Global Information Assurance Certification Paper

JDE Security 101 J.D. Edwards - User Security Levels.
Fred Hansen - SANS Level One Security Certification
Submitted 09/14/2000

JD Edwards & Company develops, markets and supports enterprise software and supply chain computing solutions and is one of the leading suppliers of Enterprise Resource Planning (ERP) software. The JDE AS/400 software package is used to record and report financial data by the Financial Staff, Financial Managers and External Auditors. JDE contains financial data used for daily operations, management reports, and formal financial reports geared to shareholders and the Security and Exchange Commission (SEC). For this reason, accuracy and security of JDE data is imperative.

This paper will provide an overview of the user security levels for the JDE systems which reside on an AS/400 platform in central or distributed locations. It is written for JDE System Administrators who have access and basic knowledge of the security menus. This document may also be used as a policy template to use to coordinate multiple environments which may have several Security Administrators.

JDE Security Administrators

JDE provides multi-level data security which features flexibility and depth. The complexity involved in configuring these features may lead to inadvertently providing user's the right to access, change or delete sensitive data. Setup of access security must include a carefully planned and executed set of procedures to ensure that logical access paths are correctly defined. In order to accomplish this, the JDE Security Administrator is required to have a thorough understanding of how the business will be using the JDE financial systems, the details of individual user job responsibilities and how the security levels may over-ride each other. The JDE Security Administrator should also have a strong aptitude and experience in Information Technology with training in JDE Financials. He/she should have accounting experience and knowledge of general financial processes. As with all computer applications, good analytical and problem solving skills are required.

A JDE Security Administrator should be assigned to control security within their region or area of responsibility. A backup administrator should also be trained and available. JDE Application Programmers need to be kept informed of current security policies to assure that the security infrastructure is maintained.

JDE Security Level Overview

1. AS/400 Computer Level Security - To be setup on the JDE Financial System on the AS/400, the user must have access to the AS/400. The AS/400 Security Officer should assign the JDE user restricted menu access, limited to the users job requirements. For additional security from hackers, corporate policy should require passwords be reset every 35 days.

2. Super User Level Access - Menu Travel, Command Entry and Fast Path.
Super User level access is granted by the JDE Security Administrator by placing a "Y" in the users profile under the User Security/ User Information screen. Placing an "N" in these fields denies access for that user. This field should never be left blank.

a) **Menu Travel** - allows a user to access a menu by typing the screen identifier on the command line, even if the user does not have access via Menu Level Security access. Menu travel to other menus and functions within JDE should be disabled. When the menu travel has been revoked, the JDE menu log is active. This will log the time and duration a user has accessed the programs.

b) **Command Entry** - This access should be used by Administrative or Security level users only. This will allow a user to submit administrative and operating system commands directly from the initial menu screen.

Note: The "Limit Capabilities" flag on the AS/400 user profile must be set to "Yes" for Command Line access to be in effect.

c) **Fast Path** - allows a user to access a menu by typing the menu name on the command line.

Note: Access to the Super User features may negate other security settings by giving users the ability to circumvent security features offered by other menu restrictions.

3. JDE Menu Level Security and Menu Level Locks

User security is restricted by assigning access values to the User Key field in the User Security/User Information screen. Menu security is restricted by assigning menu lock values to the Menu Lock fields in the Security/Menu Information screen. Menu security is determined by the combination of user keys and menu locks. If no level / code is defined for a user key or menu lock, then access is allowed by default. To prevent access by default, place an "X" in the unallocated positions of the User Key field.

Each user is also assigned an 'initial' menu in their user profile which will restrict access to a specific group of menus and/or programs at startup. If properly configured, the user should only have access to the functions provided on the initial menu, however, as noted above, users may be able to access sensitive system commands or other options which are not otherwise restricted, if Super User level access is allowed.

Menu "masking" is a method of securing entire menus or individual menu selections on a menu by user. JDE provides several User Key fields as follows:

Security Field	Type of Comparison:
A (Authority)	Hierarchical
J (Job)	Direct
K (Knowledge)	Hierarchical
DP (Dept)	Direct
F (Future use)	Direct

In a "Hierarchical" field, A is the highest authority. "Z" would be low authority .

If blank, then access is allowed by default.
A "Direct" field must match exactly

As an example, we can assign codes to the "A" and "J" fields to determine the user access rights and levels for Accounts Payable or Accounts Receivable access. Under field "J", we will put a "P" for A/P users and we place an "R" for A/R users. In the Menu Security field "J" menu selection lock is set to "P" only accounts payable personnel should be able to access that menu.

In User Security, under the "A" field, we put an "Z" for all users except the Supervisor which we will assign a "S". If field "A" in the Menu Security, menu selection "lock" is set to "Z" all A/P accounts payable personnel should be able to access that menu item, however, If field "A" menu selection lock is set to "S" only the accounts payable supervisor will be allowed to access that menu.

4. **Function Key Security**

The function key security feature should only be enabled for selected users, such as those who need to maintain files and enter General Ledger data. All others will should be set to "N" and not be able to use the function keys at the bottom of each screen. If the field is left blank, access to the function key is given by default. Users can use function keys to access locations which are not on the menus they usually encounter, allowing a 'back door' to sensitive data.

5. **Cost Center Security**

Local users can be set to restricted access to their area of responsibility. The user must have a "Y" under User Security/Cost Center Security and assigned restrictive business unit numbers under the Security/Cost Center security screen. Cost center security can be specified by user ID or file ID . Within a company or subsidiary, additional cost centers can be created to segregate user access. This is very useful when several entities need to do individual reporting.

6. **Action Code Security**

Action Code Security requires specific program access rights be granted to each user. On the User Security/ User Information screen, Action Code Security set to "Y" indicates that a user ID must be granted in the Security/Action Code Security list for each program they are required to access. If left blank, by default, a user is not restricted by Action Code Security. The recommendation is to require Action Code Security for all users.

The Security/Action Code Security screen, have three action codes, Add, Change or Delete, which may be defined as "Y" for access or "N" to deny access. Every program Action Code Security List should begin with the User *PUBLIC with all access denied. This setting will only allow user listed with a "Y" access to the program.
Action code security can be defined by (1) Program ID with a list of users granted access to the program or (2) by User ID with a list of programs that each user is granted access.

Note: The above Action Code recommendation requires the Security Administrator to specifically grant each user rights to use each program. As there are hundreds of programs, this effort will be time consuming for larger environments. A carefully planned and executed set of procedures will reduce the time and effort required.

Security Profiles

In order to expedite user security setup, it is recommended that several security profile templates be configured by job description. The following security profile types are examples which may be used as a guide to create user templates:

1) Administration / Supervision

Persons with this access profile should have responsibility for general maintenance and administration of the system. In general, screen access includes that available to profiles 2 and/or 3, as well as additional functions such as VAT rate maintenance etc.

2) Accounts Payable Processor

This profile is required for persons with primary AP voucher input duties. Functions include voucher entry, invoice logging, voucher review, inquiry.

3) Address Book Control / Maintenance

This includes activities for the creation of new vendors, generation of reports originating from vendor file data, inquiries using name and address info., maintenance of address book details, etc.

4) Officer of Disbursement / AP Supervisor

This profile has access to the disbursement functions, including EDI and check printing.

5) Inquiry Only

Functions of individuals with this level of access are limited to vendor ledger inquiry, address book inquiry and account ledger inquiry. No add, change or delete authority is granted. Care must be taken to exclude some persons with this access from employee and vendor files for the purpose of confidentiality.

I hope this document has enabled you to understand some of the basic concepts of JDE user security. As noted above, JD Edwards software is made flexible through its use of multiple layers of security. Although it is a popular ERP software package, there is very little 'practical' information available on the web. Perhaps the flexibility does not allow for one specific 'best practices' approach or all those 'JDE Consulting' firms on the web are not willing to share their expertise.

This is an evolving document so any input would be appreciated. I may be contacted at fwhansen@usa.net.

References:

GIAC Staff. Security Essential Certification. 07/07/2000
URL: http://www.sans.org. (8/2000)

J.D. Edwards World Source Company, J.D. Edwards Online manual. 1996
URL: http://www.jdedwards.com/ (8/2000))

Perry, Mellisa. "J D Edwards Audit Program". Submitted 01/06/2000
URL: http:// www.AuditNet.org (8/2000).

Madden, Wayne and Woodbury, Carol. Implementing AS/400 Security 3rd edition.
ISACA Global information repository. 1998
URL: http//www.isaca.com. (9/2000)

Light, Lori. eGroups, J.D. Edwards message board)
http://www.egroups.com/message/jdedwards. (9/2000

JD Edwards. Our Services. Ernst and Young web site.
URL: http/www.eynx.co.nz/services/corporatefocus/jde.asp. (9/2000)