ENTRY: This entry will reposition the subfile to all users greater than PO_ENTRY.

9.4 Setting Up Search Type Security

Use the Action Code/ Search Type Security program to enforce action code/search type security. If you activate security, then address book or related information associated with particular search types is restricted by search type and action code. You must set up users with appropriate authority to inquire on, add, change or delete records.

Action code/search type security accommodates role-based security. In addition to user and group-level security, you can assign users to a security role. When users sign on with a security role, all the groups tied to that security role are considered when determining authorization to search types.

Important!: If you activate search type security, the default setting for the Search Type Security program is No Access if you have not set up records with action code types (Inquire, Add, Change, Delete) of 'Y'. To allow access to search types, you must set up records for individual users, groups, or *PUBLIC with the appropriate authorization to allow update access.

9.4.1 Activating Search Type Security

Navigation

From Master Directory (G), choose Hidden Selection 27

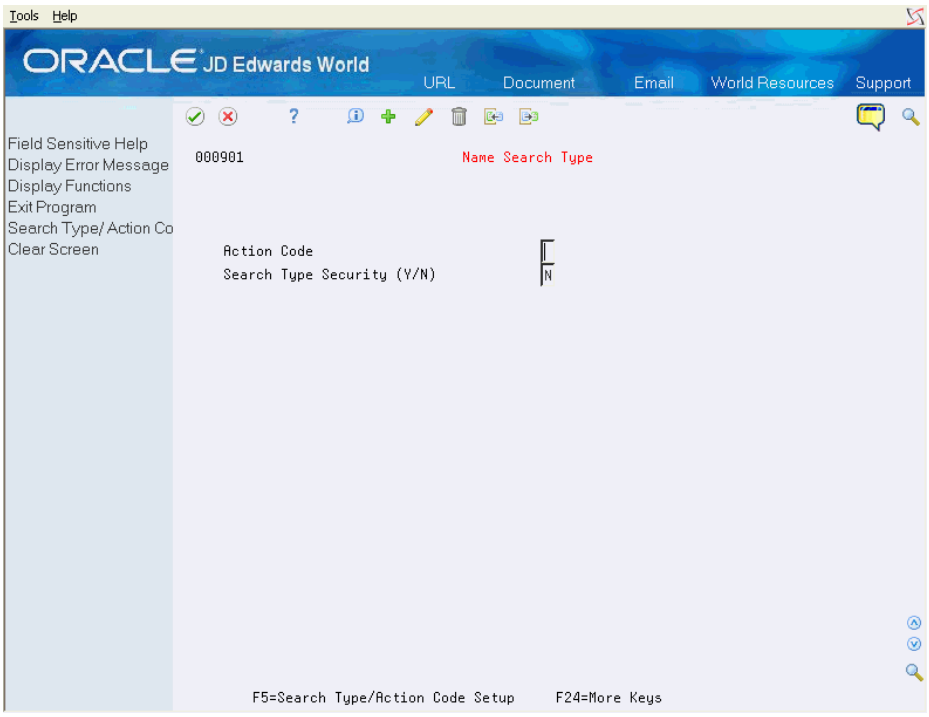
From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose Security Officer

From Security Officer (G9401), choose Name Search Type

Use the Name Search Type video (V000901)to activate or deactivate action code/search type security. Enter a 'Y' here to activate this security in programs that access address book records or information related to search types.

Figure 9–4 Name Search Type screen



From this first screen, you can use function keys to the Action Code/Search Type Security video, where you authorize users or groups of users to specific actions on search types.

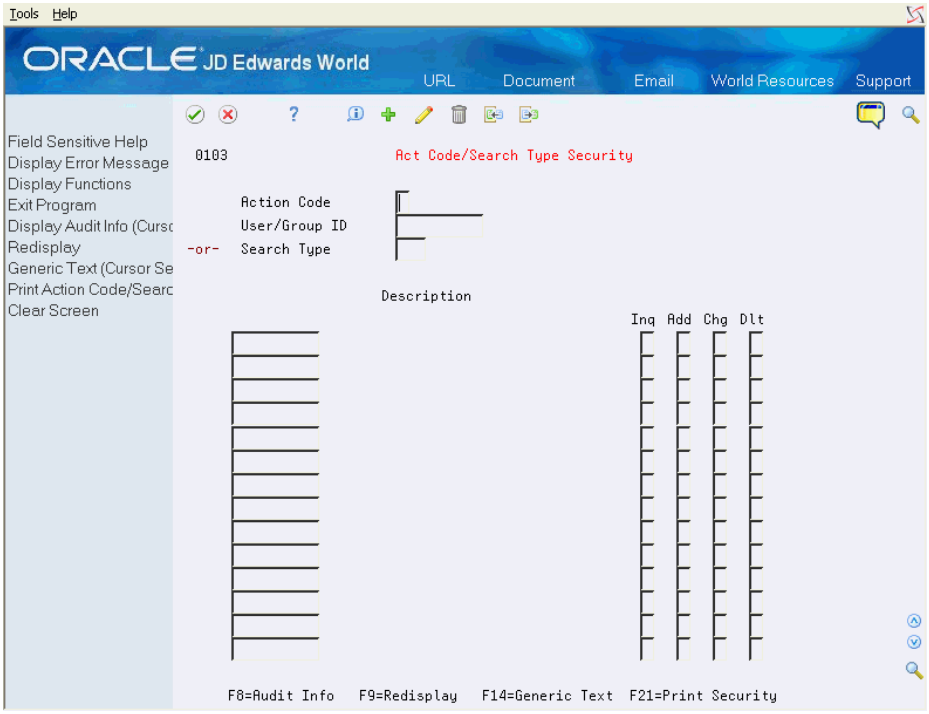
If you activate search type security, you must also set up authority to search types in the Action Code/Search Type Security file to grant access to address book records or other records with information associated with search types. Enter 'Y' in the Search Type Security field to activate search type security. Enter 'N' to deactivate search type security.

Note: Ensure you have set up appropriate authorizations for action code/search type security before activating this security.

To set up action code/search type security

1. From the Name Search Type screen, select Search Type/Action Code Setup (F5).
2. On the Action Code/Search Type Security screen, complete one the following fields:
   - User/Group ID
   - Search Type

Figure 9–5 Action Code/Search Type Security screen



3. Complete the following fields and click Add.
   - User ID # or Search Type
   - Action Code

Field	Explanation
User/Group ID # or Search Type	Enter the name of the user or search type to secure. If you entered a user or group in the top half of the screen, enter a search type to secure for that user. If you entered a search type in the top half of the screen, enter a user or group name to secure for that search type. Note. The system does not display a column label until you inquire and press Enter.
Action Code	Enter 'Y' to allow access, or 'N' to restrict access.

In the top half of the screen, you can enter either user or group ID or search type. When you press Enter, the subfile displays all search types associated with a particular user or group profile, or all profiles associated with a particular search type.

- F14 - Generic Text: Use this option to enter free-form text with any notes, comments or explanations about the security record. If a memo exists for a record, the subfile values in the Search Type column will highlight and See Memo will display above the Search Type column. The cursor must be on a subfile record in order to use this option.
- F8 - Display Audit Info: Use this option to retrieve audit information for a security record. The cursor must be on a subfile record in order to use this option.
- F21 - Print Action Code/Search Type Security: Use this option to print the security records.

Press F9 to display an inquiry again after an update.

If you want to include all users with access to a particular search type, use *PUBLIC to indicate all users. You can also specify group access to search types by entering the group profile name in the User/Group ID field. To allow a user access to all search types, the special value 'Z9' may be used to indicate all search types.

9.4.2 General Guidelines

After you set up a profile, you can use the profile as model to add new profiles. Use the following steps to add profiles based on a model profile:

1. Inquire on the model profile and press Enter.
2. Roll to the end of the subfile to be sure all records are included.
3. Enter 'A' in the Action Code field, enter the new profile, and press Enter.
4. Inquire on the new profile that you just added to verify the additions.

To add new lines to an existing user profile or search type, inquire first. You can then enter 'C' in the Action Code field and enter new information on either the first available blank space or over an existing ID. If you enter 'C' in the Action Code field and enter information in the first available blank space, the system adds the record. Regardless whether you enter a 'C' or an 'A' in the Action Code field, the record is changed if you type over an existing record.

Use the 'D' action code cautiously. If you enter 'D' in the Action Code field after you have inquired into a search type, all security records for this profile or search type is deleted. To delete just one record in the subfile, enter 'C' in the Action Code field, scroll down and clear the search type or user/group ID in the line that has to be deleted, and press Enter.

9.4.3 Check Sequence for Action Type and Search Type Security

If the user logs on with no role and is not part of a group, when checking Action Code/Search Type Security, the application checks for security records in the following order:

1. User Profile ID and Search Type
2. User Profile ID and Search Type = Z9 (all Search Types)
3. *PUBLIC and Search Type
4. *PUBLIC and Search Type = Z9

If the user logs on without selecting a role and belongs to a group (specified on the JD Edwards User Profile record in the F0092 file), the system checks the security file in the following order:

1. User Profile ID and Search Type
2. User Profile ID and Search Type = Z9 (all search types)
3. Group Profile ID (if any) and Search Type
4. Group Profile ID (if any) and Search Type = Z9
5. *PUBLIC and Search Type
6. *PUBLIC and Search Type = Z9

In either scenario described, the application stops checking after encountering an appropriate record and uses the authority on the record it has found.

If you are not using role-based security, the system uses the group profile, if any, from the JD Edwards User Profile.

If you are using role-based security, users who sign on using a role may have access to the authority for multiple groups. In this case, the system checks all active groups for the role. If any group has authority, the role is granted authority. When a user signs on using a role, the system does not check the user profile's group, if any.

9.4.3.1 Examples

The following examples illustrate how the system checks security records.

In the first example, JANEDOE is restricted from other search types at the individual user level. Restrictions might also have been define at the group or *PUBLIC level.

User ID	Search Type	Inquire	Add	Change	Delete
JANEDOE	C	Y	N	N	N
JANEDOE	Z9	N	N	N	N

In the second example, group '*ABENTRY' may add and update customer and supplier search types but may only delete suppliers. Users belonging to group *ABENTRY may inquire on all other search types. Users belonging to group *ABENTRY are allowed inquiry access to all search types. Users belonging to other groups or to no group do not have access to any search types.

User ID	Search Type	Inquire	Add	Change	Delete
*ABENTRY	C	Y	Y	Y	N
*ABENTRY	S	Y	Y	Y	Y
*ABENTRY	Z9	Y	N	N	N

In the third example, user "BOBJONES" is associated with role ACCOUNTING. This role is associated with groups *AP, *AR and *GL. BOBJONES has authority to inquire, add, change and delete customer, supplier, facilities and jobs search types.

User ID	Search Type	Inquire	Add	Change	Delete
*AP	S	Y	Y	Y	Y
*AR	C	Y	Y	Y	Y

User ID	Search Type	Inquire	Add	Change	Delete
*AR	Z9	N	N	N	N
*GL	F	Y	Y	Y	Y
*GL	J	Y	Y	Y	Y
*PUBLIC	Z9	Y	N	N	N

Since BOBJONES belongs to role ACCOUNTING, he has access to the authority from any group associated with the role. Note that group *AR has access to the customer search type only, while others have access to inquiry on all search types based on the *PUBLIC entry.

It is important to exercise caution when setting up records using global authorities such as groups, *PUBLIC, and 'Z9', and to understand the search hierarchy. Otherwise, you may allow or deny access to users that you did not intend.

10

Work with Business Unit Security

This chapter contains these topics:

- Section 10.1, "About Business Unit Security,"
- Section 10.2, "Considerations for Business Unit Security,"
- Section 10.3, "Checking Business Unit Security,"
- Section 10.4, "Technical Considerations for Business Unit Security."

10.1 About Business Unit Security

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose Security Officer

From Security Officer (G9401), choose Business Unit

Business Unit Security Revisions (P00011) allows you to set up or change business unit security for an individual user ID, a group profile ID, or *PUBLIC. Business unit security information is stored in the Business Unit Security file (F0001).

Business unit security allows you to secure a portion of the records in a file based on the business unit. Typically, business units are used to define locations, divisions, and other natural boundaries of management authority. Using business unit security, you may restrict users or groups of users from entering into areas outside of their responsibility.

Business unit security accommodates role-based security. In addition to user and group level security, users may be assigned to a security role. When users sign on with a security role, all the groups tied to that security role will be considered when determining authorization to business units.

Important: The Business Unit Security program by default denies access if you have not set up records To allow access to business unit security, you must set up records for individual users, groups, or *PUBLIC with the appropriate authorization.

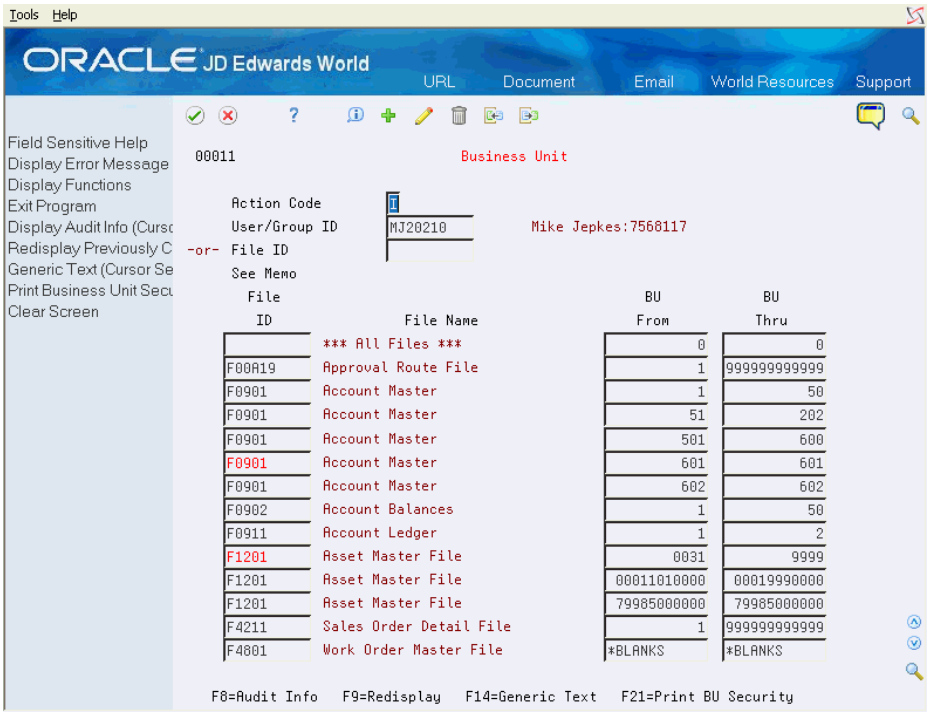
Note that if you do not set up Business Unit security to allow access, then Dream Writers that include a Business Unit coded field will automatically add the Business Unit field to the data selection with no criteria (i.e. MCU < " ") upon execution, and the programs will thus joblog with a message that no records are selected.

10.1.1 Setting up Business Unit Security

To set up business unit security

1. On Business Unit, enter a user ID, group ID or file ID.
2. Specify the range of business units using the Business Unit From and Thru fields.

Figure 10–1 Business Unit screen



Field	Explanation
User ID	The JD Edwards World software defined user profile, group profile, or *PUBLIC. The profile must be set up in the User Information file (F0092).

Field	Explanation
File ID	The member name of the file. All file names begin with F. If you are working with files in the subfile portion of the video (User/Group is filled in the header), you may leave the File ID field blank on a subfile line and fill in a business unit range. This will indicate a range which is valid for all files. You may specify business unit ranges for all files, and override with business unit ranges for specific files.
ID	Enter the name of the user or file that needs updating. If you enter a user in the top half of the screen, enter a file name to be updated for that user. If you enter a file name in the top half of the screen, enter a user name to be updated for that file.
Name	The description of the member appearing in the ID field.
Business Unit From	The lowest value of the range a given user is authorized to view and process data. It is used in conjunction with the Business Unit Through Code which defines the highest value. The business unit entered in the range does not have to be an actual business unit.
Business Unit Thru	The highest value of the range a given user is authorized to view and process data. It is used in conjunction with the Business Unit From code which defines the lower range. The business unit entered in the range does not have to be an actual business unit.

In the top half of the screen, you may enter either User/Group ID or File ID. Upon pressing enter, the subfile will display all files associated with a particular user/group ID, or all users and groups associated with a particular file ID.

To add new lines to an existing user or group ID or file ID, inquire first. You can then place an 'A' in the Action Code field and enter new information on either the first available blank space or over an existing ID. If you enter a 'C' in the Action Code field and enter information in the first available blank space, the record is added. If there is a 'C' in the Action Code field and you type over an existing record, that record's information is changed (including the key).

Use the 'D' action code cautiously. If you enter 'D' in the Action Code field after you have inquired on a user or file ID, all records in the subfile are deleted. To delete just one record in the subfile, place a 'C' in the Action Code field, scroll down and clear the User ID, Business Unit From and Business Unit To fields in the line that has to be deleted, and press Enter.

The following function keys are available on the screen - note that your cursor must be on a subfile record in order to use these options:

- F14 - Memo: Use this option to enter free-form text with any notes, comments or explanations about the security record. If a memo exists for a record, the subfile values in the User/Group ID or Video Screen column are highlighted and the text 'See Memo' displays above the column.
- F8 - Audit Information: Use this option to retrieve audit information for a security record.

Press F9 to display an inquiry again after an update.

10.2 Considerations for Business Unit Security

This section discusses important consideration for implementing business unit security.

10.2.1 Files Secured Using Business Unit Security

Business unit security is based on a business unit Data Dictionary item such as MCU. Business unit data items are identified by COSTCTRSEC in the Data Item Class field in the Data Dictionary file. The security is based on the first business unit data item found in the file. If no business unit data item resides in the file, business unit security is be in effect for that file.

10.2.2 Alphanumeric and Numeric Characters for Business Unit Setup

This sections discusses considerations for setting up business units.

10.2.2.1 Alphanumeric Business Unit Definition

An Alphanumeric business unit is a business unit name that contains at least one non-numeric character in the business unit name. The following table lists examples of alphanumeric business unit setup:

Business Unit	Description	Explanation
DEN	Denver	Every character is a letter
M30	Memphis Mfg. Plant	'M' is not a digit
02D	Denver Corporate Hq	'D' is not a digit
1983A	A Income Statement	'A' is not a digit
200-102	Milling Machine	'-' is not a digit
200.103	Milling Machine	'.' is not a digit

Each business unit name in this table is considered alphanumeric because it contains at least one non-numeric character (not including blank characters).

10.2.2.2 Numeric Business Unit Definition

A numeric business unit is a business unit name that contains only digit characters 0-9 in the business unit name. The following table lists examples of numeric business unit setup:

Business Unit	Description	Explanation
1	A Financial Company	Every character is a digit from 0-9
7	A Model Payroll Company	Every character is a digit from 0-9
07	A Different Payroll	Every character is a digit from 0-9
11	Corporate Office Systems	Every character is a digit from 0-9
4343	Vector Manufacturing Co	Every character is a digit from 0-9
0004344	Venus Universal Supply	Every character is a digit from 0-9
778882002	Valley View Subdivision	Every character is a digit from 0-9

Each business unit name in this table is considered numeric because it contains only numeric characters (not including blank characters). Note that '7' and ' 07' are different numeric business units because it is a character-based data type and not a true number.

10.2.2.3 Planning Business Unit Setup

Most interactive programs (as well as FASTR reporting) differentiate between numeric and alphanumeric business units within the business unit security ranges; SQL-based applications such as World Writer and DREAM Writer-based programs do not. To achieve consistent results with business unit security, it is very important to plan the business units that you create. It is recommended that you define either alphanumeric business units or numeric business units.

Before defining a business unit range, always print a list of Business Units (P0006P) which selects MCU values in the desired BUSINESS UNIT security range and ordered by the MCMCU column. The user running the report must have access to all business units in the F0006 file. This report lists the business units defined in the desired range and displays any discrepancies.

If you already have a mix of alphanumeric and numeric business units set up, you can block out and define specific ranges of business units as either all alpha or all numeric within those business unit definition ranges. You can then run P0006P to validate that the business units that you created follow the guidelines that you have defined. This will assist you in defining business unit security ranges so that both World applications and SQL based reporting will recognize the same business unit range data.

10.2.3 Business Unit Ranges

Business unit security compares business units in the application file to be secured against ranges defined in the Business Unit Security file. There are three types of ranges: numeric, alphanumeric, and *BLANK:

Type of Range	From	Through
Numeric	1	999999999999 (entire numeric range)
Numeric	100	9999 (numeric BUs between 100 and 9999)
Alphanumeric	A	99999999999Z (entire alphanumeric range)
Alphanumeric	AA	Z9 (alphanumeric BUs between AA and Z9)
Blank business unitq	*BLANKS	*BLANKS (only when the business unit is blank

Avoid mixing numeric and alphanumeric business units in the same range, but you can have both numeric ranges and alphanumeric ranges for the same user/group ID and file ID.

The *BLANKS business unit range is used when securing a file for which the business unit is optional, and therefore might be blank on some records.

When you create a business unit security rule in the Business Unit Security program (P00011), you must define a start and end value for each specific rule. Both the start and end values must be of the same type: Either they are both alphanumeric or they are both numeric.

An alphanumeric business unit security range is a rule in P00011 where the start and end MCU values of the ranges are both alphanumeric. An alphanumeric business unit security range authorizes only alphanumeric business units within that range. Any numeric values in the range are not authorized.

Similarly, a numeric business unit security range is a rule in P00011 where the start and end MCU values of the ranges are both numeric. A numeric business unit security range authorize only numeric business units within that range. Any alphanumeric values in the range will not be authorized.

10.3 Checking Business Unit Security

Business unit security is checked in the following order:

1. User Profile ID and File ID
2. User Profile ID and File ID = blank (all files)
3. Group Profile ID (if any) and File ID
4. Group Profile ID (if any) and File ID = blank
5. *PUBLIC and File ID
6. *PUBLIC and File ID = blank

At each check, if at least one business unit range is found, the program grants the user access to the business units that fall into the range or ranges found in the Business Unit Security File.

If you are using role- based security, a user signed on using a role may have access to the authority for multiple groups. In this case, the checks for group profile check all active groups for the role. If any group has authority, the role is granted authority. When a user is signed on using a role, the user profile's group, if any, is not checked. If you are not using role-based security, the system uses the group profile, if any, from the JD Edwards User Profile.

If you do not specify a particular file during setup, the system applies the ranges of business units that you designate by user ID to all secured files. The same applies to group and *PUBLIC records.

Conversely, if you do specify a file, the ranges of business units listed are applied to that particular file only. Please note that the default authorization is 'no access'. If no applicable record for a business unit check is found, the user is not granted access. The system secures anything that is not on their list for that file.

10.4 Technical Considerations for Business Unit Security

Set up business unit security for those master files that are relevant to the system that you want to secure. Since you only gain access to detail files through the master file, there is usually no need to apply business unit security to that level. Business unit security is checked in the following ways:

- In DREAM Writer, business unit security adds additional selection criteria to the OPNQRYF statement.

- In World Writer, business unit security adds additional selection criteria to the SQL SELECT statement.
- In World interactive applications and in FASTR, business unit security is checked using a common security program.

> **Note:** Not all interactive applications are programmed to check business unit security. You should test to be sure business unit security is active for the files you want to secure.

The system performs business unit security for master file, including

- Business Unit Master
- Address Book Master
- General Ledger Account Master
- Payroll Master
- Property & Equipment Master
- Lease Master
- Contract Administration Master
- Item Branch Master
- Sales Order Header
- Purchase Order Header

11

Work with Function Key Security

This chapter contains these topics:

- Section 11.1, "About Function Key Security,"
- Section 11.2, "Working with Function Key Security,"
- Section 11.3, "Standard Function Keys."

11.1 About Function Key Security

Function key security allows you to secure function key and selection options in a particular video or *ALL videos by user, group, or *PUBLIC profiles.

Function key security accommodates role-based security. In addition to user and group level security, users may be assigned to a security role. When users sign on with a security role, all the groups tied to that security role will be considered when determining authorization to function keys and selection options.

> **Important:** The Function Key Security program by default denies access if you have not set up records for function keys and selection options with the Allow Usage flag set to 'Y'. TO allow access to function key security, you mut set up records for individual users, groups, or *PUBLIC with the appropriate authorization.

Secured function keys/options do not display in the Available Functions/Options screen F24 or when you use F1 on the Selection Options column.

Secured function keys still display on Line 24. Use the Vocabulary Overrides program (P9220) to remove them if you have locked all users out of a particular function key.

Use function key security to restrict menu level function keys. Use video V00MENU.

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose Security Officer

From Security Officer (G9401), choose Function Keys

Function Key security allows you to set up security for function keys and/or options by screen or user:

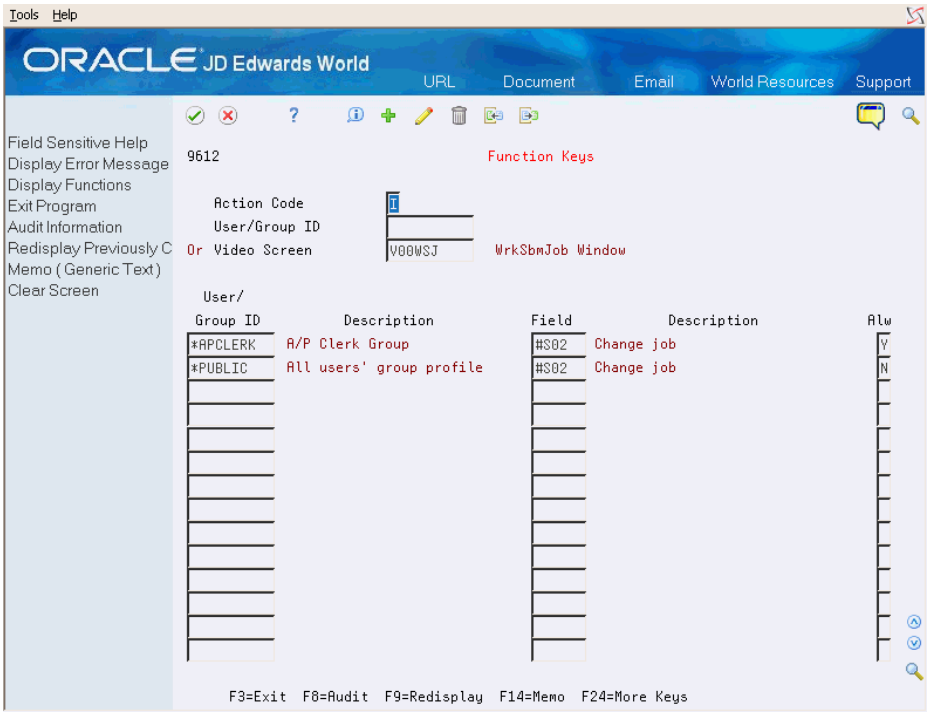
- Secured function keys/options do not display in Available Functions/Options screen F24 or F1.
- Secured function keys still display on Line 24. Use Vocabulary Overrides to remove them.
- Use Function Key security to restrict menu level function keys. Use screen V00MENU.
- Use Data Dictionary item #JDEFNC to modify run-time text on *ALL security.

The function key security file is F9612 and is in the common library.

11.2 Working with Function Key Security

To work with function key security

Figure 11–1 Function Keys screen



Field	Explanation
Video Screen	Screen or report file name (e.g., V01011 or R01402).
User/Group ID	The JD Edwards World software defined user profile.
User/Group ID or Video Screen	Enter the name of the user, group, or video that needs updating. If you enter a user or group in the top half of the screen, enter a video name to be updated for that user or group. If you enter a video name in the top half of the screen, enter a user or group name to be updated for that file.
Description	The description of the selected video screen or user/group ID.

Field	Explanation
Field	The RPG field name of the function key or selection exit. Function keys exits are prefaced with #F, selection keys are prefaced with #S, and the user-defined function keys are prefaced with #G. Output only. NOTE: The Field column is the internal program name for a function key or selection option. It does not relate directly to the external name. For example: in video V01051, field #FEOJ refers to the F3 function key, while field #F03 refers to the F11 function key. To determine what function keys and selection options are available for a particular video, use the F1 key in the Field column. A window will display the function keys and selection options for the video entered. If you enter '*ALL' in the Video Screen field, you may only use values of '*ALL' or '*STD' in the Field column.
Description	The name of the function key or selection exits.
Allow Usag	Use this field to tell the system if the user, group, or *PUBLIC has access to a video's function keys or selection options. Valid codes are: ■ Y Yes, allow access ■ N No, prevent access ■ Blank Yes, allow access (default) If you enter '*STD' in the Field column, you may only use a value of 'Y' in the Allow Usage field.

In the top half of the screen, you may enter either User/Group ID or Video Screen ID. After you press Enter, the subfile displays all videos associated with a particular user or group ID, or all users and groups associated with a particular video.

The following function keys are available on the screen - note that your cursor must be on a subfile record in order to use these options:

- F14 - Memo: Use this option to enter free-form text with any notes, comments or explanations about the security record. If a memo exists for a record, the subfile values in the User/Group ID or Video Screen column will highlight and See Memo displays above that column.
- F8 - Audit Information: Use this option to retrieve audit information for a security record.

Press F9 to display an inquiry again after an update.

11.2.1 General Guidelines

To add new lines to an existing user or video, inquire first. You may then place a 'C' in the Action Code field and enter new information on either the first available blank space or over an existing ID. If you enter 'C' in the Action Code field and enter information in the first available blank space, the system adds the record. Regardless whether you enter a 'C' or an 'A' in the Action Code field, the record is changed if you type over an existing record.

After you set up a 'model' profile, you may use that model to add new profiles. Use the following steps to add profiles based on a model profile:

1. Inquire on the model
2. Roll to the end of the subfile to be sure all records are included.

3. Enter 'A' in the Action Code field, enter the new profile, and press Enter.
4. Inquire on the new profile that you just added to verify the additions.

Use the same approach for videos.

Use the 'D' action code cautiously. If you enter 'D' in the Action Code field after you have inquired into a profile or video screen, all function key security coding for this profile or video is deleted. To delete just one record in the subfile, place a 'C' in the Action Code field, scroll down and clear the video screen or user/group ID in the line that has to be deleted, and press Enter.

11.2.2 Function Code Security - Helpful Hints

When working with function code security, the following considerations apply:

- If you do not use role-based security, the system uses the group profile from the JD Edwards user profile, if a use profile exists.
- The system checks for security records in the following order:
  1. User Profile ID, Video and Field
  2. User Profile ID, Video and Field = *STD (Standard Keys)
  3. User Profile ID, Video and Field = *ALL (All Function Keys)
  4. User Profile ID, Video = *ALL and Field = *ALL
  5. Group Profile ID, Video and Field
  6. Group Profile ID, Video and Field = *STD (Standard Keys)
  7. Group Profile ID, Video and Field = *ALL (All Function Keys)
  8. Group Profile ID, Video = *ALL and Field = *ALL
  9. *PUBLIC, Video and Field
  10. *PUBLIC, Video and Field = *STD (Standard Keys)
  11. *PUBLIC, Video and Field = *ALL (All Function Keys)
  12. *PUBLIC, Video = *ALL and Field = *ALL

When the system locates an appropriate record, the application stops checking and uses the authority on the record it has found. Thus records higher in the order override lower records.

11.3 Standard Function Keys

The standard function keys for a video are F1, F3, F7, F24, Rollup, Rolldown, and Help keys. Standard function keys are made available automatically whenever the user has any other access to the video.

Use of '*STD' in Field allows the user or group to use the standard function keys in the video. You can enter the value 'Y' in the Allow Usage field only if Field = '*STD'.

To lock out a video completely, use '*ALL' in Field with the Allow Usage field set to 'N', with no other security records that grant access to the video. If users try to access the video they are notified of a security violation and are not able to see the video.

1. On Function Keys, enter a screen ID in the Video Screen field, such as V01051 - Address Book Information.

2. Add *PUBLIC or a group profile record with the Field field set to *ALL and the A (allow) field set to N.
3. Add a user record with the Field field set to *STD and the A (allow) field set to Y.

11.3.1 Examples

The following examples illustrate function code security.

11.3.1.1 Example 1

In this example, the user does not belong to a group and is not associated with a security role.The following setup demonstrates the setup for authorization to the standard function keys in video V01051 in addition to function key F6. This setup does not allow access to any other videos:

User/Group	Video	Field	Function Key	Allow Usage
SALLYJONES	V01051	#F14	F6	Y
*PUBLIC	*PUBLIC	*ALL	*ALL	N

The user has access to the standard function keys because they are automatically authorized whenever any other function key or selection option is authorized.

11.3.1.2 Example 2

In this example, the user belongs to GROUPONE, defined onthe user's JD Edwards User Profile. The user does not belong to a security role, so has access to security defined for his user ID or group ID. The following setup demonstrates the setup for authorization to the standard function keys in all videos except V01051, where the is locked out completely:

User/Group	Video	Field	Function Key	Allow Usage
JOHNDOE	V01051	*ALL	All functions	N
GROUPONE	*ALL	*STD	Standard keys	Y
*PUBLIC	*ALL	*ALL	*ALL	N

11.3.1.3 Example 1

ROLEONE is a security role with associated groups GROUPONE, GROUPTWO and GROUPTHREE. The following setup demonstrates the setup for authorization to the standard function keys in video V01051, when signed on under role ROLEONE:

User/Group	Video	Field	Function Key	Allow Usage
GROUPONE	V01051	*ALL	All functions	N
GROUPTWO	V01051	*ALL	All functions	N
GROUPTHREE	V01051	*STD	Standard keys	Y
*PUBLIC	*ALL	*ALL	*ALL	N

The user has access to the standard function keys because they are automatically authorized whenever any other function key or selection option is authorized.

12

Work with Field Level Masking

This chapter contains these topics:

- Section 12.1, "Understanding Field Level Masking,"
- Section 12.2, "Reviewing the Field Level Masking Flow,"
- Section 12.3, "Tasks to Set up Field Level Masking,"
- Section 12.4, "Field Masking Inclusions,"
- Section 12.5, "Setting up Data Item Masking Definitions,"
- Section 12.6, "Setting up Database Field Level Masking,"
- Section 12.7, "Working with Field Level Masking Workbench,"
- Section 12.8, "Setting Field Level Masking,"
- Section 12.9, "Dropping Field Level Masking,"

12.1 Understanding Field Level Masking

You use the Field Level Masking application to mask certain portions or all of the data in a database field within a database file in a specific library.

You can mask all characters in a field/file/library or for a range of characters within the field.

Field Level Masking Application Functionalities

- Oracle JD Edwards World recommends to mask only certain fields and files. These recommended fields are defined within the files for use within the application.
- You can create a masking definition for a recommended field within a database file. You can also create multiple masking definitions for a field (data item), but only one masking definition can be set at any one time for a field with a database file in a specific library combination.
- You can define a masking value to be the replacement character when a masking definition is established and Field Level Masking is applied to a field. The masking value can be any character for an alphanumeric field. The masking value must be zero for a numeric field. Therefore, only a zero value displays in a numeric field that has Field Level Masking set.
- You can apply Field Level Masking at an IBM database field level. This field level mask is applied using an IBM Authorization List. The IBM Authorization List determines the users that have access to view or update the field as opposed to users who cannot view or update the field within a file/library combination.

- You use a workbench to maintain Field Level Masking components as well as set and drop the field for masking.

Caution: If you allow fields to be masked, system performance can be impacted based on the number of fields masked on a file, the number of records in the file, and the number of times the file and field is accessed or updated. For performance purposes, in most cases, place field level masking only on fields in a master file, not in a transaction file.

Navigation

From Master Directory (G), choose Field Level Masking G941 Menu

12.2 Reviewing the Field Level Masking Flow

The following describes the Field Level Masking flow.

Figure 12–1 Field Level Masking flowchart

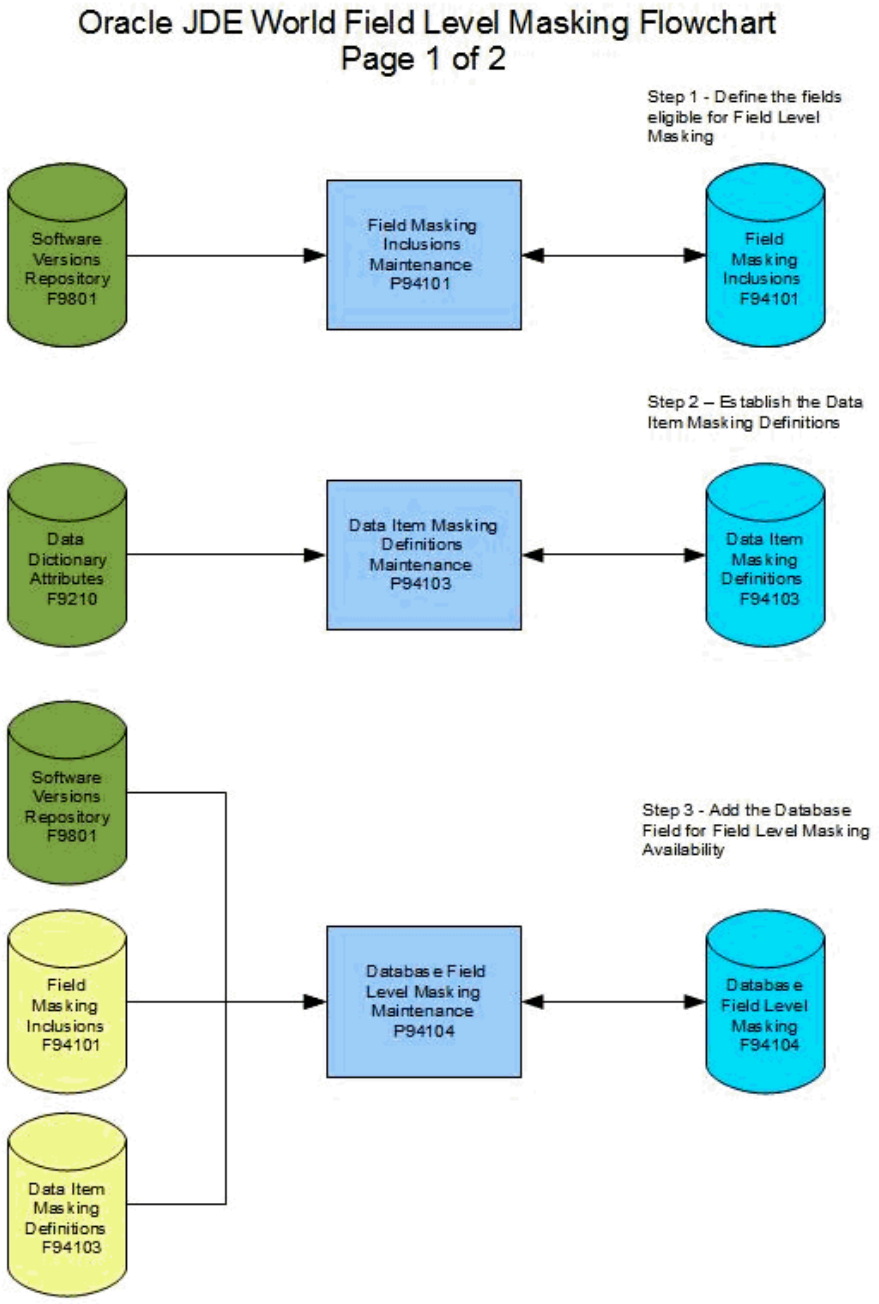
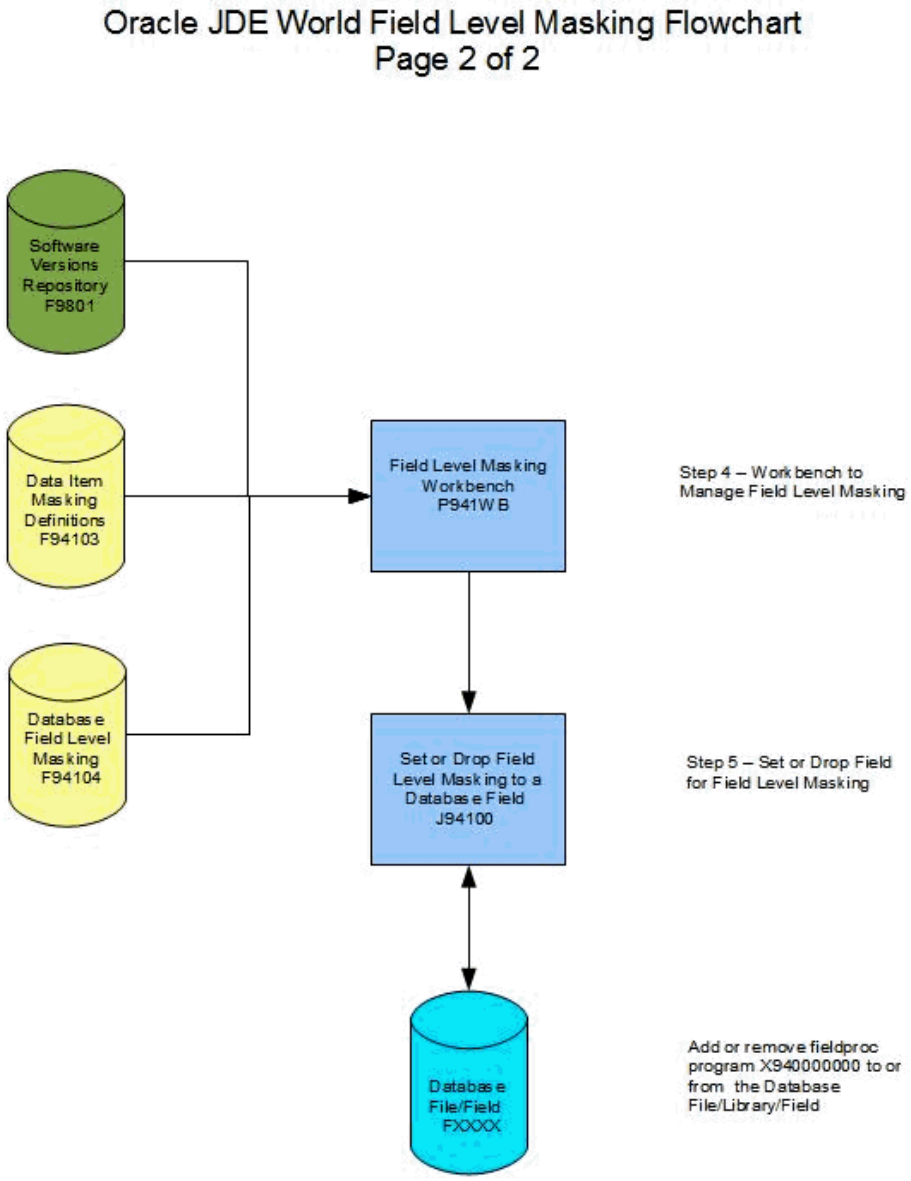


Figure 12–2 Field Level Masking flowchart



12.3 Tasks to Set up Field Level Masking

Setting up Field Level Masking includes the following tasks:

- Determine the files and fields available for field level masking.
- Define the Item Masking.
- Attach the Masking Definition to the database field and file within a library.
- Set or Drop the database field for Field Level Masking.

12.4 Field Masking Inclusions

Navigation

From Field Level Masking (G941), choose Field Masking Inclusions

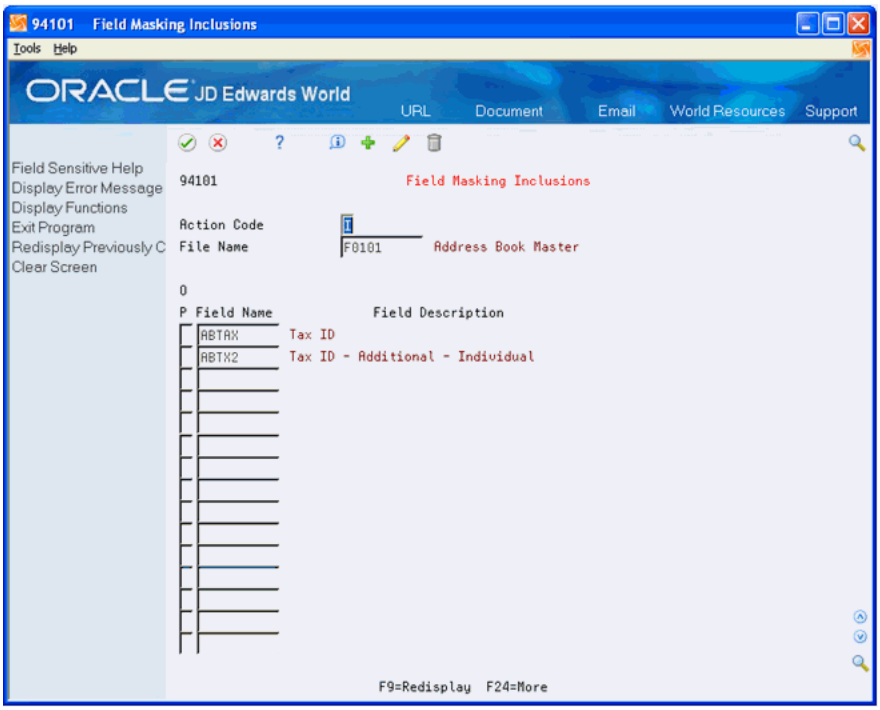
You use the Field Masking Inclusions maintenance program (P94101) to maintain the Field Masking Inclusions file (F94101).

The Field Masking Inclusions file allows only specifically recommended fields by file to be used for Field Level Masking purposes. Oracle JD Edwards World ships the Field Masking Inclusions file (F94101) with these recommended database fields included. Any modifications to the files and fields are made at your own discretion.

If the File/Field combination does not exist in the Field Masking Inclusions file, Field Level Masking cannot be set on that field within the database file through this application.

The Field Masking Inclusions maintenance program and screen are intended to be used only for inquiry purposes to determine which files and potential fields are made available for Field Level Masking.

Figure 12–3 Field Masking Inclusions screen

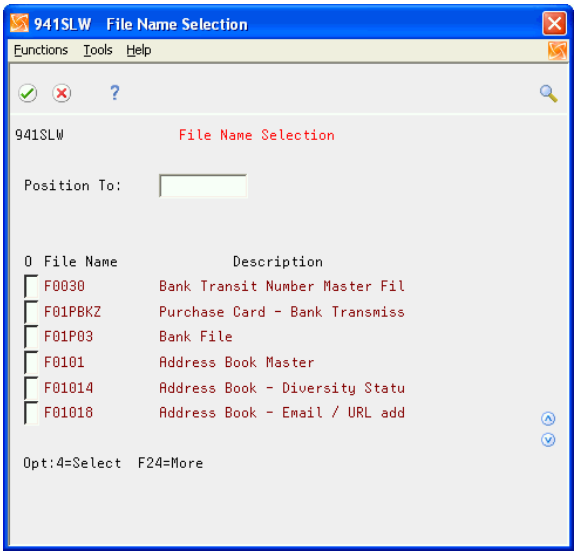


Field	Explanation
File Name	The member name of the file. All file names begin with F.
Field Name	This field contains a value that identifies an exit or action in Extensibility or a database field allowed for use in Field Level Masking. *Screen-Specific Information* In Field Level Masking, the Field Name is used to define the field within a data base file that is to be included and/or enabled in Field Level Masking.
Field Description	The description of the selected video screen or user ID.

12.4.1 File Name Selection Window (P941SLW)

You use the File Name Selection (P941SLW) window for Field Level Masking to display a list of the files and select a file value to be returned to the calling program.

Figure 12–4 File Name Selection window



12.5 Setting up Data Item Masking Definitions

Navigation

From Field level Masking (G941), choose Data Item Masking Definitions

You use the Data Item Masking Definitions program (P94103) to maintain the Data Item Masking Definitions file (F94103). The Data Item Masking Definitions program defines the various potential maskings for a Data Item (field).

The system uses a Masking Code to define different and multiple maskings for each Data Item.

The system uses the Data Item Masking Definition to format the mask of the database field when it is set for Field Level Masking.

The combination of Data Item and Masking Code defines the Data Item mask.

The Masking Value defines the character to be used to mask the Data Item field. The Masking Value character must be a 0 for numeric Data Items (defined as packed or signed fields). There are no restrictions on Masking Values that can be used for alphanumeric Data Item fields.

For alphanumeric Data Items, the Masking Starting and Ending Positions define the range of characters within the Data Item character string to be masked when Field Level Masking is set on the database field.

The Masking Starting and Ending Positions default to the entire field length for numeric Data Items since the Masking Value is 0 and displays accordingly based on the Data Item's Edit Code.

The system displays the Data Item attributes on the screen for information purposes, you can review the Field Size, Display Decimals, Edit Code, and Data Type

Description. Use the Data Item attributes to determine the Non-mask and Mask Display values.

The Non-mask and Mask Display values display the result of the masking definition created for the Data Item. If the Data Item's Field Size is greater than 60 characters, the Non-mask and Mask Display fields will not be displayed.

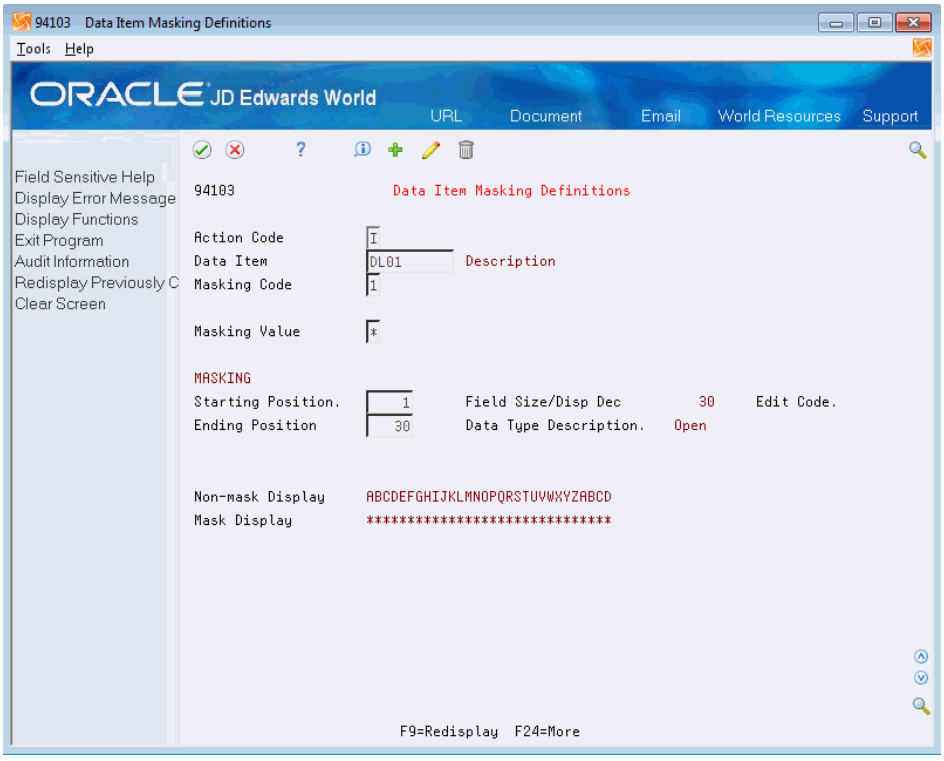
For alphanumeric Data Items, the Non-mask Display field displays using alpha characters A-Z, repeated when necessary. The Mask Display field then displays the Masking Value replacing the characters within the Starting and Ending Position range.

For numeric Data Items, the Non-mask Display field displays using numeric characters 1-9 and 0, repeated when necessary. This field displays commas and decimal points as defined based on the Data Item attribute fields displayed. The Mask Display field displays the zero or not, again based on the Data Item attributes, including the Edit Code.

12.5.1 Examples of Data Item Masking Definitions

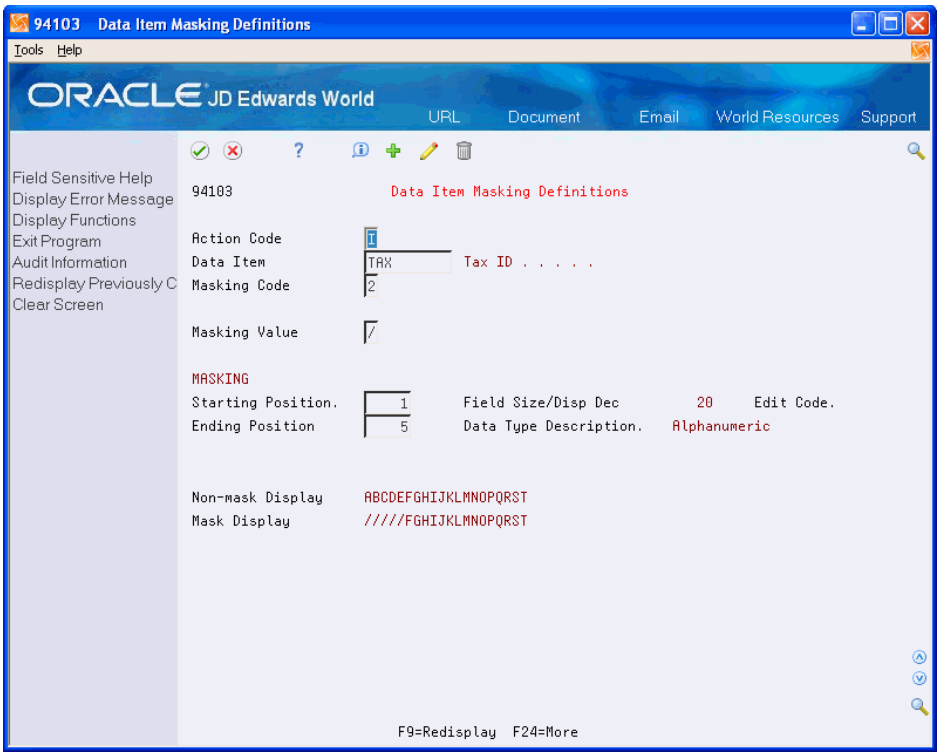
The following screen displays the Description field with all 30 characters masked with a * Masking Code

Figure 12–5 Data Item Masking Definitions screen



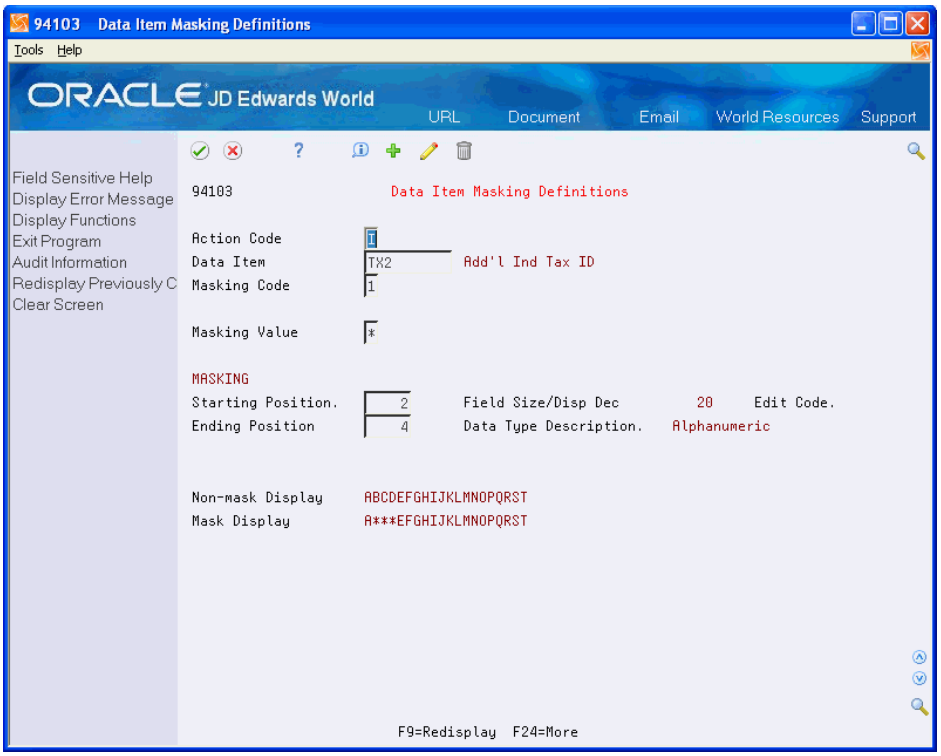
The following screen displays the Tax ID with the first 5 characters masked with a / Masking Code

Figure 12–6 Data Item Masking Definitions screen



The following screen displays the Additional Tax ID field with positions 2-4 masked with a * Masking Code

Figure 12–7 Data Item Masking Definitions screen



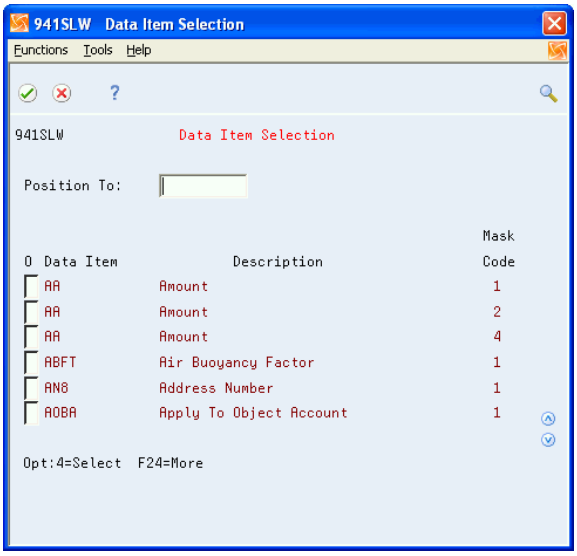
Field	Explanation
Data Item	For World, the RPG data name. This data field has been set up as a 10-byte field for future use. Currently, it is restricted to 4 bytes so that, when preceded by a 2-byte table prefix, the RPG data name will not exceed 6 bytes. Within the Data Dictionary, all data items are referenced by this 4-byte data name. As they are used in database tables, a 2-character prefix is added to create unique data names in each table specification (DDS). If you are adding an error message, this field must be left blank. The system assigns the error message number using next numbers. The name appears on a successful add. You should assign error message numbers greater than 5000. Special characters are not allowed as part of the data item name, with the exception of #, @, $. You can create protected data names by using $xxx and @xxx, where you define xxx. Create new data items using system codes 55-59. The alias cannot be changed.

Field	Explanation
Masking Code	The Masking Code is used in Field Level Masking to identify a Data Dictionary Item that is being masked in a certain defined way. This Masking Code allows multiple ways to mask the Data Dictionary Item at a database file field level. For example, a Tax ID field can be masked to show the last 4 numbers only with an * appearing in the first 5 positions. A second Masking Code might be defined on this field to use a Masking Value of / rather than *. A third Masking Code might identify the Tax ID field to show only the last two numbers with a Masking Value of > in the first 7 positions.
Masking Value	The Masking Value is used in Field Level Masking to mask a database field with the specified character value at the Data Dictionary Item level. For example, a Tax ID field can be masked to show the last 4 numbers only with an * being used as the Masking Value to display in the first 5 characters. Any character can be used for the Masking Value, except for numeric fields which must have a Masking Value of 0.
Starting Position	Within Field Level Masking, the Mask Starting Position identifies the first position within the Data Dictionary Item and database field where the Masking Values will be displayed.
Ending Position	Within Field Level Masking, the Mask Ending Position identifies the last position within the Data Dictionary Item and database field where the Masking Values will be displayed.
Field Size/Disp Dec	The field size of the data item. Note: All amount fields should be entered as 15 bytes, 0 decimals, and the data item type should be P (packed).
Edit Code	Determines how data is printed or displayed. Depending on the code, you can change the appearance of the fields as follows (standard IBM edit codes): ■ Show commas - 1, 2, A, B, J, K, N, or O ■ Show decimal point - 1, 2, 3, 4, A, B, C, D, J, K, L, M, N, O, P, Q ■ Show sign for negative - A, B, C, D ("CR") or J through Q ("-") ■ Suppress leading zeros - 1 through 4, A through D, J through Q, Y, and Z Refer to user defined codes (system 98/type EC) for all valid codes, including additional J.D. Edwards edit codes.
Data Edit Code	Defines the type of data to be stored in the field. The data item types are user defined codes (98/DT). Note: All amount fields should be entered as 15 bytes, 0 decimals, and data item type P<SP>(packed).

12.5.2 Data Item Selection window (P941SLW)

You use the Data Item Selection (P941SLW) window for Field Level Masking to display a list of the data item masking definitions and select a Data Item and Mask Code combination value to be returned to the calling program.

Figure 12–8 Data Item Selection window



12.6 Setting up Database Field Level Masking

Navigation

From Field level Masking (G941), choose Database Field Level Masking

You use the Database Field Level Masking program (P94104) to maintain the Database Field Level Masking file (F94104) and to set up the masking of a field within a file and its library.

If you create a Database Field Level Masking for the file, library, and field combination, the system does not set the field for Field Level Masking at this point. Use the Field Level Masking Workbench to complete the setting and dropping of the field level masking.

The Database Field Level Masking is based on a combination of File Name, Data File Library, and Field Name.

You can set up the Field Level Masking for only a valid field within an existing database file in a library.

> **Note:** Before you create the Database Field Level Masking record, you must verify the edits in the following section.

Verify the following edits before you create the Database Field Level Masking record

1. The File Name and Field Name must exist in the Field Masking Inclusions file (F94101).

2. The Masking Definition (combination of Data Item and Masking Code) entered must exist in the Data Item Masking Definitions file (F94103).
3. The Field Name must be valid within an existing object for the File Name and Data File Library entered.
4. The Authorization List must be a valid IBM Authorization List object (see Appendix C - IBM Authorization Lists – Object Authority Information, for more information on IBM Authorization Lists).
5. The Data Item must match the Field Name disregarding the File Prefix.
6. The user must be authorized to the object (File Name and Data File Library combination).

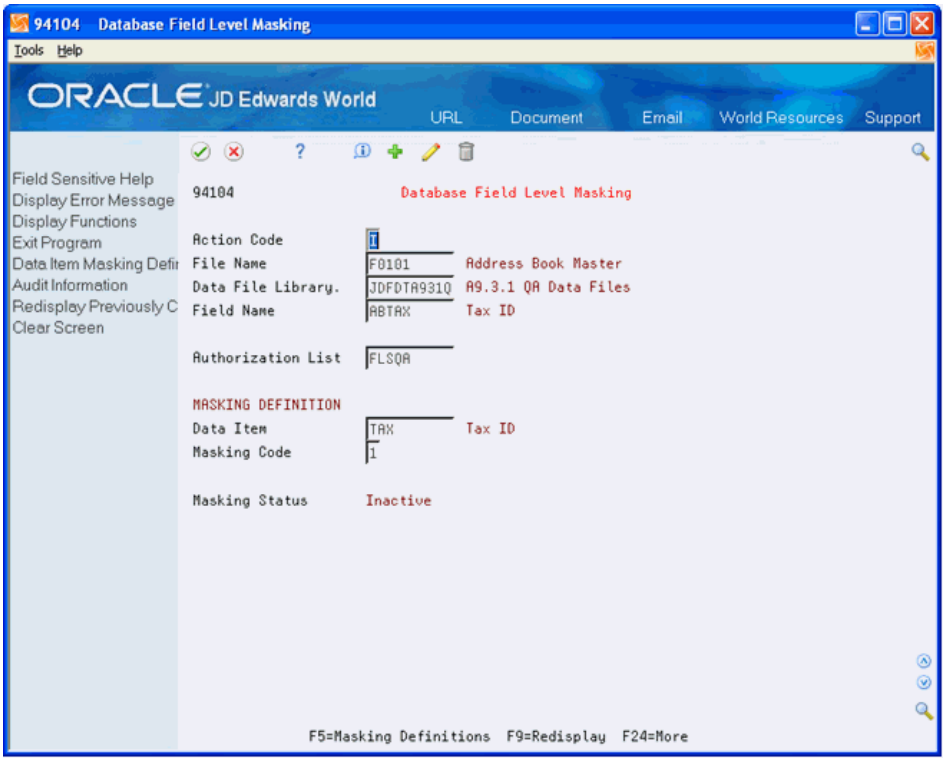
The Masking Definition you entered, defines the Masking Value (character) and the Starting and Ending Positions that display the Masking Values for an alphanumeric database field.

The Masking Definition for a numeric database field always display as either 0 or blanks, based on the Data Item's Edit Code determining whether the zero should display.

If the Field Level Masking is set for the File/Library/Field combination, the Masking Status on the screen displays Active.

If the Field Level Masking has been dropped for the File/Library/Field combination, the Masking Status on the screen displays Inactive.

Figure 12–9 Database Field Level Masking screen



Field	Explanation
File Name	The member name of the file. All file names begin with F.

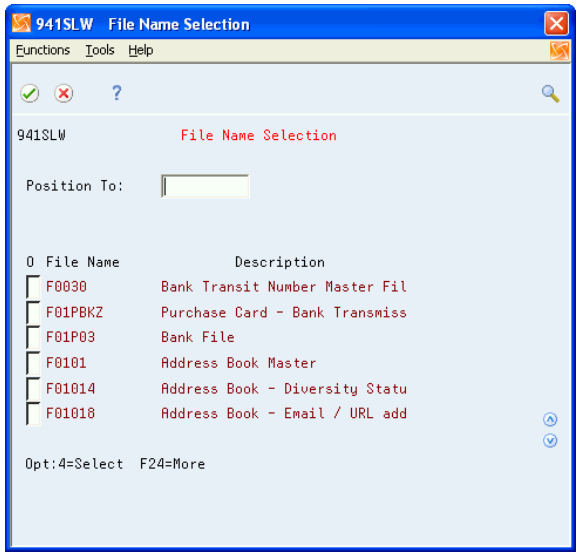
Field	Explanation
Data File Library	The Data File Library Name designates the library location of the data base files.
Field Name	This field contains a value that identifies an exit or action in Extensibility or a database field allowed for use in Field Level Masking. *Screen-Specific Information* In Field Level Masking, the Field Name is used to define the field within a data base file that is to be included and/or enabled in Field Level Masking.
Authorization List	The Authorization List will be used in Field Level Masking for authorizing the database field for viewing or updating purposes to a list of user profiles.
Data Item	For World, the RPG data name. This data field has been set up as a 10-byte field for future use. Currently, it is restricted to 4 bytes so that, when preceded by a 2-byte table prefix, the RPG data name will not exceed 6 bytes. Within the Data Dictionary, all data items are referenced by this 4-byte data name. As they are used in database tables, a 2-character prefix is added to create unique data names in each table specification (DDS). If you are adding an error message, this field must be left blank. The system assigns the error message number using next numbers. The name appears on a successful add. You should assign error message numbers greater than 5000. Special characters are not allowed as part of the data item name, with the exception of #, @, $. You can create protected data names by using $xxx and @xxx, where you define xxx. Create new data items using system codes 55-59. The alias cannot be changed.
Masking Code	The Masking Code is used in Field Level Masking to identify a Data Dictionary Item that is being masked in a certain defined way. This Masking Code allows multiple ways to mask the Data Dictionary Item at a database file field level. For example, a Tax ID field can be masked to show the last 4 numbers only with an * appearing in the first 5 positions. A second Masking Code might be defined on this field to use a Masking Value of / rather than *. A third Masking Code might identify the Tax ID field to show only the last two numbers with a Masking Value of > in the first 7 positions.

Field	Explanation
Masking Status	The Masking Status is used in Field Level Masking to determine whether the data base field in a file and library has been set. The values for Masking Status are: Active - Field Level Masking is set for this field. Inactive - Field Level Masking is not set for this field or it has been dropped.

12.6.1 File Name Selection window (P941SLW)

You use the File Name Selection (P941SLW) window for Field Level Masking to display a list of the files and select a file value to be returned to the calling program.

Figure 12–10 File Name Selection window



12.7 Working with Field Level Masking Workbench

Navigation

From Field level Masking (G941), choose Field Level Masking Workbench

You use the Field Level Masking Workbench program (P98XWB) as a tool to manage the Field Level Masking database fields that are set up within the application. The workbench provides the mechanism to set and drop the database field to and from Field Level Masking.

The workbench is driven by the Database Field Level Masking file (F94104).

All inquiries and filtering are performed to the Database Field Level Masking file (F94104).

The Field Level Masking Workbench program allows several selection options for each database file set up within the Field Level Masking application tool.

Selection options to call the various programs or to perform the processes

- Field Masking Inclusions (calls program P94101).
- Data Item Masking Definitions (calls program P94103).
- Database Field Level Masking (calls program P94104).
- Set Field Level Masking (calls program J94100).
- Drop Field Level Masking (calls program J94100)

The system displays error messages if you attempt to set a database field with an Active Masking Status or if you attempt a Drop for a database field with an Inactive Masking Status (never set or has been dropped).

You can filter selection of the Database Field Level Masking file (F94104) on the following fields:

- File Name
- Library Name
- Field Name
- Authorization List

12.8 Setting Field Level Masking

The Masking Status field displays as Active on the workbench for a database field that has been set with Field Level Masking and masking.

To set a field in a file and library for Field Level Masking based on the Authorization List and the Masking Definition (Data Item and Mask Code) specified, select option 4 (Set) from the Field Level Masking Workbench screen.

When you select option 4 (Set) to set the field, the system completes the following steps:

1. The object (file and library) is checked first for existence and both *OBJMGT and *OBJOPR rights for the user attempting the set. If the object does not exist (IBM error CPF9801) or any other error occurs on the check object command, the system displays error message 941E.
2. The IBM Authorization List is also checked to determine if the user has *READ or *UPD rights. If the user is not authorized, the system displays error message 941F on the workbench.
3. If no errors occur, the object is then attempted to be allocated with a *EXCL exclusive lock. If it cannot be allocated, the system displays error 941C on the workbench.
4. If no allocation error, the RUNSQL statement is executed on the field/file/library to attach the fieldproc program X940000000. If an error occurs on the RUNSQL statement, the system displays error message 941G on the workbench.
5. If no error occurs on the RUNSQL statement, the file is de-allocated for the exclusive lock and the process ends.
6. If the process ends successfully, the IBM command DSPFFD can be run for the file and library where the Field Level Masking was placed. Then, you can scan for the field using F16 to confirm that the fieldproc X940000000 program has been attached to the field. See the example in the Appendix B - Example of Setting a

Field with Field Level Masking, to use the DSPFFD command and finding the fieldproc attached to the field.

7. You can run the following SQL statement to verify that the field has been set up for Field Level Masking:

   - Select sys_cname, sys_tname, sys_dname, fldproc from qsys2/sysfields

   This file contains every Field/File/Library combination in the system that has Field Level Masking applied, so the combination now exists.

8. If the process did not end successfully, review the error message and refer to the interactive session job log for further details for the specific issue found.

12.9 Dropping Field Level Masking

The Masking Status field displays as Inactive on the workbench, if a database field is not set or has been dropped from Field Level Masking.

To drop a field in a file and library from Field Level Masking based on the Authorization List and the Masking Definition (Data Item and Mask Code) specified, select option 5 (Drop) from the Field Level Masking workbench screen.

When you select option 5 (Drop) to drop the field, the system completes the following steps:

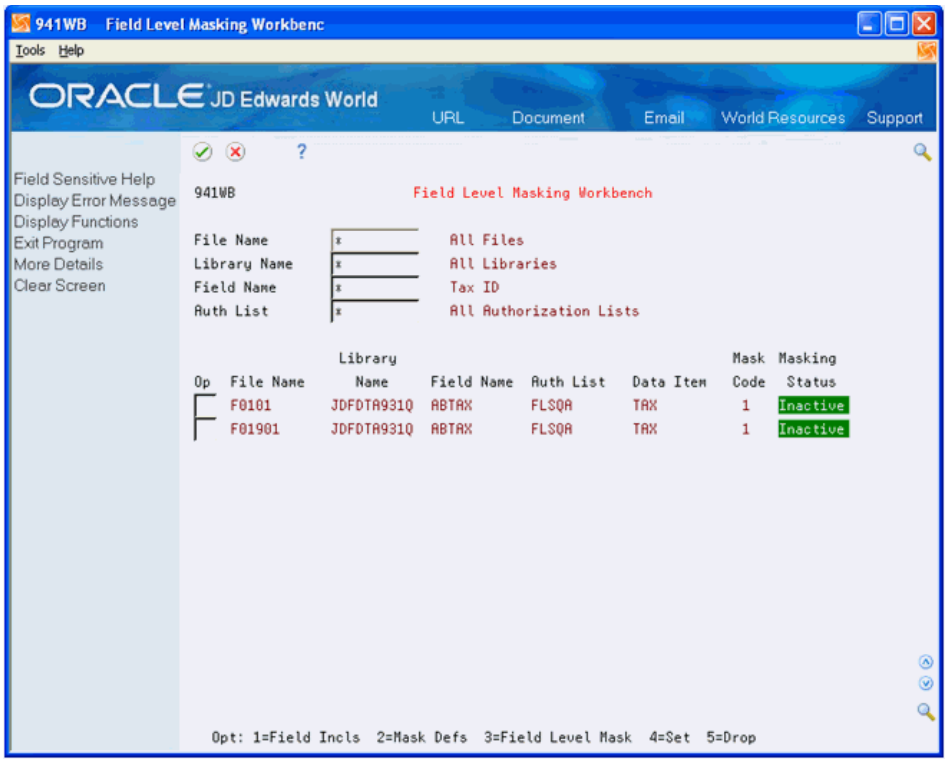
1. The object (file and library) is checked first for existence and both *OBJMGT and *OBJOPR rights for the user attempting the set. If the object does not exist (IBM error CPF9801) or any other error occurs on the check object command, the system displays error message 941E.
2. The IBM Authorization List is also checked to determine if the user has *READ or *UPD rights. If the user is not authorized, the system displays error message 941F on the workbench.
3. If no errors occur, the object is then attempted to be allocated with a *EXCL exclusive lock. If it cannot be allocated, the system displays error 941C on the workbench.
4. If no allocation error, the RUNSQL statement is executed on the Field/File/Library to drop the fieldproc program X940000000. If an error occurs on the RUNSQL statement, the system displays error message 941H on the workbench.
5. If no error on the RUNSQL statement, the file is de-allocated for the exclusive lock and the process ends.
6. If the process ends successfully, the IBM command DSPFFD can be run for the file and library where the Field Level Masking was dropped. Then, scanning for the field using F16, confirms that the fieldproc X940000000 program has been dropped from the field. See the example in the Appendix B - Example of Setting a Field with Field Level Masking, to use the DSPFFD command and finding the fieldproc dropped from the field.
7. You can run the following SQL statement to prove the field has now been removed from Field Level Masking:

   - Select sys_cname, sys_tname, sys_dname, fldproc from qsys2/sysfields

   This file contains every Field/File/Library combination in the system that has Field Level Masking applied, so the combination no longer exists.

8. If the process did not end successfully, review the error message and refer to the interactive session job log for further details for the specific issue found.

Figure 12–11 Field Level Masking Workbench screen



Field	Explanation
File Name	The identification, such as program number, table number, and report number, that is assigned to an element of software.
Library Name	The Data File Library Name designates the library location of the data base files.
Field Name	This field contains a value that identifies an exit or action in Extensibility or a database field allowed for use in Field Level Masking. *Screen-Specific Information* In Field Level Masking, the Field Name is used to define the field within a data base file that is to be included and/or enabled in Field Level Masking.
Auth List	The Authorization List will be used in Field Level Masking for authorizing the database field for viewing or updating purposes to a list of user profiles.

Field	Explanation
Op	Selection exit codes are options and function keys that are used to perform a specific function for a selected line or form of data. The most commonly used selection exits for each program are displayed in highlighted text at the bottom of the form. To display all available selection exits, press F24. Press F1 in the Option field to display all available Options for the program.
File Name	The identification, such as program number, table number, and report number, that is assigned to an element of software.
Library Name	The Data File Library Name designates the library location of the data base files.
Field Name	This field contains a value that identifies an exit or action in Extensibility or a database field allowed for use in Field Level Masking. *Screen-Specific Information* In Field Level Masking, the Field Name is used to define the field within a data base file that is to be included and/or enabled in Field Level Masking.
Auth List	The Authorization List will be used in Field Level Masking for authorizing the database field for viewing or updating purposes to a list of user profiles.
Data Item	For World, the RPG data name. This data field has been set up as a 10-byte field for future use. Currently, it is restricted to 4 bytes so that, when preceded by a 2-byte table prefix, the RPG data name will not exceed 6 bytes. Within the Data Dictionary, all data items are referenced by this 4-byte data name. As they are used in database tables, a 2-character prefix is added to create unique data names in each table specification (DDS). If you are adding an error message, this field must be left blank. The system assigns the error message number using next numbers. The name appears on a successful add. You should assign error message numbers greater than 5000. Special characters are not allowed as part of the data item name, with the exception of #, @, $. You can create protected data names by using $xxx and @xxx, where you define xxx. Create new data items using system codes 55-59. The alias cannot be changed.

Field	Explanation
Mask Code	The Masking Code is used in Field Level Masking to identify a Data Dictionary Item that is being masked in a certain defined way. This Masking Code allows multiple ways to mask the Data Dictionary Item at a database file field level. For example, a Tax ID field can be masked to show the last 4 numbers only with an * appearing in the first 5 positions. A second Masking Code might be defined on this field to use a Masking Value of / rather than *. A third Masking Code might identify the Tax ID field to show only the last two numbers with a Masking Value of > in the first 7 positions.
Masking Status	The Masking Status is used in Field Level Masking to determine whether the data base field in a file and library has been set. The values for Masking Status are: Active - Field Level Masking is set for this field. Inactive - Field Level Masking is not set for this field or it has been dropped.
File Description	The description of the selected video screen or user ID.
Data Item Description	Additional text that further describes or clarifies a field in the J.D. Edwards systems.

13

Set Up User Defined Codes Security

This chapter contains the topic:

- Section 13.1, "Setting Up User Defined Codes Security."

13.1 Setting Up User Defined Codes Security

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose Security Officer

From Security Officer (G9401), choose User Defined Codes

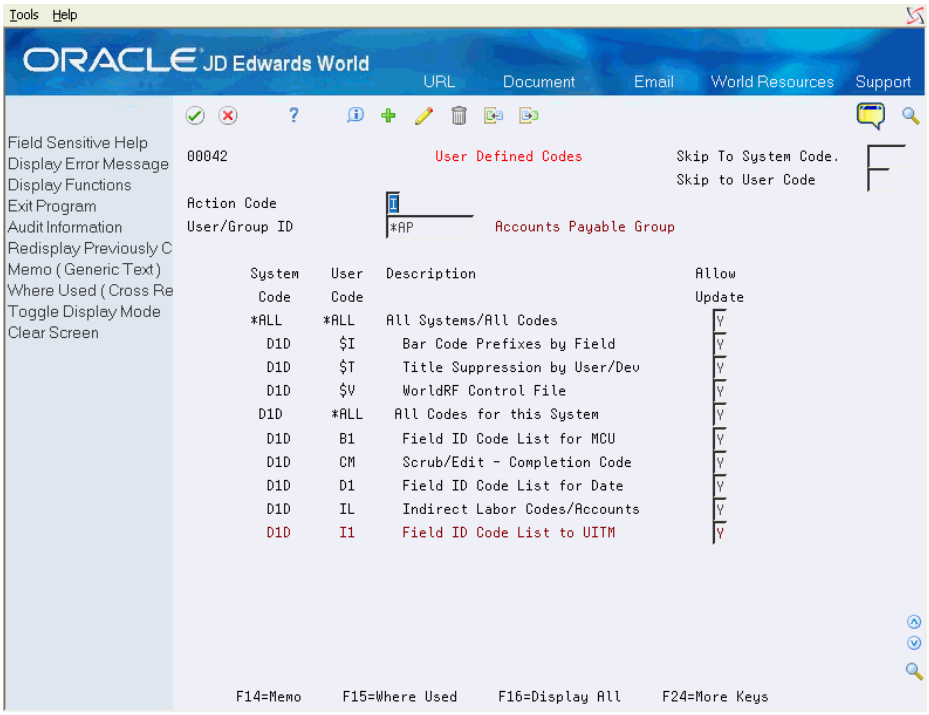
User Defined Code Security allows you to secure users, groups, or *PUBLIC from adding, changing, or deleting User Defined Code files. You may secure all User Defined Code files, all User Defined Code files within a system code, or individual User Defined Code files. When you define User Defined Security by system code, you can allow or deny access to all User Defined Codes files in a system code, without affecting authorization in other system codes.

> **Important!:** The default setting for the User Defined Codes Security program is No Access if you have not set up records with the Allow Update field set to 'Y'. To allow users to update user-defined code files, you must set up records for individual users, groups, or *PUBLIC with the appropriate authorization to allow update access to User Defined Code files.
>
> Users can always inquire on UDC files and the values in the tables.

To set up User Defined Codes security

1. On User Defined Codes, enter a user ID or group ID in the User ID field.

Figure 13–1 User Defined Codes screen



2. In the Allow Update field, enter 'Y' to allow update access, or 'N' to restrict update access.

Field	Explanation
User ID	The User/Group field is used to enter user defined code security records for a particular user, group, or *PUBLIC.
Allow Update	Enter 'Y' to allow updating or 'N' to restrict updating.

In the top half of the screen, you enter a user ID, group ID, or *PUBLIC in the User ID field. The subfile displays all User Defined Code security that is set up for the profile that you entered. When you enter a value in the User/Group ID field, that profile must exist in the User Information file (F0092).

The following function keys are available on the screen. Place your cursor on a subfile record to use these options:

- F14 - Memo: Use this option to enter free-form text with any notes, comments or explanations about the security record. If a memo exists for a record, the subfile values in the System Code and User Code columns are highlighted and See Memo displays above the System Code column.
- F8 - Audit Information: Use this option to retrieve audit information for a security record.
- F9 - Use this option to display an inquiry again after an update.

13.1.1 General Guidelines

To set up security for a profile for the first time, inquire on the profile name. The subfile is then loaded with all User Defined Code files. Set the appropriate actions for the desired codes, change the Action Code field to 'C' and press enter. If the user

profile does not exist in the User Information file (F0092), the User Defined Code files are not displayed. You cannot set up security information for a profile that does not exist.

To add new lines to an existing user record, inquire on the record. Press F16 to display all User Defined Code files, make your security selections, then change the action code to 'C', and press Enter.

To copy one user's setup to another, inquire on the record, change action code to an 'A', type the new user profile name and press Enter. Ensure that all the users' security records are loaded into the subfile before copying. Only records loaded in the subfile are copied to the new profile.

Use the 'D' action code with caution. If you enter 'D' in the Action Code field after you have inquired on a profile, all records in the subfile are deleted. To delete just one record in the subfile, place a 'C' in the Action Code field, clear the Allow Update field in the line to be deleted and press Enter.

13.1.2 User Defined Codes Security - Helpful Hints

When working with User Defined Code Security, the following considerations apply:

If you do not use roles or groups, the system checks user- defined code security in the following order:

1. User Profile ID and User Defined Code Table
2. User Profile ID and System Code, User Code=*ALL
3. User Profile ID and System Code=*ALL
4. *PUBLIC and User Defined Code Table
5. *PUBLIC and System Code, User Code=*ALL
6. *PUBLIC and System Code=*ALL

If the user logs on without selecting a role and belongs to a group (specified on the JDE User Profile record in the F0092 file), the system checks the security file in the following order:

1. User Profile ID and User Defined Code Table
2. User Profile ID and System Code, User Code=*ALL
3. User Profile ID and System Code=*ALL
4. Group Profile ID (if any) and User Defined Code Table
5. Group Profile ID (if any) and System Code, User Code=*ALL
6. Group Profile ID (if any) and System Code=*ALL
7. *PUBLIC and User Defined Code Table
8. *PUBLIC and System Code, User Code=*ALL
9. *PUBLIC and System Code=*ALL

In either of the scenarios described, the application stops checking when it encounters an appropriate record and uses the authority on the record it has found.

If you do not use role-based security, the system uses the group profile from the JD Edwards user profile, if a user profile exists.

If you use role-based security, a user who signed on using a role may have access to the authority for multiple groups. In this case, the system checks the profiles of all

active groups for the role. If any group has authority, the role is granted authority. When a user is signed on using a role, the system does not check the user profile's group.

14

Set Up Batch Approval/Post Security

This chapter contains the topic:

- Section 14.1, "Setting Up Batch Approval/Post Security."

14.1 Setting Up Batch Approval/Post Security

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose Security Officer

From Security Officer (G9401), choose Batch Approval/Post

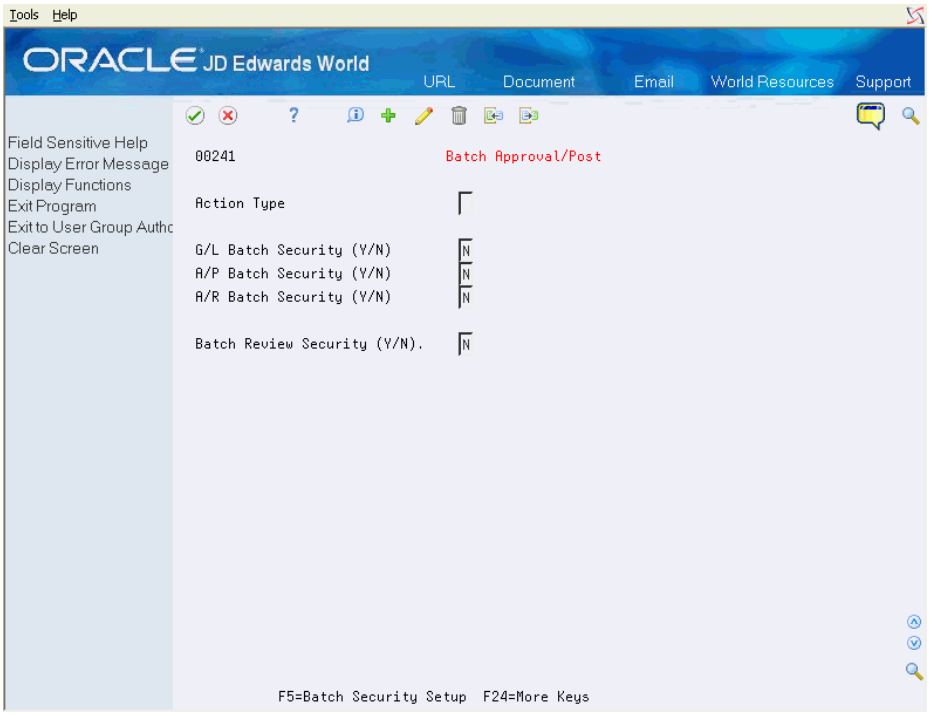
Batch Approval/Post security restricts the approval and posting of batches to certain users. Security can be set up for the General Ledger, Accounts Payable, and the Accounts Receivable systems. You set up a secured user and supervisor approval names.

Note: It is important to complete all of these steps. If you skip any of the steps, Batch Approval/Post Security does not work.

To set up Batch Approval/Post Security

1. On Batch Approval/Post, choose Exit to User Group Authority (F5) to access the Batch Approval/Post Security Revisions program (P0024) and set up the approved and secured users.

Figure 14–1 Batch Approval/Post screen

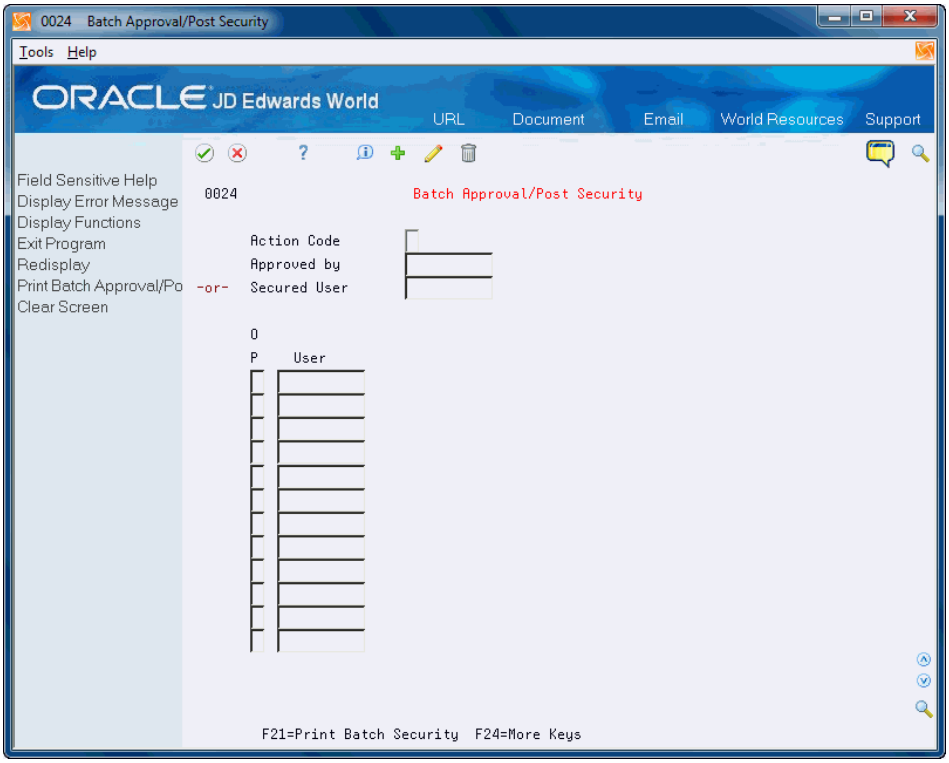


2. On Batch Approval/Post Security, complete the following fields:
   - Approved by

     Approved by user has authority to approve and post batches.
   - Secured User

     Secured user does not have authority to approve or post batches.

Figure 14–2 Batch Approval/Post Security screen

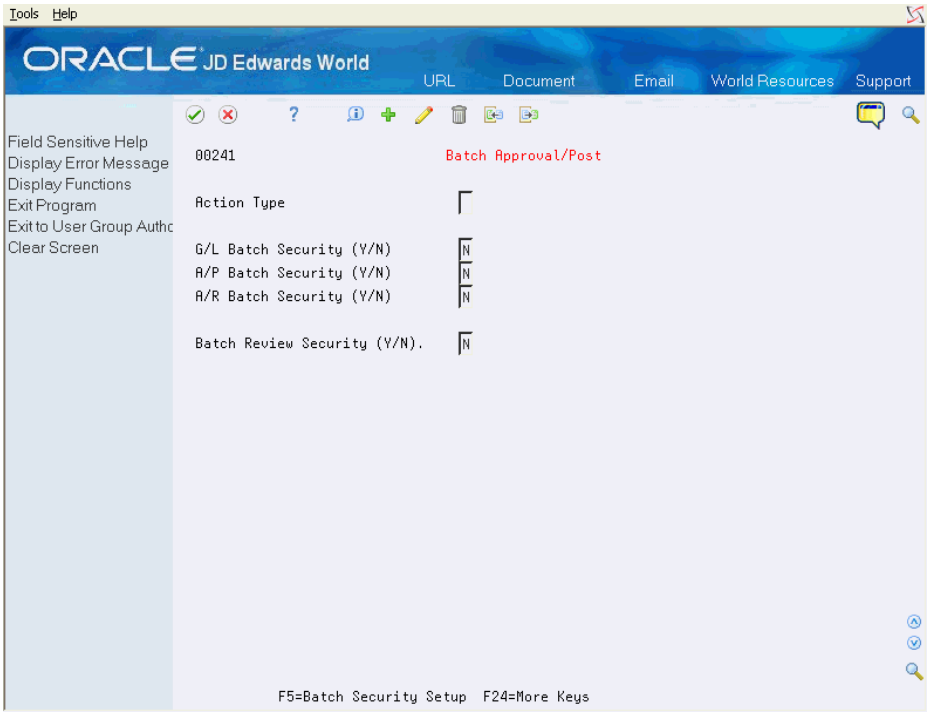


3. Enter user IDs in the User fields for those batches that the Approved by user can approve and post.
   - *ALL is valid if Approved By User has authority to all batches
   - Group profile or *PUBLIC is not valid.
4. Enter one of the following values in the Option field and click Enter.
   - 1 - Memo: Use this option to enter free-form text with any notes, comments or explanations about the security record. If a memo exists for a record, the selection option field will display in reverse image.
   - 2 - Audit Window: Use this option to access the Audit Information Window which contains add and change information as well as the date and time of the action.
   - 9 - Delete/Cancel: Use this option to delete a security record. Alternatively, you can delete a record by clearing all the fields on the line.
5. Choose Redisplay (F9) to refresh the screen after the update.
6. Optionally, perform the following:
   - To add new lines to an existing profile or program, you must first locate the record. You can enter new information on either the first available blank line or over an existing profile and click Change. If you enter information in the first available blank line and click Change, the system adds the record. If you enter information over an existing record and click Change, the program changes that record, including the key.
   - To delete an existing profile or program, you must first locate the record. After you locate a profile or program and click Delete, the system deletes all records

in the subfile. To delete one record in the subfile, clear the ID and click Delete. You can also enter 9 in Option field.

7. Exit (F3) to the Batch Approval/Post screen.
8. Enter a Y or N for each of the batch security approval/post programs.

Figure 14–3 Batch Application/Post Security (Approval/Post) screen



9. Access the Constants and enter Y in the Management Approval of Input field for each system.

   You can locate the Constants for each system on the following Setup menus:

   - General Accounting Constants (G0941)
   - Accounts Receivable Constants (G0341)
   - Accounts Payable Constants (G0441)

Figure 14–4 General Accounting Constants screen

15

Set Up Report Writer Security

This chapter contains these topics:

- Section 15.1, "Setting up Report Writer Form Security,"
- Section 15.2, "Updating Report Writer Version Security,"
- Section 15.3, "Masking DREAM Writer Processing Options."

15.1 Setting up Report Writer Form Security

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose Security Officer

From Security Officer (G9401), choose Report Writer Form

Report Writer Form security enables you to secure report writer forms and queries for any JD Edwards User ID from being executed, added, changed, or updated. A user ID can be an individual user ID, a group profile ID, or *PUBLIC. The Form ID can be any STAR, FASTR, or DREAM Writer Form ID that is found in Software Versions Repository (F9801), and the Query Group can be any World Writer Group found in User Defined Codes 82/GR.

Report Writer Form security accommodates role-based security. In addition to user and group level security, users may be assigned to a security role. When users sign on with a security role, all the groups tied to that security role will be considered when determining authorization to report writer forms.

Important!: The default setting for the Report Writer Form program is No Access if you have not set up records with action code types (Execute, Add, Change, Delete) of 'Y'. To allow users to access Report Writer Form security, you must set up records for individual users, groups, or *PUBLIC with the appropriate authorization to allow update access to User Defined Code files.

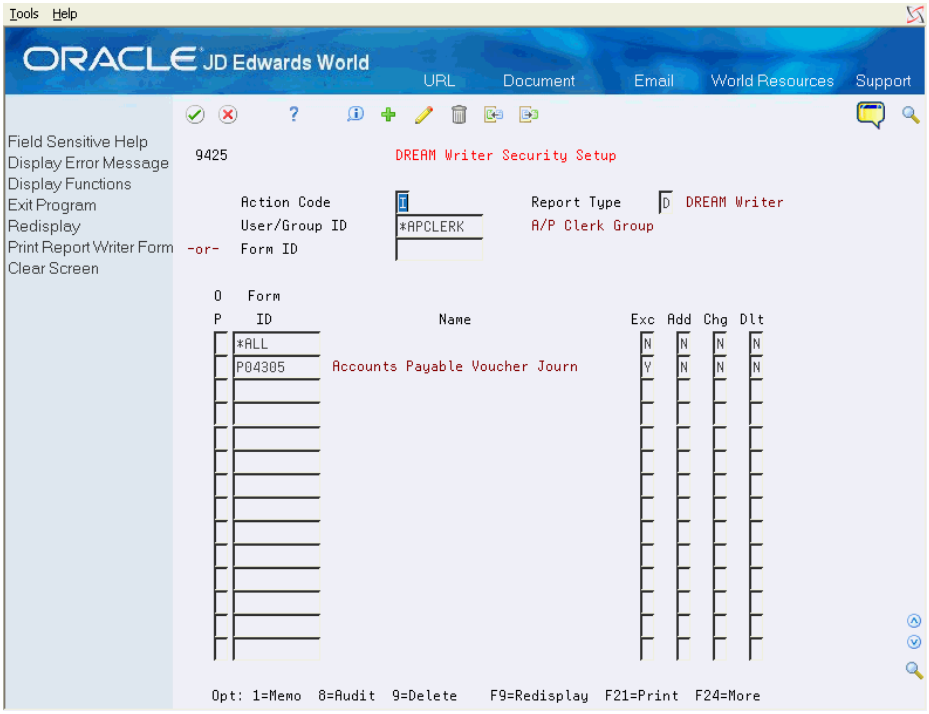
Report Version security reassigns security for DREAM Writer versions. It restricts other users from executing, changing, deleting, and copying versions.

Initially, you should place security on DREAM Writer when you create the version. Use the Report Version utility to apply or remove DREAM Writer security.

To set up Report Writer security

1. On DREAM WRITER Security Setup, complete either of the following fields:
   - User/Group ID
   - Form ID/Query Group

Figure 15–1 DREAM Writer Security Setup screen



2. Complete the ID field
3. In the Action Code field, enter 'Y' to allow access, or 'N' to restrict access.

Field	Explanation
Report Type	Indicates the type of report. Valid options are: D= DREAM Writer F= FASTR S= STAR W= World Writer These values are stored in User Defined Codes file 98/VT.
User/Group ID	A JD Edwards user or group, or *PUBLIC.
Form ID/Query Group	The DREAM Writer, FASTR, or STAR Form ID, or the World Writer Query Group
Name	The name of the User/Group or Form ID/Query Group to secure.
E (Execute)	This code designates whether the user or group has the authority to EXECUTE a version on the form. Enter 'Y' or 'N'

Field	Explanation
A (Add)	This code designates whether the user or group has the authority to ADD a version on the form. Enter 'Y' or 'N'.
C (Change)	This code designates whether the user or group has the authority to CHANGE a version on the form. Enter 'Y' or 'N'.
D (Delete)	This code designates whether the user or group has the authority to DELETE a version on the form. Enter 'Y' or 'N'.
F (Upd)	This code designates whether the user or group has the authority to UPDATE a field in the file specified in the version. Enter 'Y' or 'N'. Note that this field only appears for a World Writer Report Type.

In the top half of the screen, you may enter either user/group ID or form I/query group. When you press Enter, the subfile displays all programs associated with a particular user or group profile or all profiles associated with a particular form ID, that are set up for the report writer type.

The following fields are available on the screen:

- Option 1 - Memo: Use this option to enter free-form text with any notes, comments or explanations about the security record. If a memo exists for a record, the selection option field will display in reverse image.
- Option 8 - Audit Information Window: Use this option to retrieve audit information for a security record.
- Option 9 - Delete Line: Use this option to delete a security record. Alternatively, a record can be deleted by blanking out all the fields on the subfile line.

Press F9 to display an inquiry again after an update.

After you set up a 'model' profile, you may use that model to add new profiles. Use the following steps to add profiles based on a model profile:

1. Inquire on the model
2. Roll to the end of the subfile to be sure all records are included.
3. Enter 'A' in the Action Code field, enter the new profile, and press Enter.
4. Inquire on the new profile that you just added to verify the additions.

Use the same approach for form IDs.

To add new lines to an existing profile or form ID, inquire first. You may then enter 'C' in the Action Code field and enter new information on either the first available blank space or over an existing profile. If you enter 'C' in the Action Code field and enter information in the first available blank space, the system adds the record. If there is a 'C' in the Action Code field and you type over an existing record, the information for that record is changed, including the key.

Use the 'D' action code cautiously. If you enter 'D' in the Action Code field after you have inquired on a profile or form ID, the system deletes all records in the subfile. To delete just one record in the subfile, enter 'C' in the Action Code field, scroll down and clear the ID in the line that has to be deleted, and press Enter. You can also delete a record by entering 9 in the subfile selection field of the line that has to be deleted.

Import and Export capabilities are available on the Report Writer Form Security screen. For more information see the Work With Import/Export in the *JD Edwards World Technical Tools Guide*.

In addition to accessing the Report Writer Form (V9425) from G9401, you can also access it from the following menus, for specific report types. In these menu options, the Report Type field is hard-coded to the specific report type you are inquiring on:

- G81 - DREAM Writer Form Security
- G8331 - FASTR Form Security
- G12411 - STAR Form Security
- G8231 - Query Group Security

15.1.1 General Guidelines

If a user does not have a role or group, the Report Writer Form Security program checks for security records for a specific report writer type in the following sequence:

1. User Profile ID and Form ID
2. User Profile ID and Form ID = *ALL
3. *PUBLIC and Form ID
4. *PUBLIC and Form ID = *ALL

When the system locates an appropriate record, the application stops checking and uses the authority on the record it has found.

This order is all within the report writer type that you are working with. It is possible to define the same User/Group ID and Program ID within STAR (Report Writer Type = 'S') and within FASTR (Report Writer Type = 'F'). However, this would not be set up in the same video transaction.

If you want to secure a profile for a specific report writer type from performing any specific action in all programs, use '*ALL' in the Form ID field for that profile. The system checks the *ALL record after checking for the specific form ID. This allows for an override to the general rule.

If a user logs on without selecting a role and belongs to a group (specified on the JD Edwards User Profile record in the F0092 file), the system checks the security file in the following order:

1. User Profile ID and Form ID
2. User Profile ID and Form ID = *ALL
3. Group Profile ID (if any) and Form ID
4. Group Profile ID (if any) and Form ID = *ALL
5. *PUBLIC and Form ID
6. PUBLIC and Form ID = *ALL

When the system locates an appropriate record, the application stops checking and uses the authority on the record it has found.

If you do not use rol- based security, the system uses the group profile, if any, from the JD Edwards User Profile.

If you use role- based security, a user who signs on using a role has access to the authority for multiple groups. In this case, the checks for group profile check all active

groups for the role. If any group has authority, the role is granted authority. When a user signs on using a role, the user profile's group, if any, is not checked.

Each action code has a Y/N flag which determines whether the user/group or *PUBLIC has authority to that particular action for a form ID or *ALL.

If you want to secure a profile from any access to an interactive program, enter 'N' in the Execute Action field. All other fields must be set to 'N'. This completely locks the profile from the form ID or *ALL.

15.2 Updating Report Writer Version Security

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security & System Admin

From Security & System Administration (G94), choose Hidden Selection 27

From Security Advanced & Technical Ops (G9431), choose Report Version Security

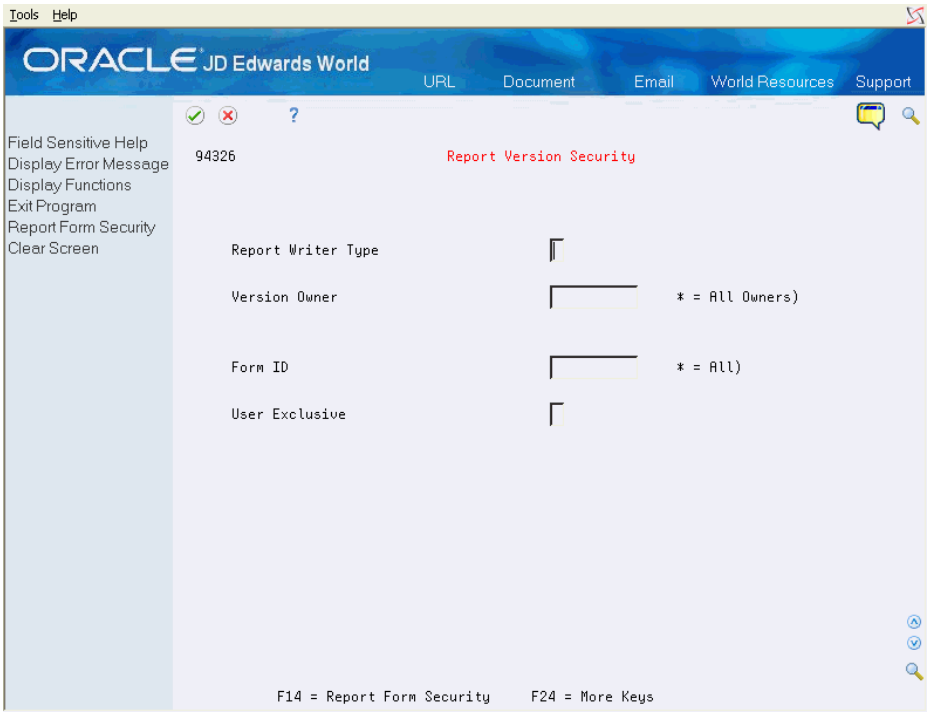
Use this program to update the Report Writer Version Security (User Exclusive Flag) for DREAM Writer, FASTR, STAR and World Writer report versions. You may update all versions or limit the versions to be updated by Version Owner and/or Form ID or Query Group.

Report version security accommodates role-based security. In addition to user and group level security, users may be assigned to a security role. When users sign on with a security role, all the groups tied to that security role will be considered when determining authorization to report writer versions.

To update report version security

1. On Report Version Security, complete the following fields:
   - Report Writer Type
   - Version Owner
   - Form ID
   - User Exclusive

Figure 15–2 Report Version Security screen



Field	Explanation
Report Type	Indicates the type of report. Valid options are: D= DREAM Writer F= FASTR S= STAR W= World Writer These values are stored in User Defined Codes file 98/VT.
Version Owner	The user or group id that currently appears as the owner of the version. You may specify '*' for all version owners.
Form ID/Query Group	The DREAM Writer, FASTR, or STAR Form ID, or the World Writer Query Group to which the report versions are assigned.

Field	Explanation
User Exclusive	This field allows you to restrict access for a report version for users or groups other than the Version Owner. Version Owner has all authority, but other users' or groups' authority is restricted as follows: 0 - No security. Others have all authority. This is the default when adding a new version. 1 - Medium security. Others can install, copy, transfer, or run the version, including changing processing options and data selection at runtime. JD Edwards Demo versions are delivered with this security. 2 - Medium to full security. Others can only install or copy the version. 3 - Full security. Others have no authority. 4 - Medium security-extended. Others can only install, copy, transfer, or run the version - but cannot change processing options and data selection at runtime. This field corresponds to the User Exclusive field in the version.

You may press F14 to access the Report Writer Form Security screen (V9425). The Report Version Security screen. provides the default value for the User/Group ID field.

In addition to accessing the Report Writer Form Security screen (V94326) from G9431, you can also access it from the following menus, for specific report types. In these menu options, the Report Type field is hard-coded to the specific report type you are inquiring on:

- G81 - DW Report Version Security
- G8331 - FASTR Report Version Security
- G12411 - STAR Report Version Security
- G8231 - WW Report Version Security

Note: File/Field Level Security (P8202) is available and is exclusive to World Writer. For more information on the File/Field Level Security program, please refer to the World Writer guide.

15.3 Masking DREAM Writer Processing Options

As a security feature, you can mask DREAM Writer Processing Options from users by entering a value in the Display Level field next to each processing option that you need to hide. You must also enter a corresponding display level to the user profile. To mask the processing option you must:

- Enter a level higher in the DREAM Writer Processing Options than the level that you enter in the individual user profiles
- Enter a display level value only in the value entry lines (these are lines where the Text Only field contains a value of 0).

Navigation

From Master Directory (G), choose Hidden Selection 27

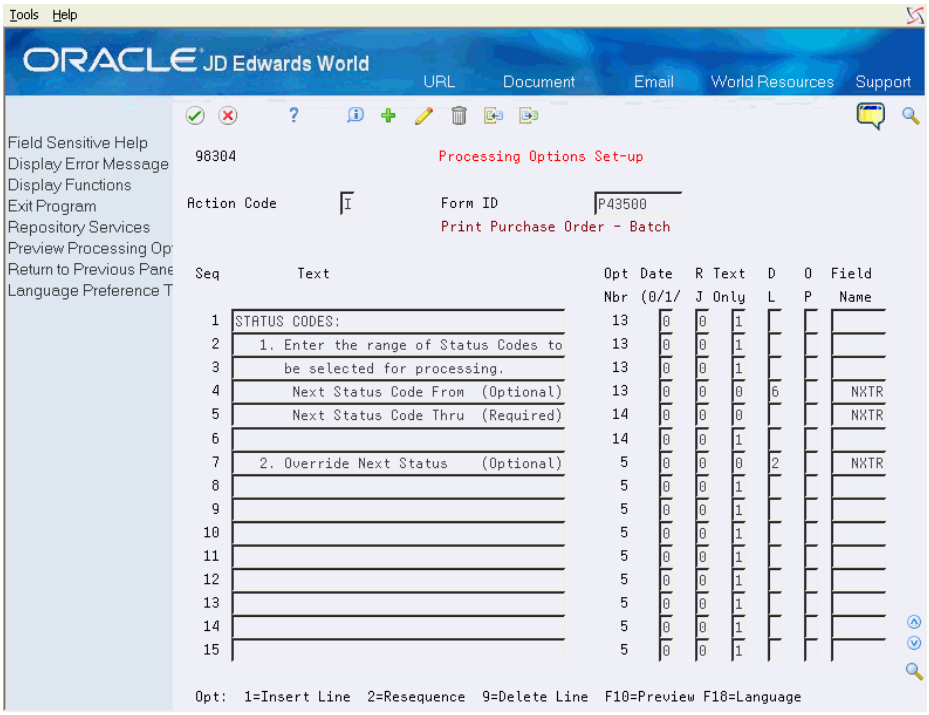
From Advanced & Technical Operations (G9), choose Run Time Setup

From Run Time Setup (G9), choose DREAM Writer

From DREAM Writer (G81), choose Processing Options Set-up

In the following example, the Next Status Code From processing option is set at display level 6. Only users with display levels of 6 through 9 in their user profile can view this processing option. Users with display levels of blank through 5 in their user profile cannot view this processing option. You require users to access the Next Status Code Thru processing option, so you should not mask this processing option. Assigning a display level of 2 to Override Next Status allows those users with levels of 2 and above in their user profile to view the option. Users with display levels of 1 and below (including the alpha character display levels) in their user profile cannot view this processing option.

Figure 15–3 Processing Options Set-Up screen



16

Change User Profile Ownership

This chapter contains the topic:

- Section 16.1, "Changing User Profile Ownership."

16.1 Changing User Profile Ownership

Navigation

From Master Directory (G), choose Hidden Selection 27

From Advanced & Technical Operations (G9), choose Security and System Admin

From Security and System Administration (G94), choose System Administration

From System Administration (G944), choose Change User Profile Ownership

This utility transfers object ownership for all objects owned by one user to another user.

Additionally, using the IBM command CHGOBJOWN allows you to specify one object at a time. You must specify the object name in the command.

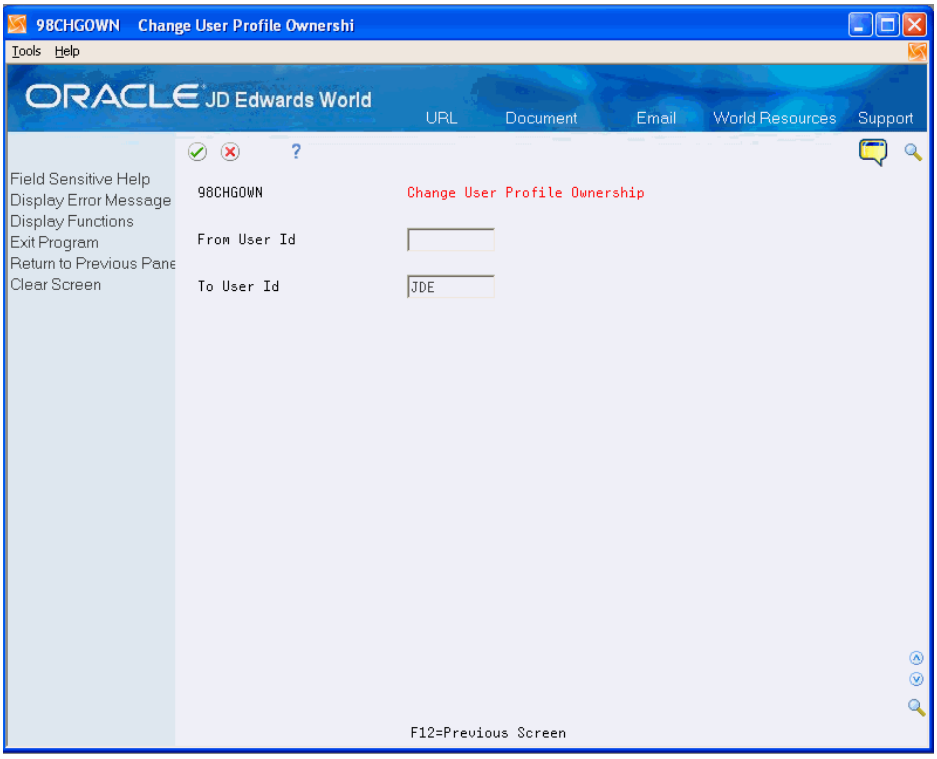
To change the user profile ownership

On Change User Profile Ownership, complete the following fields:

- From User Id
- To User Id

Note: Use caution when using this option. It changes all objects, including IBM objects.

Figure 16–1 Change User Profile Ownership screen



17

Work With the Security Workbench

This chapter contains these topics:

- Section 17.1, "Understanding the Security Workbench,"
- Section 17.2, "Using the Security Workbench,"
- Section 17.3, "Working With the Security Tester,"
- Section 17.4, "Understanding the Security Detail Report."

17.1 Understanding the Security Workbench

Navigation

From Master Directory (G), choose Hidden Selection 27

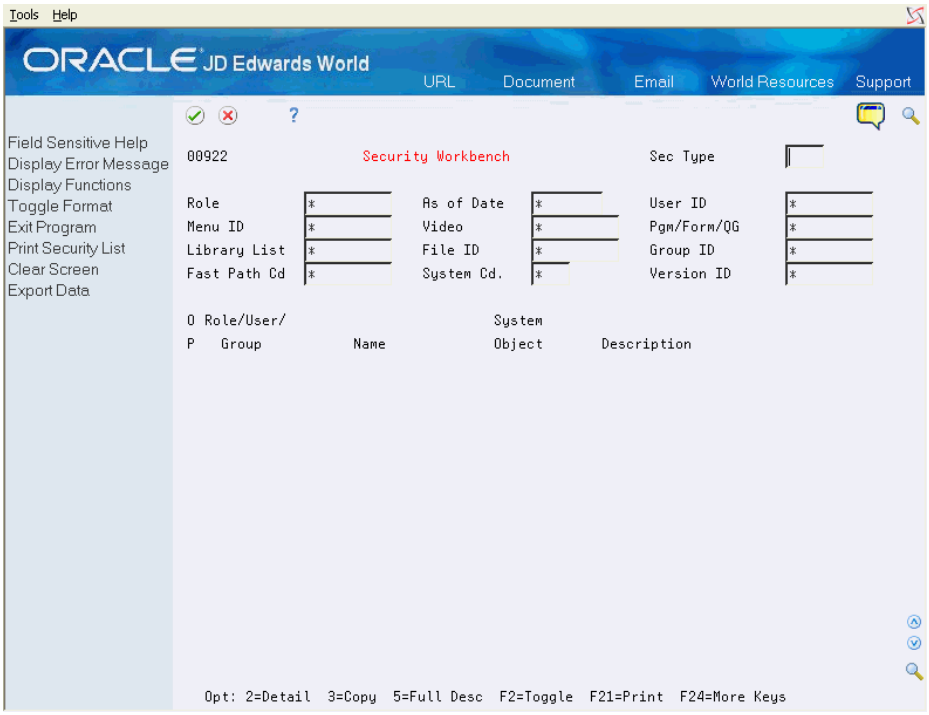
From Advanced & Technical Operations (G9), choose Security and System Admin

From Security Administration (G94), choose Security Officer

From Security Officer (G9401), choose Security Workbench

The Security Workbench program provides a summary view of your security setup and allows you to test certain aspects of your security. Option exits are provided to most security maintenance types. A flexible inquiry capability enables you to answer a variety of security questions. Print and export options allow you to document your security setup.

Figure 17–1 Security Workbench screen



The Security Workbench program contains a number of features to support its function as a single access point for security inquiries and a starting point for accessing specific security maintenance programs.

Use the Security Workbench program to inquire on all major security types, such as user profiles, menu security, action code security, and function key security. The workbench adjusts many fields based on which security type you are currently viewing:

- Position/Filter fields in the header portion display based on the value in the Security Type field.
- A filter field above the Details column changes format based on the security type.
- The subfile column headings text changes based on the security type.
- The Details column on the right of the subfile displays different information based on the security type, showing details relevant to that security type. The filter field works in conjunction with the Details column to allow additional filtering on the detail information.

The Position/Filter fields in the header are enabled for wildcard search which allow you to use the same field to position the subfile or limit the subfile display to specific groups of records. Configurable wildcard characters control the behavior of these fields.

See Also:

- Section 17.3.3, "Wildcard Search."

17.2 Using the Security Workbench

Beginning with JD Edwards World release A9.3, a Security Workbench video (V00922) is available to help the security administrator gain an overall perspective of the JD

Edwards World security setup. The security workbench supersedes the User Review video (V00921).

View Security Information

The security workbench is a multiple-purpose video that displays information relevant to the various types of security information supported. Enter the security type and press Enter. The video will reformat itself to display information related to that particular security type. The header portion of the video will display only those filtering fields that apply to the security type. The subfile portion of the video will display users/groups and the secured system resources.

Use Wildcard Search Characters

The security workbench supports wildcard search characters in the filter fields in the header portion of the video. See the program helps for the security workbench for examples of using the wildcard characters.

Toggle Format/Sort Sequence

In the security workbench video, the F2 function key allows you to toggle the display to switch the positions of the user/group information versus the system resources information. This will also change the sort sequence of the subfile information; whichever type of information appears on the left will be the primary sort sequence.

Copy and Delete User Profiles

The security workbench allows you to exit to the Copy User/Group Security (V00922C) or Delete User/Group (V00922D) videos.

Test Authorizations

The security workbench also has an exit to the Security Tester video (V00922T), which helps you drill down into specific authorizations. Currently, the action code and function key security types are supported in the security tester. The security tester video displays the authorization for a user or group, using a role or not. The security records that come into play in determining the authorization appear below the net result, separated by a dashed line.

Report Security Setup Information

The security workbench has a Print (F21) function key to quickly print the current subfile display. The Security Detail Report (R00922P) is also available from the Security Officer menu. The advantage of the menu option is that multiple security types may be selected at once, whereas the security workbench is limited to display only one security type at a time. This functionality is useful, for example, if you want to print all security information for a given user.

To Use the Security Workbench

1. On Security Workbench, press F1 on the Security Type field and select security type.

Field	Explanation
Security Type	Use this field to specify which type of security you wish to view or test. The security type controls many aspects of the video. In addition to security, this field can also be used to show report version ownership. Once you select a security type, the full security type description will appear under the program title.

Field	Explanation
Position/Filter	These wildcard-enabled fields control which records are displayed in the subfile (lower) portion of the video. Only the Position/Filter fields which are relevant to the security type are displayed.
Filter by	Use this field to filter the subfile based on the information in the Details column. This field is for filtering the subfile only; it does not work as a positioning field.
Effective Dates	Security role records and the records for users, groups and library lists which associate to security roles have effective dates. These are shown in the subfile fold area. Press F4 to show the fold area.
Business Unit Thru Number	For the business unit security records, the From Business Unit number is shown on the primary subfile line in the Details column, and the Thru Business Unit number is shown directly beneath the From number in the Details column in the fold area. Press F4 to show the fold area. Filter by is based on the From Business Unit number.

For advanced menu security records, the value 'all menu selections' is displayed as a zero in the Details column, allowing you to filter on that value. On the Advanced Menu Security maintenance video (V008231), these values are displayed as blank.

17.2.1 Security Workbench Options

The following options are available for each subfile record:

- Option 1 - Generic Text: Use this option to call the Generic Text window for the selected security record to add notes. This is the same generic text that you access in the maintenance program for the selected security type. If text exists for a security record, the Option field displays in reverse image for that record. This option is only active for those security types that support generic text.
- Option 2 - Details: Use this option to select the current row and call the appropriate maintenance program to edit the data.
- Option 3 - Copy User/Group: Use this option to call the Copy User/Group program (P00922C), which allows you to copy the user profile and security records for a user or group. This option is only active for security types which display user/group information.
- Option 4 - Security Tester: Use this option to call the Security Tester video (V0092T). This video allows you test the selected security record to see if authorization is granted or not, and what security records are involved in the decision.

  See Section 17.3, "Working With the Security Tester" for additional information. NOTE: Not all security types are supported for the Security Tester. Currently supported security types for the test option are:

  – Action code security

  – Function key security
- Option 5 - Display Full Descriptions: Use this option to call the Full Descriptions video (V009221) which displays the full descriptions for the selected subfile record.

- Option 8 - Audit Information: Use this option to display the Audit Information Window (V0045) for the selected subfile record.
- Option 9 - Delete User/Group: Use this option to call the Delete User/Group program (V00922D), which allows you to delete the user profile and security records for a user or group. This option is only valid for those security types that display user/group information.

  See Deleting a User Group in the JD Edwards World Technical Foundation Guide for additional information.

17.2.2 Security Workbench Function Keys

following function keys are available on the Security Workbench screen:

- F2 - Toggle Format: Use this function key to toggle the video display by switching the left and right parts of the subfile display and also switching the sequence of the subfile records. When you access the Security Workbench screen, the left half shows User/Group/*PUBLIC IDs for most security types; the right half shows the system resource appropriate to the security type currently displayed. The primary sequence of the subfile is always based on the information displayed in the far left column
- F21 - Print: Use this function key to print the Security Detail Report for the current inquiry settings. **NOTE**: In order to see the report, you will need to do a WRKSPLF after using the F21 utility.
- F23 - Export Data: Use this function key to export data from the screen.

17.2.3 DREAM Writer Considerations

The processing options for the DREAM Writer program control default behaviors for the Security Workbench program. Use these options to specify the DREAM Writer versions of programs called by the Security Workbench program:

1. Copy User/Group Security (P00922C)

   There are DREAM Writer processing options which control certain aspects of the copy behavior. Check these to be sure the copy will do what you want.

2. Report Writer Form Security - DREAM Writer (P9425)

   Use program P9425 for maintaining report form security for all four report writers. The version contains a processing option which sets the video to the correct report writer for the security type. This version should set the video to look at DREAM Writer form security records.

3. Report Writer Form Security - FASTR (P9425)

   Use program P9425 for maintaining report form security for all four report writers. The version contains a processing option which sets the video to the correct report writer for the security type. This version should set the video to look at FASTR form security records.

4. Report Writer Form Security - STAR (P9425)

   Use program P9425 for maintaining report form security for all four report writers. The version contains a processing option which sets the video to the correct report writer for the security type. This version should set the video to look at STAR form security records.

5. Report Writer Form Security - World Writer (P9425)

Use program P9425 for maintaining report form security for all four report writers. The version contains a processing option which sets the video to the correct report writer for the security type. This version should set the video to look at World Writer form security records.

17.2.4 Security Workbench Examples

The following examples illustrate how you can select and display security data using the Security Workbench program.

17.2.4.1 Example 1

In this example, you inquire on all user profiles whose user ID begins with the letters 'MJ', and filter the subfile to determine which of these users have both Menu Travel and Command Entry authority. This example assumes that the wildcard search character is set to '*'. Use the following steps to perform the inquiry:

1. Enter Security Type = USER (User Profiles Security Type)
2. Press the Enter key to allow the header portion of the video to format to this security type.
3. Enter the following values:
   - User = MJ* (All User IDs starting with 'MJ')
   - Group = * (All Groups)
   - Filter by = Y Y * * * (MT=Y, CE=Y, DL=Any, AM=Any, BU=Any)
4. Press the Enter key to view the results displayed in the subfile.

After you have selected the USER security type, the system displays only the User and Group Position/Filter fields in the header. The Details column shows security information from the user profile:

- MT = Menu Travel Allowed Y/N
- CE = Command Entry Allowed Y/N
- DL = Menu Display Level
- AM = Advanced Menu Security Activated for This User Y/N
- BU = Advanced Business Unit Security Activated for This User Y/N

17.2.4.2 Example 2

In this example, you inquire on action code security and determine all users and groups that are locked out of Data Item Revisions. In action code security, if a user or group is denied authority to the Inquire and Add action codes, the user or group has no access to the program). This example assumes that the wildcard search character is set to '*':

1. Enter Security Type = SAC (Action Code Security Type)
2. Press the Enter key to allow the header portion of the video to format to this security type.
3. Enter the following values:
   - User = * (All User IDs)
   - Group = * (All Groups)
   - Pgm/Form/QG = P9201* (Data Item Revisions)

- Filter by = N N * * * (I=N, A=N, C=Any, D=Any, F=Any, T=Any)

4. Press the Enter key to view the results displayed in the subfile.

After you have selected the SAC security type, the system displays only the User, Group and Pgm/Form/QG Position/Filter fields in the header. The Details column shows security information from the Action Code Security file for user/group and program:

- I = Allow Inquire Y/N
- A = Allow Add Y/N
- C = Allow Change Y/N
- D = Allow Delete Y/N
- F = Allow From Y/N (Import)
- T = Allow To Y/N (Export)

17.2.5 Exporting Security Data from the Security Workbench

You can export records displayed on the Security Workbench screen to an export file on the Integrated File System (IFS). To export records, inquire on the records first. Then use Function Key F23 to display the Interactive Export Parameters (P00SFDLP). See the help instructions for that window for more information on how to proceed with exporting records to an export file.

The Security Workbench program does not allow you to import records from a file on the IFS.

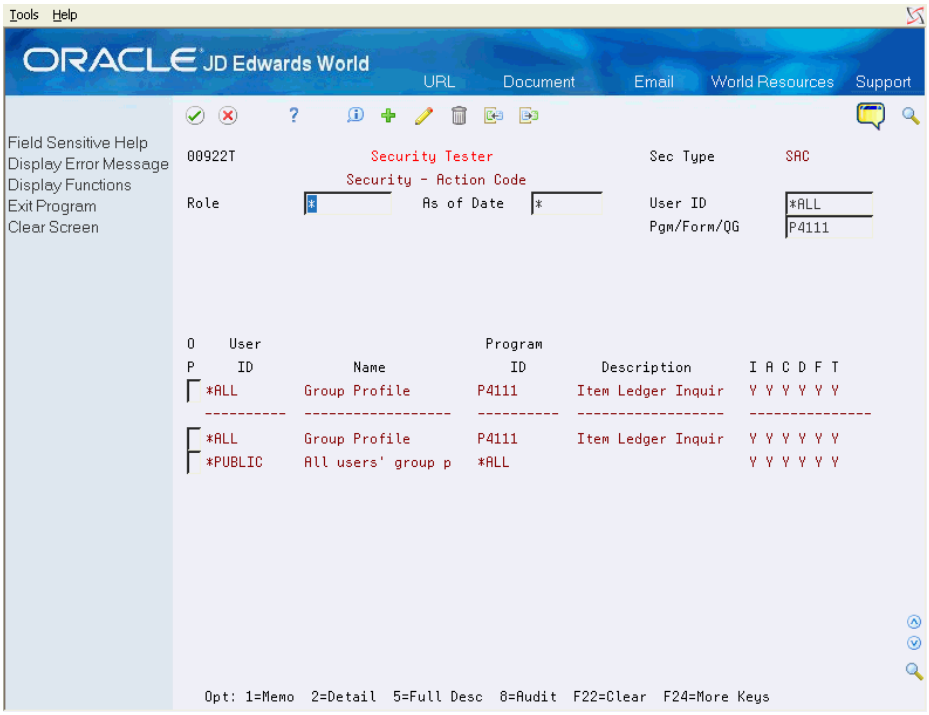
17.3 Working With the Security Tester

The Security Tester screen allows you to test whether specific security combinations allow or deny authority, and to see which security setup records are involved in the decision.

You access the Security Tester screen from the Security Workbench screen. The system adjusts the display of the header fields of the Security Tester screen in a manner similar to the header of the Security Workbench screen based on the security type that you display. However, the Security Tester displays one specific security scenario at a time, so the header fields are not Position/Filter fields as on the Security Workbench screen. You must enter specific values in the header fields. A special Details column at the right of the subfile displays different information based on security type, showing details relevant to the selected security type.

On the Security Workbench screen, use the Option column (Option 4) to test security for a specific security record. The Security Tester screen (V00922T) appears.

Figure 17–2 Security Tester screen



Use the Security Tester screen to inquire on the authority for specific security scenarios for the supported security types. The security types supported by the Security Tester are:

- Action Code Security
- Function Key Security

The Security Tester adjusts fields based on which security type you are currently viewing:

- Selection fields in the header portion display based on the security type
- The subfile column headings change the column heading text based on the security type

The program hides and protect selection field that are not relevant to the security type being displayed. Column headings and the Details column display information that is relevant to the security type.

Field	Explanation
Security Type	The security type selected displays in the upper right corner of the video. You may not change the displayed security type in this video.
Selection Fields	These fields are used to select specific security scenarios to display. Only the selection fields which are relevant to the security type are displayed. Role, As of Date, and User ID are always displayed.

Field	Explanation
Subfile Records	The subfile will display the final result of the authorization test in the first subfile line. i.e., does the user, group or *PUBLIC profile have authorization to the system resource. A dashed line separates the authorization result line from the list of security records which are potentially accessed in this specific security scenario.

17.3.1 Security Tester Options

The following options are available on the Security Tester screen:

- Option 1 - Generic Text: Use this option to call the Generic Text window for the selected security record to add notes. This is the same generic text that you access in the maintenance program for the selected security type. If text exists for a security record, the Option field displays in reverse image for that record.
- Option 2 - Details: Use this option to select the current row and call the appropriate maintenance program to edit the data.
- Option 5 - Display Full Descriptions: Use this option to call the Full Descriptions video (V009221) which displays the full descriptions for the selected subfile record.
- Option 8 - Audit Information: Use this option to display the Audit Information Window (P0045) for the selected subfile record.

17.3.2 Security Tester Examples

The following examples illustrate how you can test security setup using the Security Tester screen:

17.3.2.1 Example 1

In this example, you test which actions Joe User has authority for in the Address Book Revisions program (P01051). Joe belongs to the *APCLERK group. Use the following steps to perform the test:

1. Access the Security Tester screen from the Security Workbench by selecting Option 4, for the SAC Security-Action Code Security Type.
2. Enter the following values:
   - User ID = JOEUSER (Joe Users' profile name)
   - Pgm/Form/QG = P01051 (Address Book Revisions)
3. Press the Enter key to test the security authorization. The Security Tester screen displays the following information:

User ID	Name	Program ID	Description	I	A	C	D	F	T
JOEUSER	Joe User	P01051	Address Book Revis	Y	N	N	N	Y	N
*APCLERK	A/P Clerk Group	P01051	Address Book Revis	Y	N	N	N	Y	N
*PUBLIC	All users' group p	*ALL		N	N	N	N	N	N

In this example, Joe User has Inquire (I) and Export (F) authority in the Address Book Revisions program (P01051). No security record is set up for Joe User in the Action Code Security file, and Joe's authority derives from the record set up for the *APCLERK group. A *PUBLIC security record exists, but it is not checked because the group record is found first.

17.3.2.2 Example 2

In this example, you test what actions Sally Manager is authorized for in the program Address Book Revisions (P01051). Sally Manager signs on with role GLSUPR which is associated with groups *APCLERK, *ARCLERK and *GLCLERK.

1. Access the Security Tester screen from the Security Workbench by selecting Option 4, for the SAC Security-Action Code Security Type.
2. Enter the following values:
   - Role = GLSUPR (Security Role for G/l Supervisors)
   - User ID = SALLYMGR (Sally Managers' profile name)
   - Pgm/Form/QG = P01051 (Address Book Revisions)
3. Press the Enter key to test the security authorization. The Security Tester screen displays the following information:

User ID	Name	Program ID	Description	I	A	C	D	F	T
SALLYMGR	Sally Manager	P01051	Address Book Revis	Y	Y	Y	Y	Y	Y
*APCLERK	A/P Clerk Group	P01051	Address Book Revis	Y	N	N	N	Y	N
*ARCLERK	A/R Clerk Group	P01051	Address Book Revis	Y	N	N	N	Y	N
*GLCLERK	G/L Clerk Group	P01051	Address Book Revis	Y	Y	Y	Y	Y	N
*PUBLIC	All users' group p	*ALL		N	N	N	N	N	N

In this example, Sally Manager has access to all actions for the Address Book Revisions program (P01051). No specific security record is set up for Sally in the Action Code Security file, and Sally's authority derives from the records set up for the groups associated with the GLSUPR role. A *PUBLIC security record exists, but it is not checked because a group record for the role is found first.

17.3.3 Wildcard Search

Wildcard search characters can substitute for one or more characters when searching for data in the subfile. Use Configuration Master Setup (P00CFG) on menu G944 option 19 to set up wildcard characters.

For more information, see Chapter 18, "Work with Configuration Master Records" in this guide.

Using wildcards in a search tells the system to search for characters relative to their position in the field. Using wildcard characters will result in an exclusive search as opposed to a subfile reposition.

Wildcard search options include:

- * = Default wildcard search character for zero or many characters
- _ = Default wildcard search character for one and only one character
- | = Default escape wildcard search character. Use the escape wildcard search character to override the wildcard search character to the literal character value.

17.3.3.1 Wildcard Search Examples

These examples illustrate wildcard search options and the records they return:

-
- User/Group = A*: This entry will return all users beginning with A.
- Using 'AN' in the User/Group field repositions the User/Group subfile in alphabetical order starting with AN.
- Using 'AN*' in the User/Group field returns only the User/Group subfile values with A in the first position, N in the second position, then any number of characters after that.
- User/Group = *8: This entry returns all users ending with 8.
- User/Group = *88: This entry returns all users ending with 88.
- User/Group = *8*: This entry returns all user records containing an 8 anywhere in the user ID.
- User/Group = T__1: This entry returns all users beginning with T, then any two characters, then 1 (and no characters after that).
- User/Group = I__253*: This entry returns all users beginning with I, then any two characters, then 253, then any number of characters.
- User/Group = _N*: This entry will return all users beginning with any single character, then N, then any number of characters.
- User/Group = |*AN: This entry repositions the subfile to all users greater than *AN.
- User/Group = PO|_ENTRY: This entry repositions the subfile to all users beginning with or greater than PO_ENTRY.

17.3.4 Detail Column

The Details column changes based on the security type. The column headings for each security type are as follows:

- GU Group/Users
  - None
- IM Initial Menu
  - None
- IP Initial Program
  - None
- JDE JDE Environments
  - None
- RG Role/Group
  - None

- RL Role\Library List
  - None
- RU Role/User
  - None
- SABU Security - Advanced Bus. Unit
  - None
- SAC Security - Action Code
  - None
- GU Group / Users
  - I = Allow Inquire Y/N
  - A = Allow Add Y/N
  - C = Allow Change Y/N
  - D = Allow Delete Y/N
  - F = Allow From Y/N (Import)
  - T = Allow To Y/N (Export)
- SAM Security - Advanced Menu
  - None
- GU Group / Users
  - Sy Cd = System Code
  - Mnu Sel = Menu Selection
  - Auth = Authorized Y/N
- SBA Security - Batch Approval
  - None
- SBU Security - Business Unit
  - Bus. Unit From = Beginning Business Unit in Range
  - Bus. Unit Thru = Ending Business Unit in Range (shown in fold)
- SFFL Security - File/Field
  - Field Name = File Field Name
  - Alw D = Allow Display Y/N
  - Alw U = Allow Update Y/N
- SFK Security - Function Keys
  - Field Name = Field Name for Function Key
  - Alw Use = Allow Use Y/N
- SFP Security - Fast Path
  - Allow Fast Path = Allow Fast Path Command Y/N
- SGT Security - Generic Text
  - Sy Cd = System Code

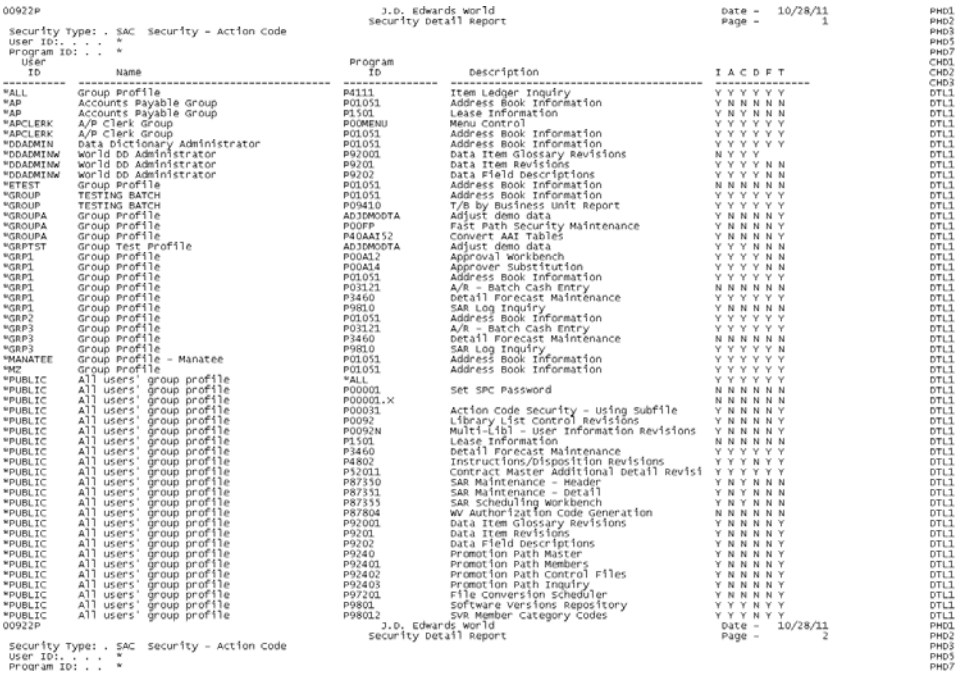
  - Inq = Allow Inquiry Y/N
  - Upd = Allow Update Y/N
- SM Security - Menu
  - A = Authorization Mask
  - J = Job Mask
  - K = Knowledge Mask
  - DP = Department Mask
  - F = Future Use Mask
- SNS Security - Name Search
  - I = Allow Inquire Y/N
  - A = Allow Add Y/N
  - C = Allow Change Y/N
  - D = Allow Delete Y/N
- SUDC Security - UDC
  - UDC Code = User Defined Code or *ALL
  - Auth = Update Authorized Y/N
- SVA Sleeper Versions
  - Sy Cd = System Code
  - Object Library = Library
- USER User Information
  - MT = Menu Travel Allowed Y/N
  - CE = Command Entry Allowed Y/N
  - DL = Menu Display Level
  - AM = Advanced Menu Security Activated for This User Y/N
  - BU = Advanced Bus Unit Security Activated for This User Y/N
- VODW Version Owned - DW
  - Version ID = DREAM Writer Version ID
  - EX = User Exclusive Flag
- VOF Version Owned - FASTR
  - Version ID = FASTR Version ID
  - EX = User Exclusive Flag
- VOS Version Owned - STAR
  - Version ID = STAR Version ID
  - EX = User Exclusive Flag
- VOWW Version Owned - WW
  - Version ID = World Writer Version ID
  - EX = User Exclusive Flag

- VSDW Version Security - DW Report
  - Exec Auth = Allow Execute Y/N
  - A = Allow Add Y/N
  - C = Allow Change Y/N
  - D = Allow Delete Y/N
  - U = Allow Update Y/N
- VSF Version Security - FASTR Reprt
  - Exec Auth = Allow Execute Y/N
  - A = Allow Add Y/N
  - C = Allow Change Y/N
  - D = Allow Delete Y/N
  - U = Allow Update Y/N
- VSS Version Security - STAR Report
  - Exec Auth = Allow Execute Y/N
  - A = Allow Add Y/N
  - C = Allow Change Y/N
  - D = Allow Delete Y/N
  - U = Allow Update Y/N
- VSWW Version Security - WW Report
  - Exec Auth = Allow Execute Y/N
  - A = Allow Add Y/N
  - C = Allow Change Y/N
  - D = Allow Delete Y/N
  - U = Allow Update Y/N

17.4 Understanding the Security Detail Report

The Security Detail Report program generates a printed report of your security setup. The Security Detail report is based on the Security Workbench program (P00922). The processing options for the report provide the same flexible inquiry capability that the Security Workbench program provides.

Figure 17–3 Security Detail Report



```
00922P                          J.D. Edwards World                    Date -  10/28/11   PHD1
                                Security Detail Report                Page -        1   PHD2
 Security Type: . SAC  Security - Action Code                                           PHD3
 User ID:. . . .  *                                                                     PHD5
 Program ID: . .  *                                                                     PHD7
   User                                Program                                          CHD1
     ID          Name                    ID      Description                I A C D F T   CHD2
----------  ------------------------------  ----------  -------------------------  ---------  CHD3
*ALL        Group Profile                   P4111       Item Ledger Inquiry        Y Y Y Y Y Y  DTL1
*AP         Accounts Payable Group          P01051      Address Book Information   Y N N N N N  DTL1
*AP         Accounts Payable Group          P1501       Lease Information          Y N Y N N N  DTL1
*APCLERK    A/P Clerk Group                 P00MENU     Menu Control               Y Y Y Y Y Y  DTL1
*APCLERK    A/P Clerk Group                 P01051      Address Book Information   Y Y Y Y Y Y  DTL1
*DDADMIN    Data Dictionary Administrator   P01051      Address Book Information   Y Y Y Y Y Y  DTL1
*DDADMINW   World DD Administrator          P92001      Data Item Glossary Revisions N Y Y Y   DTL1
*DDADMINW   World DD Administrator          P9201       Data Item Revisions        Y Y Y Y N N  DTL1
*DDADMINW   World DD Administrator          P9202       Data Field Descriptions    Y Y Y Y N N  DTL1
*ETEST      Group Profile                   P01051      Address Book Information   N N N N N N  DTL1
*GROUP      TESTING BATCH                   P01051      Address Book Information   Y Y Y Y Y Y  DTL1
*GROUP      TESTING BATCH                   P09410      T/B By Business Unit Report Y Y Y Y Y Y  DTL1
*GROUPA     Group Profile                   ADJDMODTA   Adjust demo data           Y N N N N Y  DTL1
*GROUPA     Group Profile                   P00FP       Fast Path Security Maintenance Y N N N N Y  DTL1
*GROUPA     Group Profile                   P40AAI52    Convert AAI Tables         Y N N N N Y  DTL1
*GRPTST     Group Test Profile              ADJDMODTA   Adjust demo data           Y Y Y N N N  DTL1
*GRP1       Group Profile                   P00A12      Approval Workbench         Y Y Y Y N N  DTL1
*GRP1       Group Profile                   P00A14      Approver Substitution      Y Y Y Y N N  DTL1
*GRP1       Group Profile                   P01051      Address Book Information   Y Y Y Y Y Y  DTL1
*GRP1       Group Profile                   P03121      A/R - Batch Cash Entry     N N N N N N  DTL1
*GRP1       Group Profile                   P3460       Detail Forecast Maintenance Y Y Y Y Y Y  DTL1
*GRP1       Group Profile                   P9810       SAR Log Inquiry            Y N N N N N  DTL1
*GRP2       Group Profile                   P01051      Address Book Information   Y Y Y Y Y Y  DTL1
*GRP3       Group Profile                   P03121      A/R - Batch Cash Entry     Y Y Y Y Y Y  DTL1
*GRP3       Group Profile                   P3460       Detail Forecast Maintenance N N N N N N  DTL1
*GRP3       Group Profile                   P9810       SAR Log Inquiry            Y Y Y Y Y N  DTL1
*MANATEE    Group Profile - Manatee         P01051      Address Book Information   Y Y Y Y Y Y  DTL1
*MZ         Group Profile                   P01051      Address Book Information   Y Y Y Y Y Y  DTL1
*PUBLIC     All users' group profile        *ALL                                   Y Y Y Y Y Y  DTL1
*PUBLIC     All users' group profile        P00001      Set SPC Password           N N N N N N  DTL1
*PUBLIC     All users' group profile        P00001.X                               N N N N N N  DTL1
*PUBLIC     All users' group profile        P00031      Action Code Security - Using Subfile Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P0092       Library List Control Revisions Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P0092N      Multi-Libl - User Information Revisions Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P1501       Lease Information          N N N N N N  DTL1
*PUBLIC     All users' group profile        P3460       Detail Forecast Maintenance Y Y Y Y Y Y  DTL1
*PUBLIC     All users' group profile        P4802       Instructions/Disposition Revisions Y Y Y N Y Y  DTL1
*PUBLIC     All users' group profile        P52011      Contract Master Additional Detail Revisi Y Y Y Y Y Y  DTL1
*PUBLIC     All users' group profile        P87330      SAR Maintenance - Header   Y N Y N N N  DTL1
*PUBLIC     All users' group profile        P87331      SAR Maintenance - Detail   Y N Y N N N  DTL1
*PUBLIC     All users' group profile        P87335      SAR Scheduling Workbench   Y N Y N N N  DTL1
*PUBLIC     All users' group profile        P87804      WV Authorization Code Generation N N N N N N  DTL1
*PUBLIC     All users' group profile        P92001      Data Item Glossary Revisions Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P9201       Data Item Revisions        Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P9202       Data Field Descriptions    Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P9240       Promotion Path Master      Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P92401      Promotion Path Members     Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P92402      Promotion Path Control Files Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P92403      Promotion Path Inquiry     Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P97201      File Conversion Scheduler  Y N N N N Y  DTL1
*PUBLIC     All users' group profile        P9801       Software Versions Repository Y Y Y N Y Y  DTL1
*PUBLIC     All users' group profile        P98012      SVR Member Category Codes  Y Y Y N Y Y  DTL1
00922P                          J.D. Edwards World                    Date -  10/28/11   PHD1
                                Security Detail Report                Page -        2   PHD2
 Security Type: . SAC  Security - Action Code                                           PHD3
 User ID:. . . .  *                                                                     PHD5
 Program ID: . .  *                                                                     PHD7
```

The Security Workbench program contains a number of features. Like the Security Workbench program, the Security Detail report has many features to support its function as a single access point for generating security setup lists. For example, depending on the security type for which you creating the report, the header portion of the report adjusts the display for the selected security type. A special Details column on the right side of the report displays a variety of information including details that are relevant to the selected security type.

Use the Security Detail Report program to run a report for all major security types, such as user profiles, menu security, action code security, abd function key security. The report adjusts the display of fields based on which security type you are currently viewing.

You can generate this report directly from the Security Workbench screen using the Print function key (F21). If you run the report from the Print function key, the report displays the current subfile from the Security Workbench screen. For greater flexibility in print options, run the report from DREAM Writer. For example, you can generate the report for all security types at once.

Note: In order to see the report, you will need to do a WRKSPLF after using the F21 utility.

17.4.1 DREAM Writer Considerations

Use the processing options for the DREAM Writer program to set selection criteria for the report.

- Security Type: Use this field to specify which type of security you wish to view or test. The security type controls many aspects of the video. In addition to security, this field can also be used to show report version ownership and user exclusive flags.

- Sequence: Use this field to specify how to print the detail portion of the report. Select ’1’ to list the User/Role/Group object first. Select '2' to list the system object first on the report.
- Security Role: Use this field to specify the security role value to be used for selecting data for the report.Wildcard values are accepted.
- As Of Date: this field to specify the As Of Date to be used for selecting data for the report.
- User ID: Use this field to specify the user ID value to be used for selecting data for the report. Wildcard values are accepted.
- Menu ID: Use this field to specify the menu ID value to be used for selecting data for the report. Wildcard values are accepted.
- Video ID: Use this field to specify the video ID value to be used for selecting data for the report.
- Program/Form/Query Group: Use this field to specify the program ID, form ID or query group value to be used for selecting data for the report.
- Library List: Use this field to specify the library list value to be used for selecting data for the report. Wildcard values are accepted.
- File ID: Use this field to specify the file ID value to be used for selecting data for the report. Wildcard values are accepted.
- Group ID: Use this field to specify the group ID value to be used for selecting data for the report. Wildcard values are accepted.
- Fast Path Code: Use this field to specify the fast path code value to be used for selecting data for the report. Wildcard values are accepted.
- System Code: Use this field to specify the system code value to be used for selecting data for the report. Wildcard values are accepted.
- Version ID: Use this field to specify the version ID value to be used for selecting data for the report. Wildcard values are accepted.

17.4.2 Exporting Security Data from the Security Detail Report

You can export this report to an export file on the Integrated File System (IFS). To export this report, access the Additional Parameters screen in your DREAM Writer Version and press F6 to display the Spooled File Export Parms (P00SPDLP). See the help instructions for that window for more information on how to proceed with exporting the report.

When Export is enabled, the system displays literals that guide the export on the right-hand side of the report. If you want to generate a printed version of the report without these literals, run a DREAM Writer Version with the Export feature disabled.

You are not required to have Printer Overrides set for this report. However, if do you have Printer Overrides for the DREAM Writer version that you use for export, you must set the Maximum Form Width value to 138.

18

Work with Configuration Master Records

This chapter contains the topic:

- Section 18.1, "Working with Configuration Master Records."

18.1 Working with Configuration Master Records

The Configuration Master file (F00CFG) stores configuration information which programs use to determine the program functionality. For example, you can use this program to determine the display of data on the screen or use of a wildcard. You use the Master Configuration Maintenance program (P00CFG) to view, create, change, or delete records from the F00CFG.

This program allows you to configure a program by entering values in the Profile (User Profile), Environment, and Program fields. You also choose a value for the Key field from UDC 00/CK. The X00CFG Server program retrieves a configuration value from the file for a specific Key, User, Environment and Program combination.

You can override the default value of SQL wildcards in programs which allow SQL wildcards in filter fields. Enter the value of SQL_SCRB in the Key field to modify the SQL wildcard.

For example, you can choose the value SQL_SCRB for the value in the Key field to specify the SQL escape and wildcard characters to use on inquiry screens which allow SQL wildcards. This value is a three character string which specifies the search wildcard, single character wildcard, and escape character values to use on the inquiry screen. Default values for these characters can be set up using the *PUBLIC profile, but you can override this value for a specific user by adding an additional record specifying the individual user profile.

When retrieving values from the Configuration Master, the X00CFG server program examines records in the following order:

1. Using the input profile, environment and program.
2. Using the input profile, environment and program = "*ALL".
3. Using the input profile, environment = "*ALL" and program.
4. Using the input profile, environment = "*ALL" and program = "*ALL".
5. Using profile = "*PUBLIC", environment and program.
6. Using profile = "*PUBLIC", environment and program = "*ALL".
7. Using profile = "*PUBLIC", environment "*ALL" and program = program.
8. Using profile = "*PUBLIC", environment = "*ALL" and program = "*ALL".

Working with Configuration Master Records includes the following tasks:

- To create a configuration master record
- To change a configuration master record
- To delete a configuration master record

Navigation

From Advanced & Technical Operations (G9), choose Security & System Admin

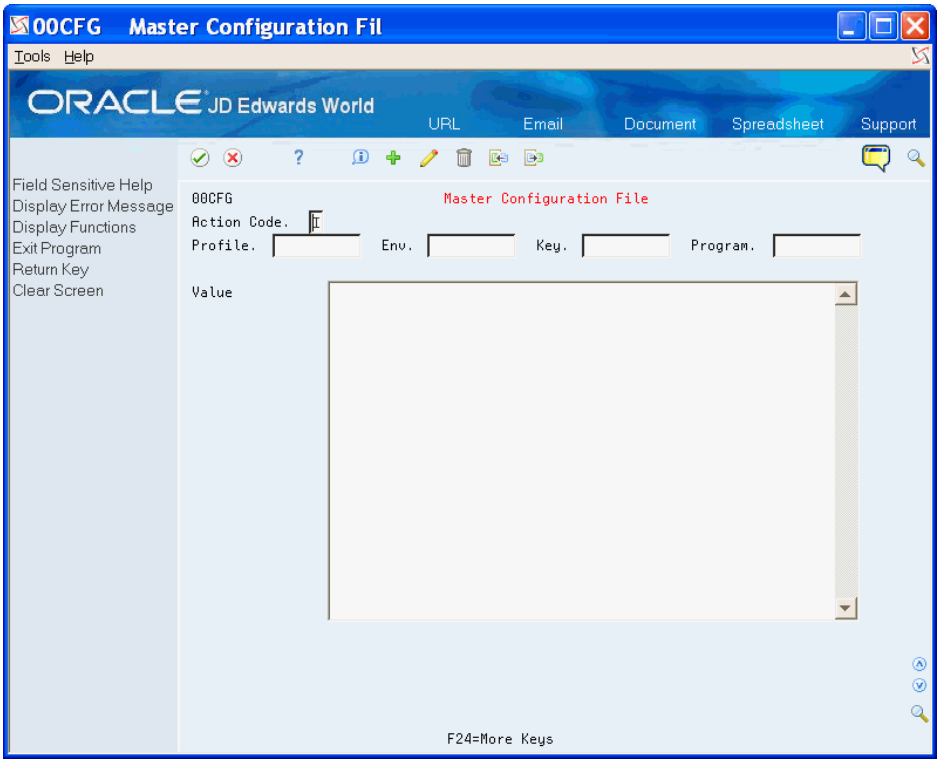
From System Administration (G94), choose Security Administration

From System Administration (G944), choose Master Configuration File

To create a configuration master record

1. On Master Configuration File, complete the following fields and click Add.
   - Profile.
   - Env. (Environment)
   - Key.
   - Program.
   - Value

Figure 18–1 Master Configuration File screen



Field	Explanation
Profile	This is the user profile used in the Configuration Master File (F00CFG). *Screen-Specific Information* This can be a specific user or *PUBLIC to apply to all users.
Environment	Choose the name of a library list. *Screen-Specific Information* This can be a specific environment or *ALL to apply to all environments.
Key	This value is the key value used for retrieving data from the F00CFG file. *Screen-Specific Information*
Program	This is the Program ID used in the Configuration Master File (F00CFG). *Screen-Specific Information* This can be a specific program or *ALL to apply to all programs.
Value	This is the value in the Configuration Master File (F00CFG) for a specified Profile, Environment, Program and Key combination. When retrieving this value from the configuration file, the program will look up the value in the following order: **1.** Using the input profile, environment and program. **2.** Using the input profile, environment and program = "*ALL". **3.** Using the input profile, environment = "*ALL" and program. **4.** Using the input profile, environment = "*ALL" and program = "*ALL". **5.** Using profile = "*PUBLIC", environment and program. **6.** Using profile = "*PUBLIC", environment and program = "*ALL". **7.** Using profile = "*PUBLIC", environment "*ALL" and program = program. **8.** Using profile = "*PUBLIC", environment = "*ALL" and program = "*ALL".

To change a configuration master record

1. On Master Configuration File, change any of the following fields and click Change.
   - Profile.
   - Environment
   - Key.
   - Program.
   - Value

To delete a configuration master record

1. On Master Configuration File, locate the record that you want to delete.
2. Click Delete.

19

Security Reporting

This chapter contains these topics:

- Section 19.1, "General Guidelines,"
- Section 19.2, "Configuring and Using User Activity Reporting,"
- Section 19.3, "Configuring and Using Database Audit Manager,"
- Section 19.4, "Configuring and Using Segregation of Duties Reports,"

19.1 General Guidelines

Several reports and inquiries are available to help security administrators understand whether the authorizations and access controls in place are effectively protecting the JD Edwards World environment. Use the following general guidelines when devising a self- auditing strategy:

Keep Audited Information Manageable

Although self-auditing is relatively inexpensive, you should limit the number of audited events as much as possible. Two log files are available for capturing user activity: the Menu Selection History file (F0082H) and the User Job Activity Log (F009250). Both of these files grow rapidly when logging is turned on. In addition, the Database Audit Manager (DBAM) facility is available to track additions, changes, and deletions on selected files. Limiting the periods in which logging is turned on minimizes the performance effect on the processing of audited statements and the size of the audit trail, making it easier to analyze and understand.

Evaluate the Purpose for Auditing

After you have a clear understanding of the reasons for auditing, you can devise an appropriate auditing strategy and avoid unnecessary auditing. For example, suppose you are auditing to investigate suspicious database activity. This information by itself is not specific enough. What types of suspicious database activity do you suspect or have you noticed? Perhaps you could use DBAM to track one or two files. Another focused auditing purpose might be to audit unauthorized deletions from arbitrary tables in the database. This purpose narrows the type of action being audited and the type of object being affected by the suspicious activity.

Audit Knowledgeably

Audit the minimum number of statements, users, or objects required to get the targeted information. This prevents unnecessary audit information from cluttering the meaningful information and consuming valuable space in your system. Balance your need to gather sufficient security information with your ability to store and process it.

For example, if you are auditing to gather information about database activity, then determine exactly what types of activities you want to track. Audit only the activities of interest and audit only for the amount of time necessary to gather the information that you need.

19.2 Configuring and Using User Activity Reporting

Beginning with JD Edwards World release A9.2, a facility called user activity reporting is available to support self-auditing. Three types of information may be monitored: user activity, menu selection history, and file update activity. All three reports display totals by user license type as defined for users in the User License Type file (F00925). You set the user license type file to categorize users in a way that helps you self-determine compliance with your software license. These reports cannot determine compliance; that determination must be done by analyzing your actual software license document.

Monitor User Activity

The primary purpose of the User Activity Summary Report (R009253P) is to capture and report the level of user activity in a given period, called a collection period. The average and peak volumes for user session and users signed on can be monitored. To run this report, you first set up definitions for the collection periods and run them using Unattended Night operations (Sleeper). After the collection periods have run and the information is collected, you may run the report.

Monitor Menu Selection History

The Menu History Summary Report (R009254P) reports the menu selections taken by users during the defined collection periods. The report displays the number of times each menu selection is processed, as well as the system code the menu selection belongs to and the user license type.

Monitor File Update Activity

The File Update Activity Summary Report (R009255P) reports the number of instances in which a user appears in the audit information for selected files. This information is meant as a quick way to monitor file update activity, but it does not provide a complete audit trail of file update activity because the file audit information only tracks the user ID of the user who last updated the record, not all users who have updated a record. Use the DBAM facility if you want a complete audit trail. The report displays the number of times the user's ID appears in the selected files, as well as the system code the file belongs to and the user license type.

19.3 Configuring and Using Database Audit Manager

As described in the previous section, User Activity Reporting has a quick method of checking for appropriate file update activity, but it does not provide a complete audit trail. Database Audit Manager (DBAM) is a user-configured audit tool that can track all database transactions you are interested in. Additionally, DBAM provides the ability to require an electronic signature (password) authentication for sensitive transactions.

Set up Audit Configuration Defaults

To configure DBAM, you first set up the system-level defaults for monitoring activity. These are the system locations for the audited files and their source. You should locate the activity logs here.

Set up Files and Fields to Track

You use the Audit Manager Workbench video (V98200) to configure individual database audit configuration records and activate monitoring activity. Each audit configuration record is then configured with a list of files and fields to track. You can also set up audit definition parameters, such as whether electronic signature and change reason codes will be required. Depending on the application, you can set up electronic signature at the record level or transaction (multiple records) level.

Review Database File Triggers

DBAM uses database file triggers. When defining a new DBAM audit configuration, you should review what other file triggers may be in place.

Review Database Audit Logs

After you set up DBAM auditing for a file, you build your own queries over the DBAM audit log files to analyze the file update activity. You can use World Writer to build these queries.

19.4 Configuring and Using Segregation of Duties Reports

The Sarbanes-Oxley Act raised the level of awareness for many types of security issues, among them problems with conflicts of interest in user's assigned responsibilities. The control principle used to resolve the conflicts of interest is called segregation of duties. When segregation of duties is not properly enforced, segregation of duties conflicts result. These are monitored using the segregation of duties reports.

Set up Process Definitions

The first step in determining segregation of duties conflicts is to define the system tasks that make up a particular business activity, called a process. Process definitions may be a single program, function key exit, or selection exit or may include multiple programs. Processes may be embedded within one another, allowing you to modularize the definitions into reusable elements.

Set up Conflict Definitions

The second step in determining segregation of duties conflicts is to define the business processes that together raise a conflict of interest. For example, the user responsible for printing accounts payable checks should not also be the person who sets up new vendors and approves payables invoices. Conflict definitions may be set up at the function key/selection option level, the program level, or the business process level.

Report Segregation of Duties Conflicts

After process definitions and conflicts definitions are in place, the system may then look at user authority and report on users who have authority to system resources that represent a segregation of duties conflict. The report is the Segregation of Duties Conflicts report (R00713). When you determine that a segregation of duties conflict exists, you may then make the appropriate changes in your security setup (and user's responsibilities, as appropriate) to remove the conflict.

Part IV

JD Edwards World Developer Security

This section provides information useful to developers who produce applications using the JD Edwards World product as a platform.

This part contains the following chapters:

- Chapter 20, "Development Environments"
- Chapter 21, "Application Security Policies"
- Chapter 22, "Object Security Policies"

20

Development Environments

This chapter contains these topics:

- Section 20.1, "Developer Access,"
- Section 20.2, "Libraries,"
- Section 20.3, "Program Source,"

20.1 Developer Access

Developers should not have access to production objects. Policies controlling promotion of development programs to the production environment should be in place. Only authorized and tested program object changes should be promoted to production environments.

20.2 Libraries

When customizing your JD Edwards World Environments, consider the libraries you will use. You should keep all customization objects in libraries that are separate from the delivered JD Edwards World object libraries, and you should use library lists to control access.

20.3 Program Source

All program source, whether provided by JD Edwards or your own custom source, should be restricted from general user access. Source code should not reside in production environments.

21

Application Security Policies

In addition to policies that control the development environment, you should implement policies regarding secure application development by design.

This chapter contains these topics:

- Section 21.1, "Menu Security,"
- Section 21.2, "Action Code Security,"
- Section 21.3, "Function Key Security,"
- Section 21.4, "Video Design,"
- Section 21.5, "DREAM Writer,"
- Section 21.6, "Data Dictionary and User Defined Codes,"
- Section 21.7, "File Audit Fields,"
- Section 21.8, "User Authentication,"

21.1 Menu Security

When adding menus or menu selections in the JD Edwards World system, you should consider how you will secure user access to the menu or selection. Group menu selections with similar functionality on the same menu so that you will be able to secure entire menus rather than menu selections. Use the more secure Advanced Operations (Gxx31) and Set Up (Gxx41) menus with higher Menu Level values to contain menu selections that should be restricted.

21.2 Action Code Security

If you add your own customized programs to the JD Edwards World environment, your programs should check Action Code Security to determine whether users have access to the program and what actions they may perform.

21.3 Function Key Security

If you add your own customized programs to the JD Edwards World environment, your programs should also check Function Key Security to determine whether users have access to the program and what function keys and selection exits they may run.

21.4 Video Design

If you add your own customized interactive programs to the JD Edwards World environment, your videos should be designed with security in mind. Do not display sensitive information in videos that a wide population of users will need to access. Do not add file update capabilities to videos that should be used as "inquiry only" by most users.

21.5 DREAM Writer

If you add your own customized reports to the JD Edwards World environment, your reports should be built to run via the DREAM Writer interface to take advantage of the security and flexibility provided by DREAM Writer.

21.6 Data Dictionary and User Defined Codes

If you add your own customized programs that accept user input through either batch or interactive means, you should consider all user input "untrusted" until it is edited against pre-determined values. Use the JD Edwards Data Dictionary and User Defined Codes to avoid hard-coded program edits.

21.7 File Audit Fields

If you add your own customized files, include at a minimum the following audit fields, where xx represents the file prefix:

- xxPID Program ID
- xxJOBN Work Station ID
- xxUSER Last Updated by User ID
- xxUPMJ Date Last Updated
- xxUPMT Time Last Updated
- xxTORG Transaction Originator User ID
- xxUPAJ Date Added
- xxTENT Time Entered

After these audit fields are added, they may appear in interactive programs using the common utility program P0045 - Display Audit Information. Note that these fields only provide the origination and "last touched" information; they do not provide a complete audit trail. Use Database Audit Manager (DBAM) if you need a complete audit trail.

21.8 User Authentication

Use the electronic signature feature of DBAM to require user authentication within the JD Edwards World application. This is done for sensitive transactions that require enhanced authentication. JD Edwards World applications must be enabled for electronic signature in the transaction entry or modification program. Applications enabled for electronic signature include:

- P3002 Bill of Material Revisions
- P3003 Routing Master Revisions

- P3013 ECO Parts List
- P30225 ECO Workbench
- P41080 Lots by Item
- P4818 Order Approval

22

Object Security Policies

Application security only protects information assets for users operating within the application. Without object level security in place, users could bypass application security by accessing data directly, without going into the application. Software tools like Query/400, JDBC, and SQL can be used for this purpose if not restricted.

This chapter contains these topics:

- Section 22.1, "File Objects,"
- Section 22.2, "Program Objects,"
- Section 22.3, "Adopted Authority,"

22.1 File Objects

Oracle recommends that applications use the security enforcement mechanisms of the IBM i database as far as possible because this security cannot be bypassed. Set up authorization at the library level rather than individual file object level, where practical, to reduce the security administration workload.

22.2 Program Objects

Protect program objects from unauthorized recompilation by securing and/or removing source code from production systems, and by controlling the promotion path for changed programs. You should restrict programs that perform massive or risky updates from general user access.

22.3 Adopted Authority

Use program objects to securely perform tasks that users are not normally allowed to do. Use adopted authority to allow users to perform tasks that should be controlled via a program versus giving users authority via their user profile authority.

Part V

Appendices

This part contains these appendices:

- Appendix A, "Secure Deployment Checklist"
- Appendix B, "Example of Setting a Field with Field Level Masking"
- Appendix C, "IBM Authorization Lists – Object Authority Information"

A

Secure Deployment Checklist

This appendix contains the topic:

- Appendix A.1, "About Secure Deployment Checklist"

A.1 About Secure Deployment Checklist

The following security checklist includes guidelines that help secure your database:

1. Install only what is required.
2. Disable default user accounts.
3. Enforce password management.
4. Enable data dictionary protection.
5. Practice the principle of least privilege.
   - Grant necessary privileges only.
   - Revoke unnecessary privileges from the *PUBLIC user group.
   - Restrict permissions on run-time facilities.
6. Enforce access controls effectively and authenticate clients stringently.
7. Restrict network access.
   - Use a firewall.
   - Never poke a hole through a firewall.
   - Monitor who accesses your systems.
   - Check network IP addresses.
   - Encrypt network traffic.
   - Harden the operating system.

B

Example of Setting a Field with Field Level Masking

This appendix contains these topics:

- Section B.1, "Proof of Field Level Masking Set,"
- Section B.2, "Test the Masking Field on a Screen and a Report."

The following section contains the steps necessary for the Field Level Masking application programs to set a masking on the ABTAX field in file F0101 Address Book in library FLSTEST.

Navigation

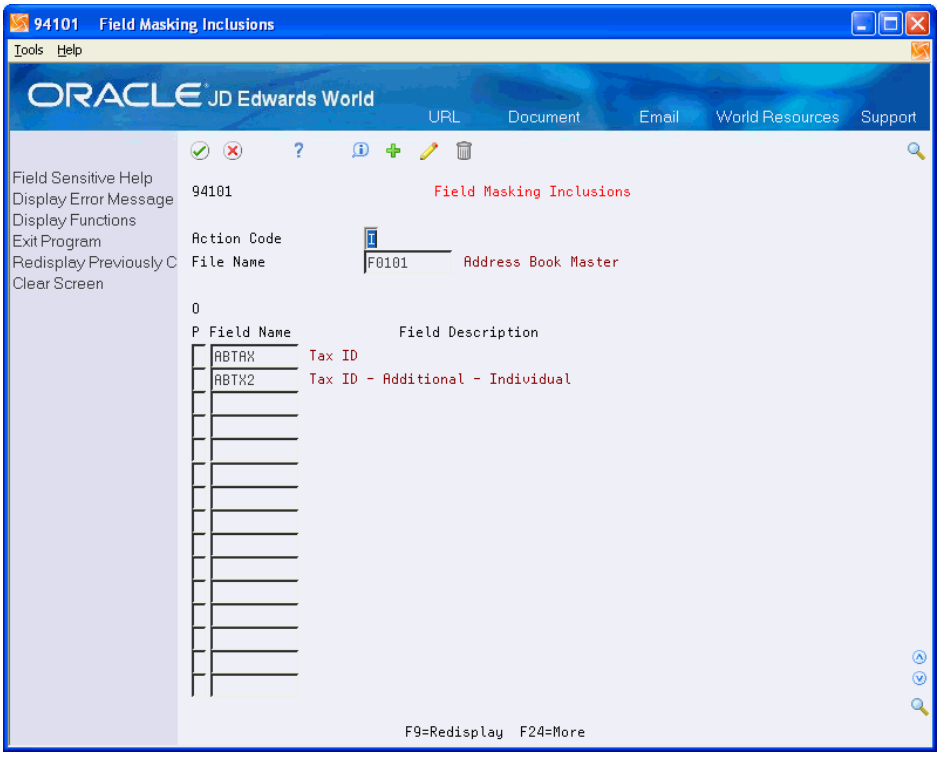
From Master Directory (G), access menu G941 Field Masking Security

To set a masking on the ABTAX field in file F0101 Address Book in library FLSTEST

1. On Field Level Masking (G941), choose Field Security Masking (P94101).
2. Ensure that the field ABTAX in the F0101 Address Book file is included in the F94101 Field Masking Inclusions file.

   To confirm ABTAX field is included in the F94101 Field Masking Inclusions file, inquire on File Name F0101.

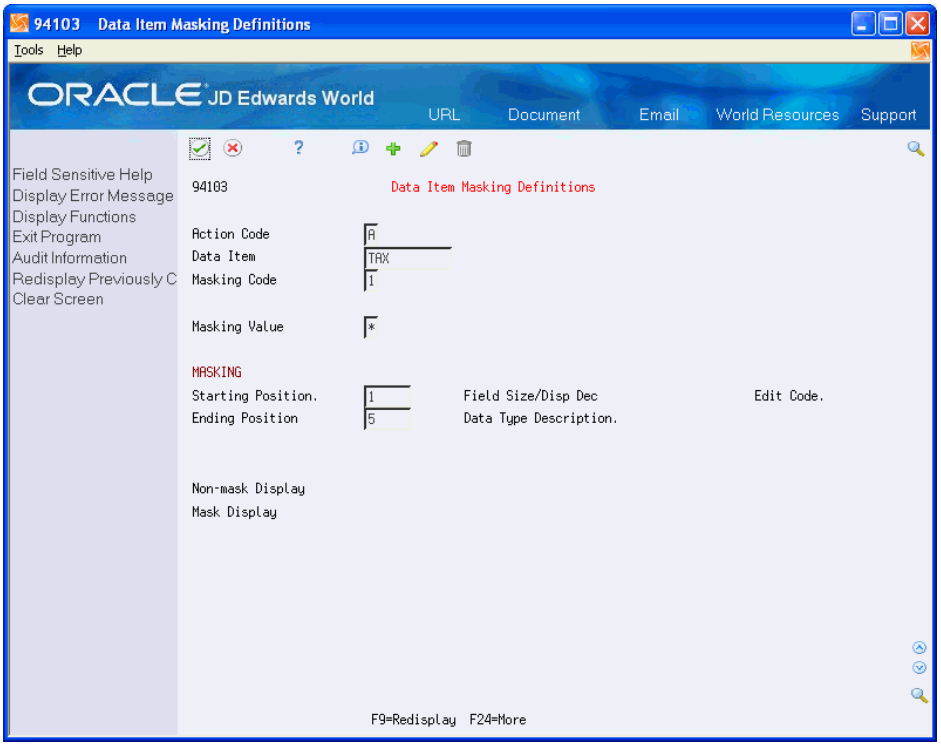
Figure B–1 Field Masking Inclusions screen



Note that ABTAX is an included field in file F0101 and can be used to mask within Field Level Masking.

3. On Field Level Masking (G941), choose Data Item Masking Definitions (P94102).

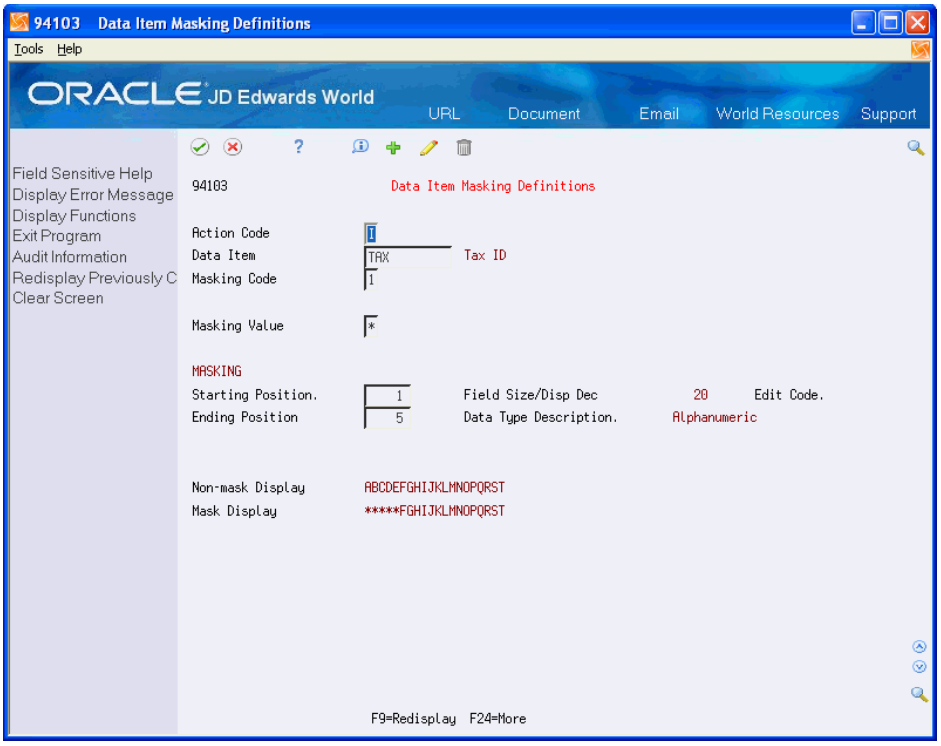
Figure B–2 Data Item Masking Definitions screen



Add a Masking Code for Data Item TAX. The Masking Value of '*' will replace the first 5 positions of the TAX field.

4. Press Enter to add the Masking Definition.
5. Press F9 to Redisplay the Masking Definition added.

Figure B–3 Data Item Masking Definitions screen

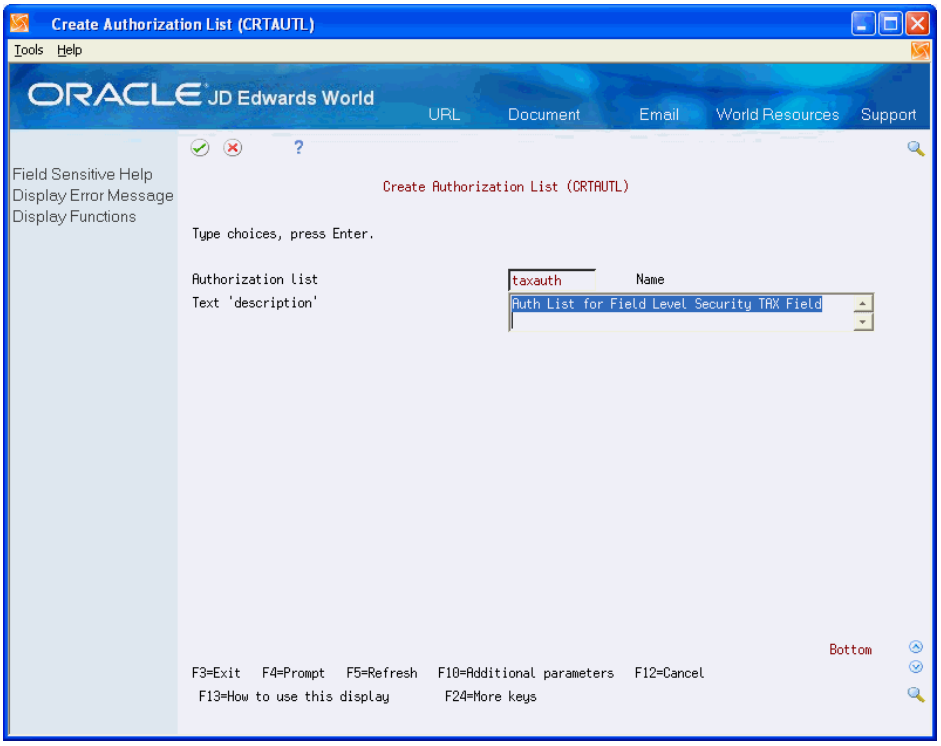


Note that the fields Field Size/Disp Dec displays 20 and Data Type Description displays Alphanumeric for the TAX Data Item from the Data Dictionary. The Non-mask Display and Mask Display fields demonstrate how the value is presented when unmasked or masked.

6. After setting up the Masking Definition for the TAX Data Item, you must create the Database Field Level Security record.
   - First, establish the IBM Authorization List, which is going to be used on the field to be masked.
   - From the command line, type the following command:

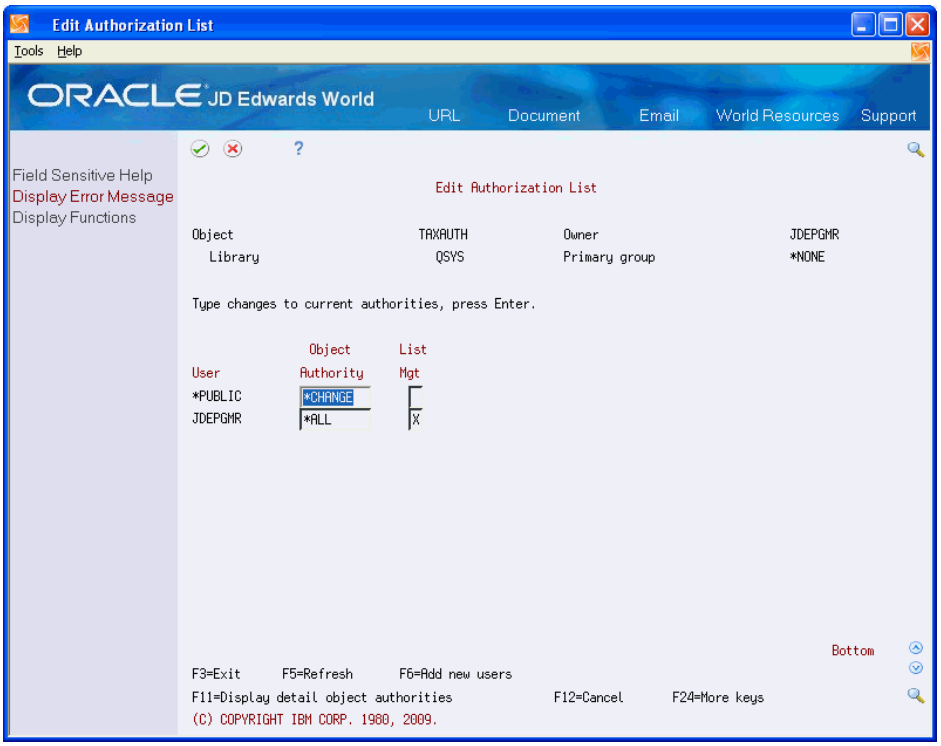
     CRTAUTL
   - Press F4 to access the Create Authorization List screen. In this example, we will use the IBM Authorization List TAXAUTH.
   - Press Enter to create the IBM Authorization List.

Figure B–4 Create Authorization List screen



7. Type the command EDTAUTL TAXAUTH to edit the Authorization List.

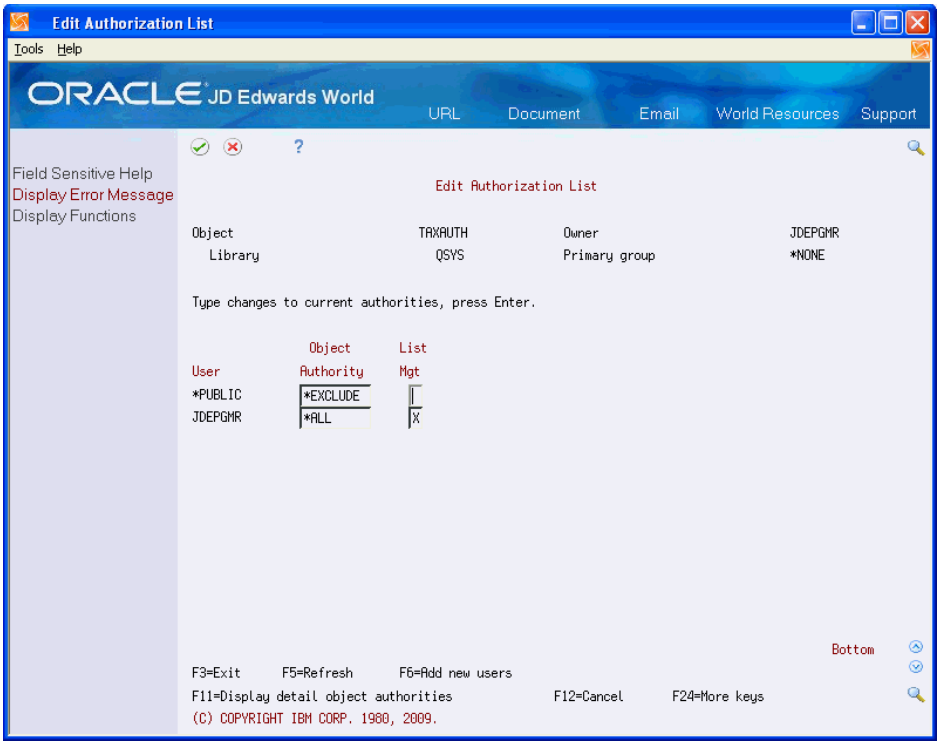
Figure B–5 Edit Authorization List screen



In this example, the Authorization List Owner, JDEPGMR has *ALL Object Authority. All other users, through *PUBLIC, have *CHANGE rights.

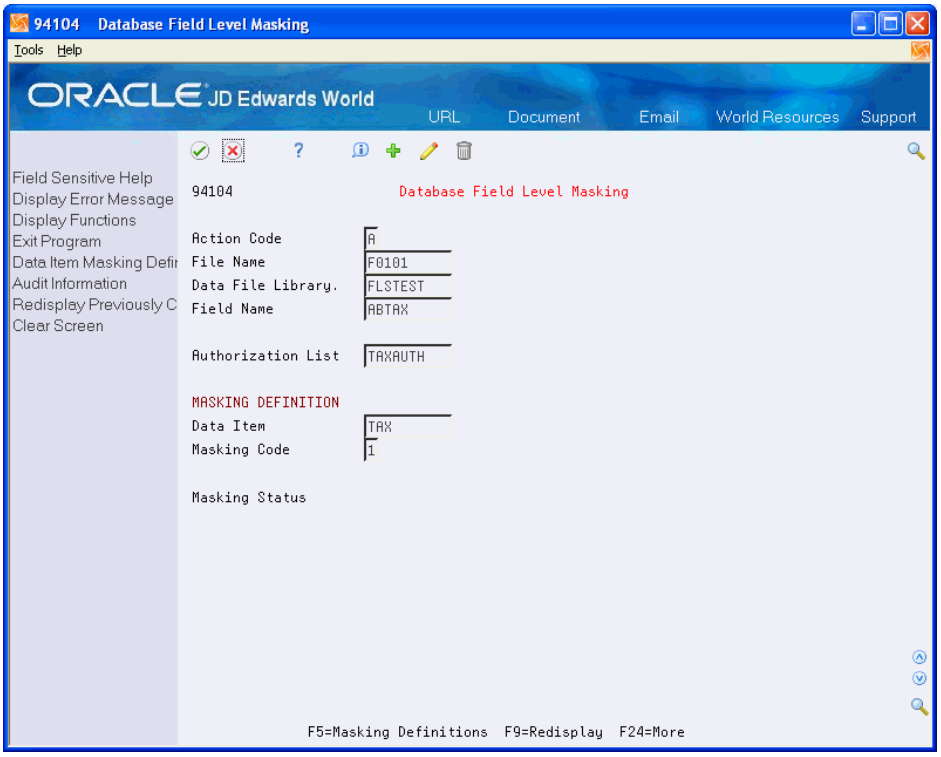
To set up field masking for users not in group profile JDEPGMR, change *PUBLIC rights to *EXCLUDE and then press Enter.

Figure B–6 Edit Authorization List screen



8. On Field Level Security (G941), choose Database Field Level Security (P94104).

Figure B–7 Database Field Level Masking screen



To add a Database Field Level Masking (F94104) record the Field Masking Inclusions and the Data Item Masking Definitions records must exist first. Using the records we created in previous steps, complete the fields as follows:

File Name F0101

Data File Library FLSTEST

Field NameABTAX

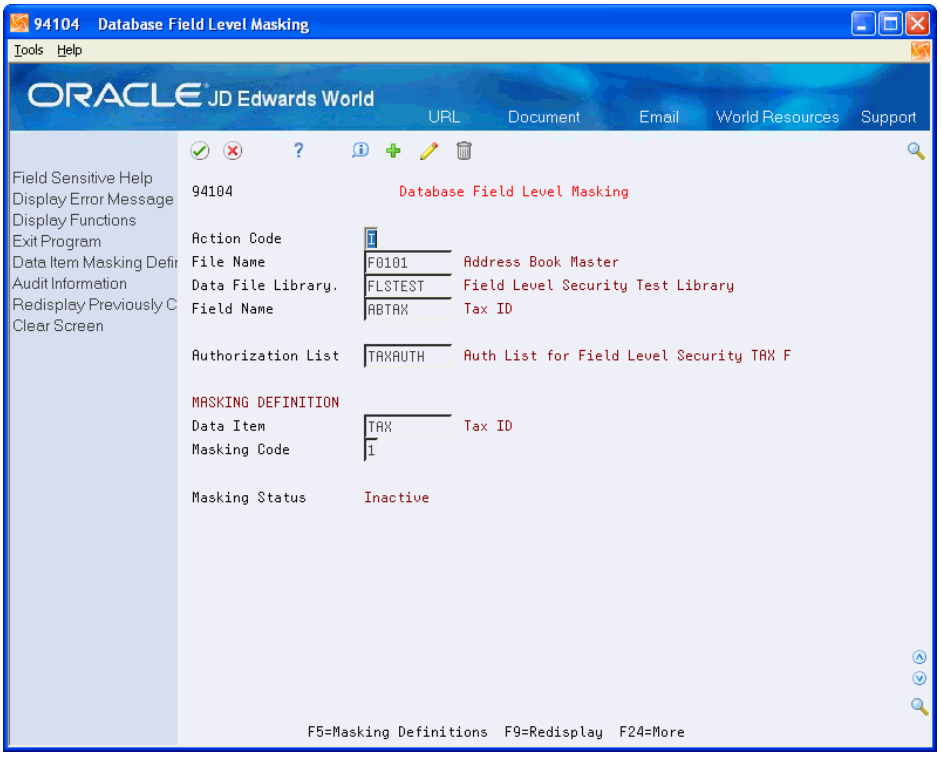
Authorization List TAXAUTH

Data ItemTAX

Masking Code11.

9. Press Enter to add the record and then press F9 to Redisplay the record.

Figure B–8 Database Field Level Masking screen

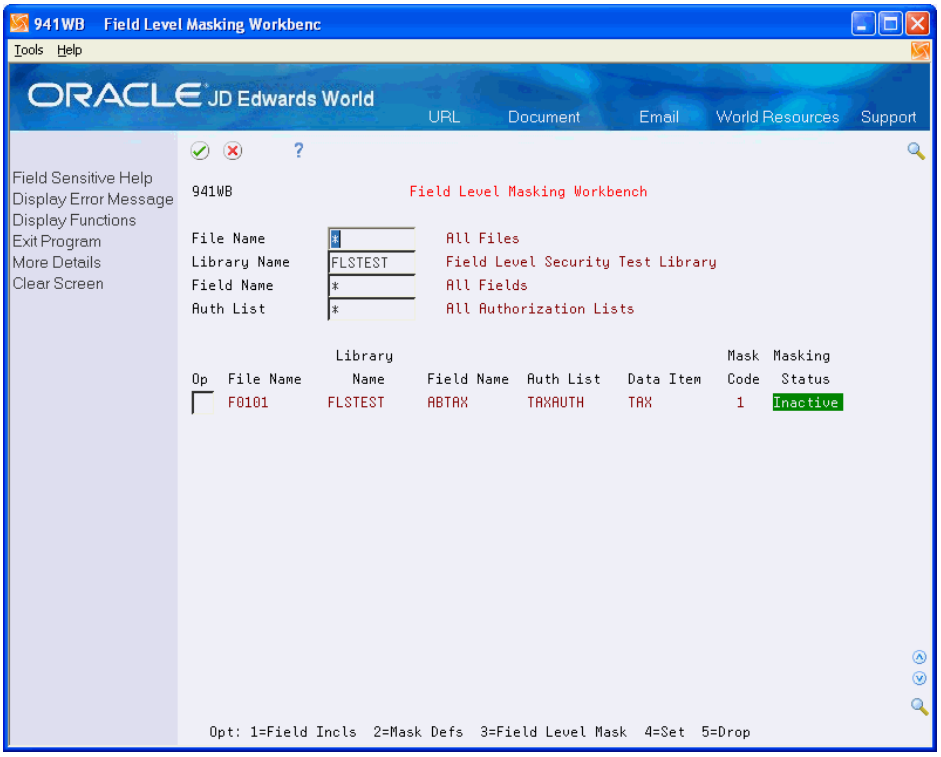


Notice that the Masking Status displays as Inactive since the Field Level Masking has not been Set for the ABTAX field in the file and library combination.

10. On Field Level Masking (G941), choose Field Level Masking Workbench (P98XWB).

Enter Library Name FLSTEST in the filter field and then press Enter.

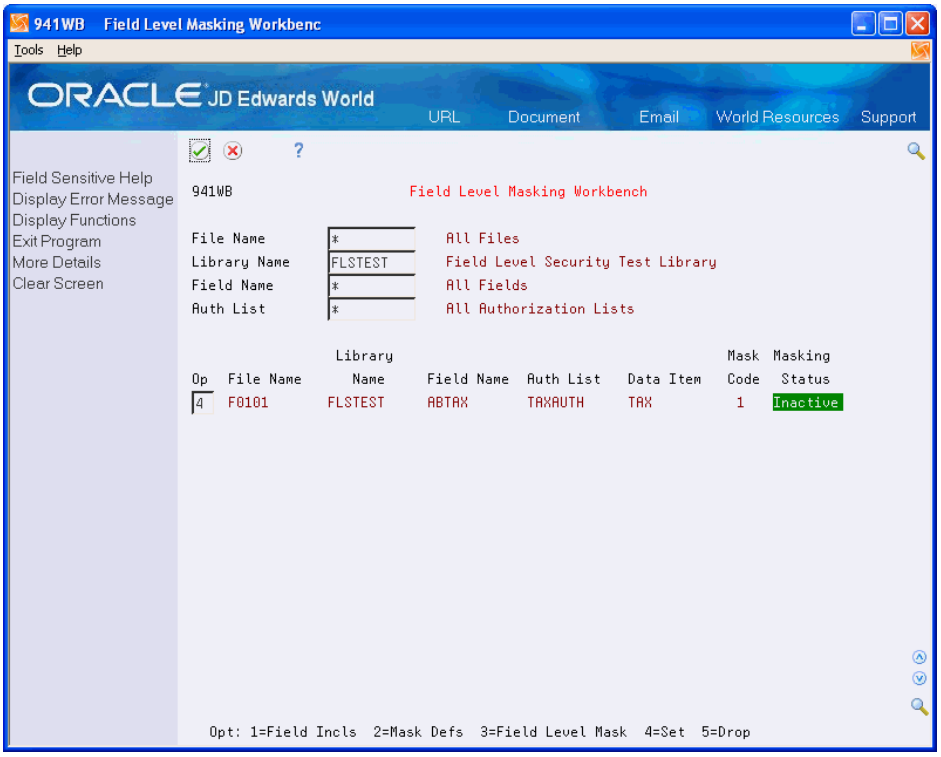
Figure B–9 Field Level Masking Workbench screen



The F94104 record for the ABTAX field in file F0101 and library FLSTEST displays in the list with a Masking Status of Inactive.

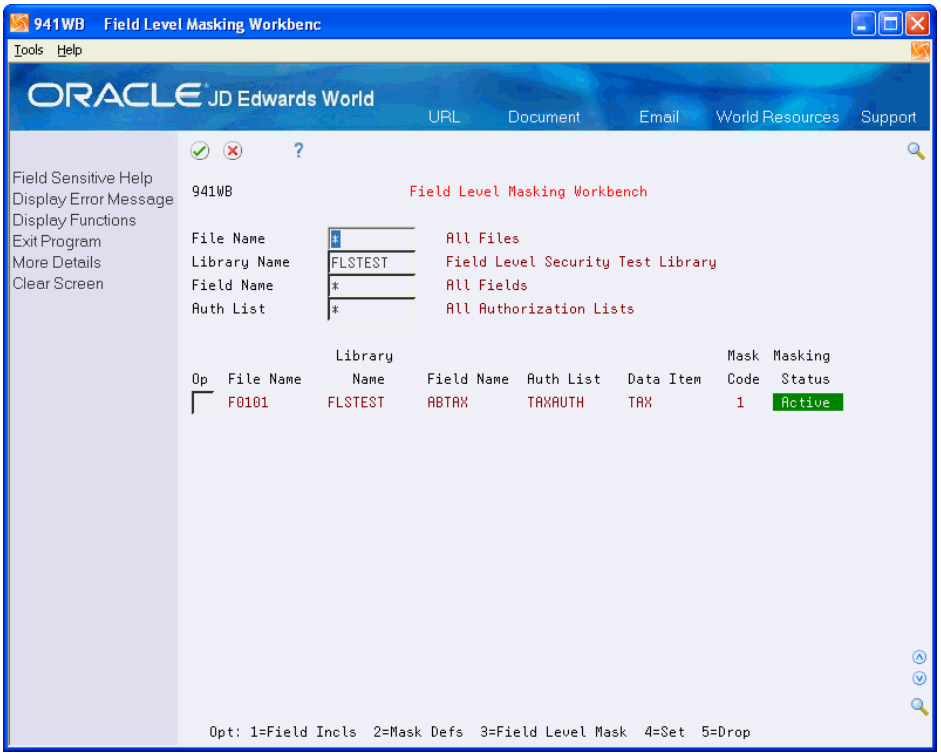
11. Set masking on this ABTAX field in the file and library, using selection Option 4 (Set) and then press Enter.

Figure B–10 Field Level Masking Workbench screen



12. The following graphic displays the result of setting the Field Level Masking, status is Active.

Figure B–11 Field Level Masking Workbench screen

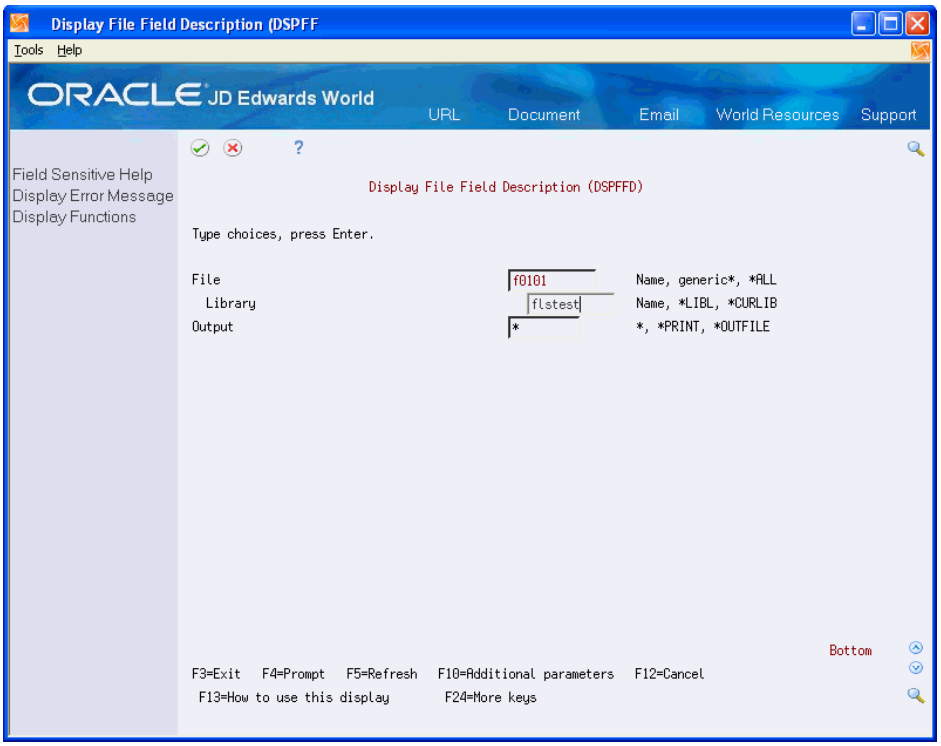


B.1 Proof of Field Level Masking Set

To prove Field Level Masking was successfully set on the ABTAX field

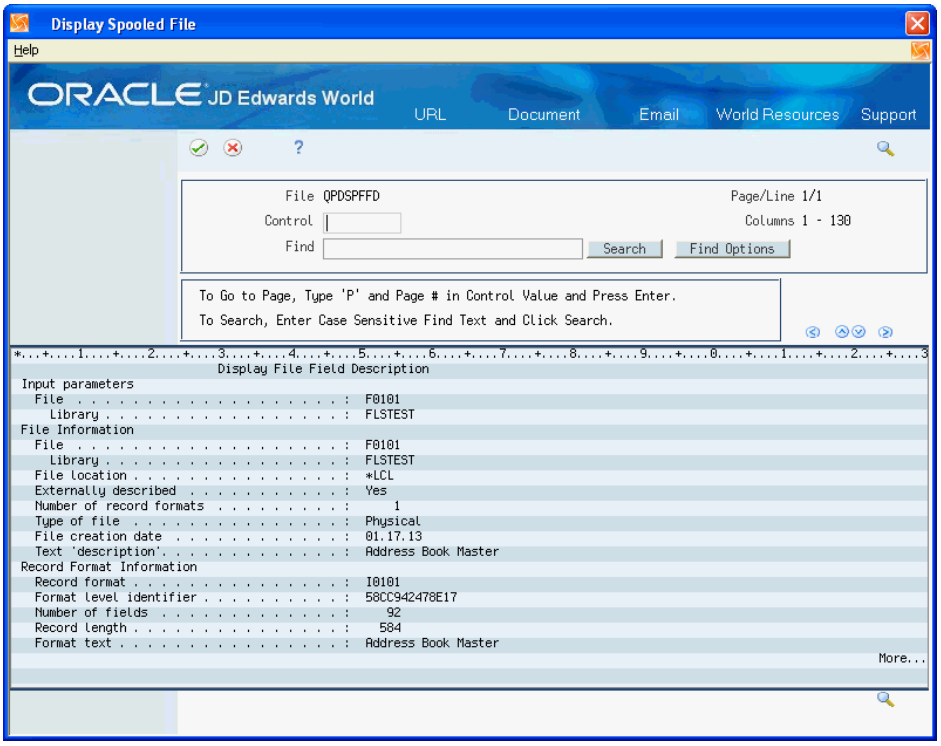
1. From the command line on Field Level Masking (G941), type DSPFFD (Display File Field Description) and press F4.
2. Type the File (F0101) and Library (FLSTEST) where the Field Level Masking was set.

Figure B–12 Display File Field Description screen



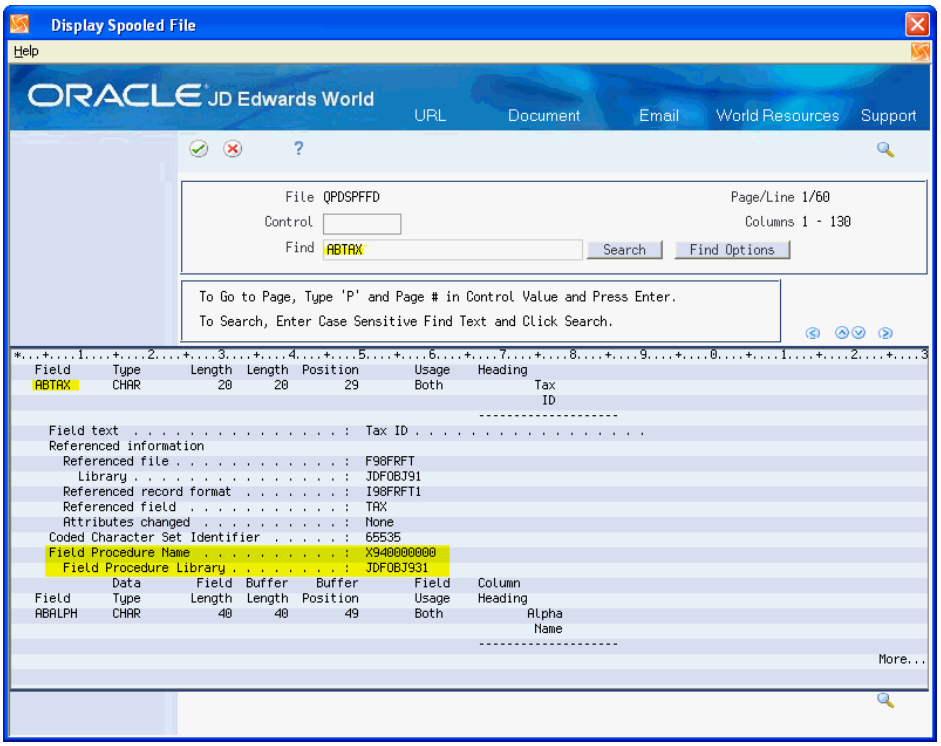
3. Press Enter to access the Display Spooled File screen.

Figure B–13 Display Spooled File screen



4. In the Find field type ABTAX and press F16.

Figure B–14 Display Spooled File screen



Note the Field Procedure Name X940000000. This is the indication that the "set" process was successful and the masking is now active for this field.

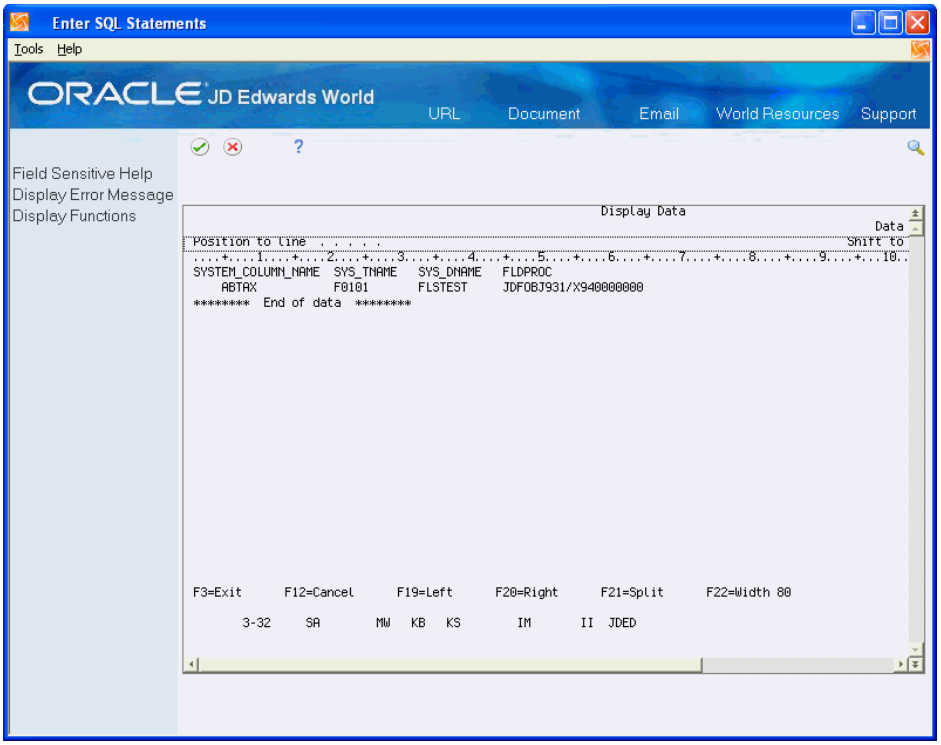
5. Another way to prove that Field Level Masking is 'Set' on a field is to run an SQL statement.

   From the command line, type STRSQL and then press Enter.

6. From the SQL command line, type the following SQL statement:

   select sys_cname, sys_tname, sys_dname, fldproc from qsys2/sysfields

Figure B–15 Enter SQL Statements screen



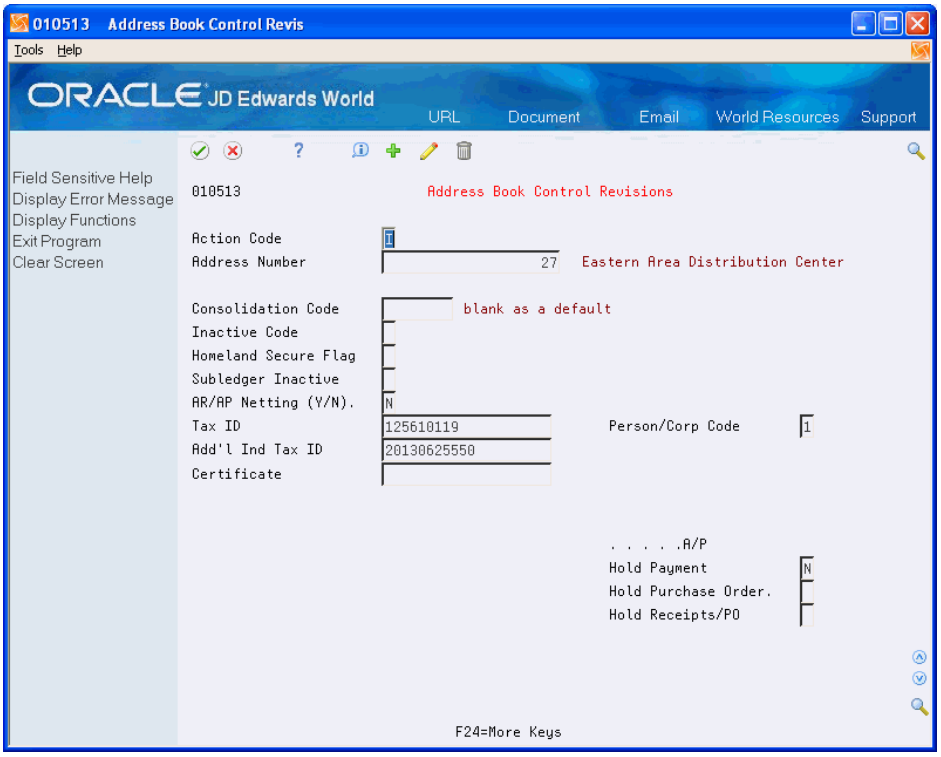
7. When you run the SQL statement as specified on Step 6, the system displays all the combinations of Fields/Files/Libraries in the entire system that have Field Level Masking applied.

B.2 Test the Masking Field on a Screen and a Report

From Address Book (G01) menu, access Address Book Revisions (V01051). Inquire on Address Number 27 and press F13 (Address Book Control Revisions). Address Number 27 is a record that has a Tax Id.

Review the following graphic of the Address Book Control Revisions (V010513) screen for Address Number 27.

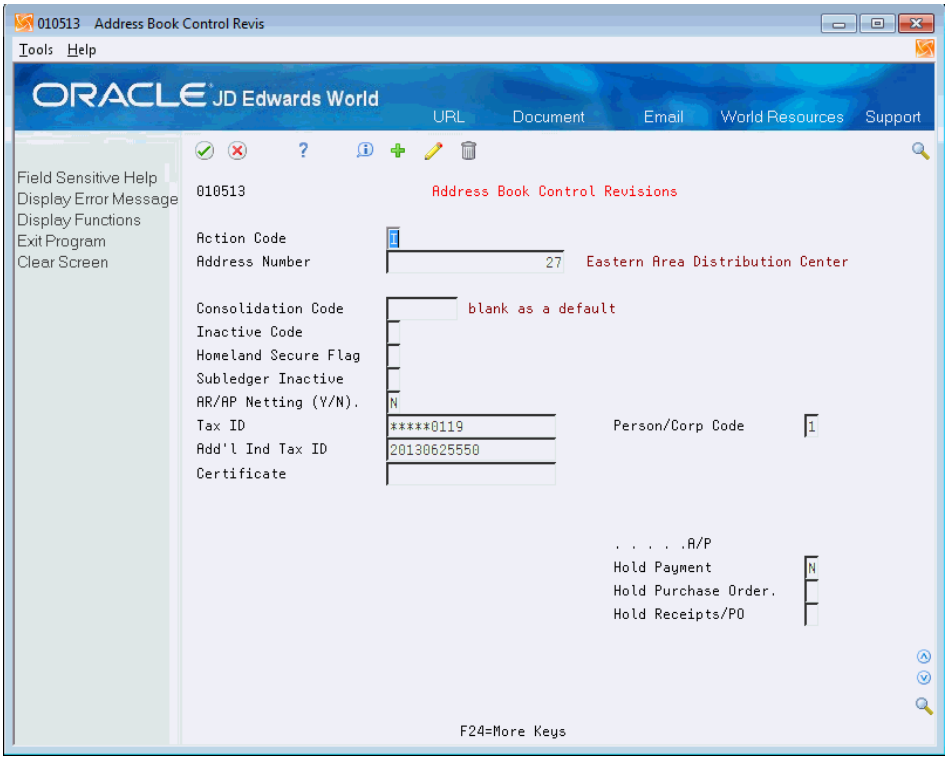
Figure B–16 Address Book Control Revisions screen



Note that the Tax Id is not masked for the user with access through group JDEPGMR.

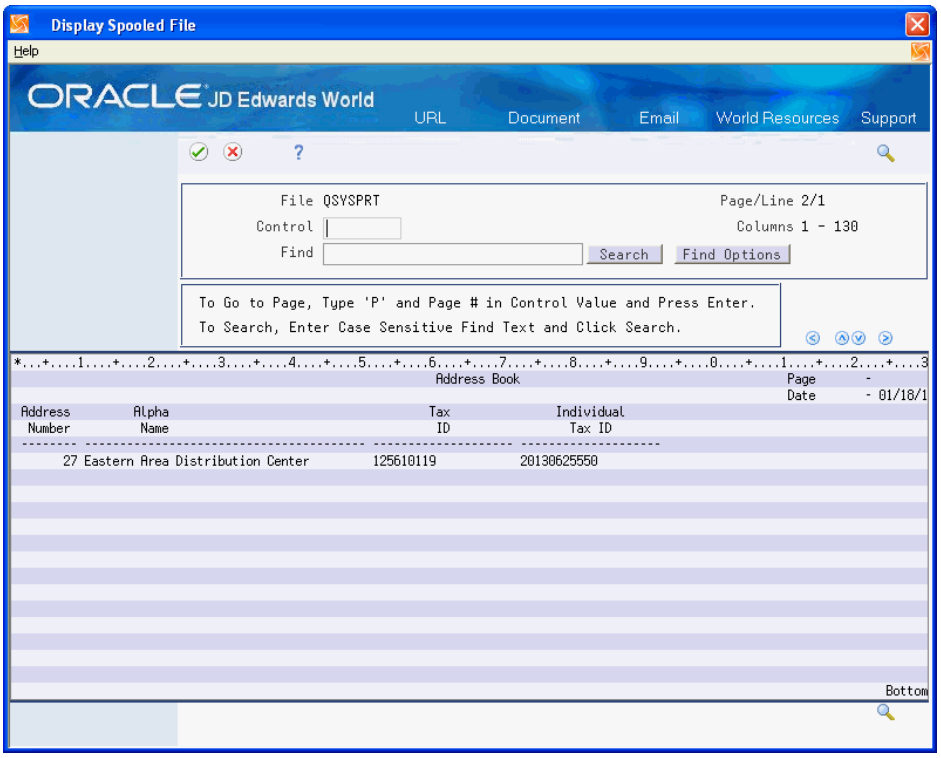
The following graphic displays the Address Book Control Revisions (V010513) screen with the Tax ID masked for the user without access through the group JDEPGMR.

Figure B–17 Address Book Control Revisions screen



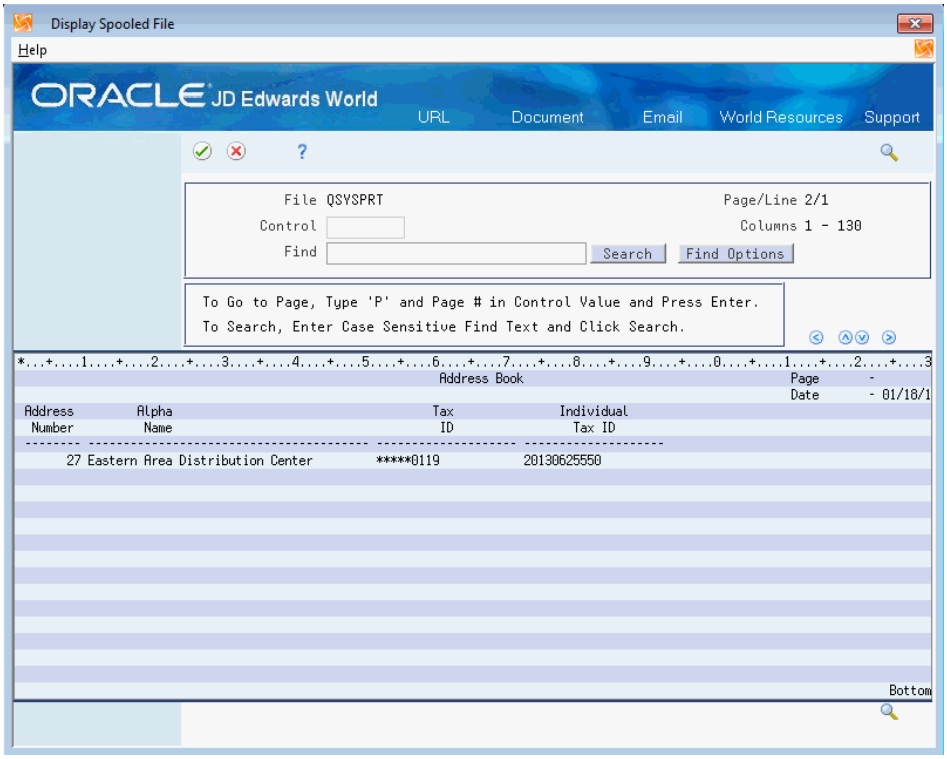
The following graphic displays a World Writer report with Address Number 27 and the Tax Id not masked for the user with access through the group JDEPGMR.

Figure B–18 Display Spooled File screen



The following graphic displays a World Writer report with Address Number 27 and the Tax Id masked for the user without access through the group JDEPGMR.

Figure B–19 Display Spooled File screen



C

IBM Authorization Lists – Object Authority Information

This appendix contains these topics:

- Section C.1, "Object Authority - Help,"
- Section C.2, "Field Level Masking – Authority Rights."

In this appendix you can review the IBM Help information for Authorization Lists and the different Object Authorities that can be assigned to each user profile.

For Field Level Masking purposes, wherever object is referenced, substitute it for the word field.

C.1 Object Authority - Help

The authority that the user has to an object.

Several different system-defined object authority levels may be assigned to users. The following table describes the object authority levels.

Authority Level	Explanation
*ALL	Allows all operations on the object except those that are limited to the owner or controlled by authorization list management authority.
*CHANGE	Allows all operations on the object except those that are limited to the owner or controlled by object existence authority, object alter authority, object reference authority, and object management authority.
*EXCLUDE	All operations on the object are prohibited.
*USE	Allows access to the object attributes and use of the object. The user cannot change the object.

C.2 Field Level Masking – Authority Rights

Both *ALL and *CHANGE rights allow users to view and change the field without masking applied.

*USE rights allow users to view the field without masking applied, but not the ability to change the field value.

*EXCLUDE rights prevent users from both viewing and changing the masked field.

Oracle JD Edwards World recommends using *CHANGE, *USE, and *EXCLUDE rights on the Authorization Lists, as those values are easily identifiable and self-explanatory.

Glossary

access provisioning

The process of setting up user and role profiles in World for sign-in security (authentication) and authorization security.

authentication

The process of verifying that users signing into World are valid World users.

authorization

The process of granting or denying users access to World applications, features, data, and data sources. In World, most authorization security is applied at the object level through the Security Workbench.

add mode

A condition of a form that enables users to input data.

data encryption

The process of transforming information into code so that it cannot be read by a third party system. World encrypts user passwords stored in the database.

data masking

Customizing a field so that specified characters are embedded in place of sensitive data that appears in applications. This prevents sensitive data from being displayed to unauthorized users.

data privacy

In World, Address Book data security enables you to restrict users from viewing Address Book information that is determined as private, personal data.

developer security

Security that determines the actions that developers can perform when customizing or developing EnterpriseOne applications in Object Management Workbench (OMW). Actions can include checking out and checking in objects, promoting objects, transferring objects, removing objects, and so forth.

object-level security

A type of authorization security that enables you to secure specific objects within JD Edwards World such as applications, forms, and various other World features. Object-level security provides flexibility with applying security and a higher level of security integrity.

*PUBLIC

A special ID within World that automatically includes all users within it. This option controls security for all users who are designated by ID type ***PUBLIC** in the User or Role field.

power form

Web-only application forms that enable users to view multiple, interrelated views of data, grids, and tab pages on one form and to pass logic between them.

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.

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.

security overrides

Security records that operate as exceptions to existing security records. Security overrides specify that users are *unsecured* from an World 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 workbench

An application that enables you to secure JD Edwards World objects, such as applications, forms, rows, tabs, and so on. It stores all objects security records in the F00950 table.

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.

subform

A subform is a control designed for use on a power form or another subform. Power forms can contain several subforms, so a single power form with multiple subforms enables users to see multiple data views.

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.

Index

A

Action Code screen (P00031), 9-2
Action code security
  setting up, 9-1
Add
  defined, 9-2, 9-6

B

Batch approval/post
  setting up security, 14-1
Break Message, 8-12
Business Unit From
  defined, 10-3
Business unit security
  set up considerations, 10-2
Business Unit Thru
  defined, 10-3

C

Change
  defined, 9-3, 9-6
Change User Profile Ownership screen
    (P98CHGOWN), 16-1
Changing user profile ownership, 16-1
Command entry
  securing, 7-2

D

Delete
  defined, 9-3, 9-7

E

Export
  defined, 9-3, 9-7

F

Fields
  Add, 9-2, 9-6
  Allow Usage, 11-3
  Business Unit From, 10-3
  Business Unit Thru, 10-3
  Change, 9-3, 9-6
  Delete, 9-3, 9-7
  Export, 9-3, 9-7
  Import, 9-3, 9-7
  Video Screen, 11-2
Function Exit, 11-1
Function key security, 11-1
  working with, 11-2

G

General Accounting Constants screen
    (P000909), 14-4
Group profile or *PUBLIC
  menu masking, 8-10
Group security
  setting up, 7-3

H

Hidden selection
  how to secure, 8-12
  how to secure hidden selection 33, 8-13

I

Import
  defined, 9-3, 9-7

M

Mask processing options
  for DREAM Writer, 15-7
Menu Locks screen (P00908), 8-9
Menu masking, 8-9
  considerations, 8-14
  example, 8-10
  group profile or *PUBLIC, 8-10
  types of comparisons, 8-9

P

Programs and IDs
  P00031 (action code), 9-2
  P00042 (user defined codes), 13-1
  P000909 (general accounting constants), 14-4

P00908 (menu locks), 8-9
P98326 (report version), 15-2
P98CHGOWN (change user profile ownership), 16-1
PUBLIC
menu masking, 8-10

R

Report security for report writer, 15-1
Report Version screen (P98326), 15-2

S

Screens
Action Code, 9-2
Change User Profile Ownership, 16-1
General Accounting Constants, 14-4
Menu Locks, 8-9
Report Version, 15-2
User Defined Codes, 13-1
Securing command entry, 7-2
Security
batch approval/post, 14-1
function key, 11-1
masking DREAM Writer processing options, 15-7
Setting up group, 7-3
setting up report writer security, 15-1
Setting up user, 6-1
user defined codes, 13-1
Security Workbench, 17-1
Send Window Message, 8-12
Standard function keys, 11-4

T

Troubleshooting menu security setup, 8-11
Troubleshooting user defined code security, 11-4

U

User defined codes
setting up security, 13-1
User Defined Codes screen (P00042), 13-1
User profile
changing ownership, 16-1
User security
setting up, 6-1

V

Video Screen
defined, 11-2