

JD Edwards Security Program

Before security can be addressed within the OneWorld product, the underlying components must be secured. This includes but is not limited to:

1) Host Systems :

- a) Deployment Server
 - i) Only allow system administrators to log onto the deployment server
 - ii) Don't share the package portions of the filesystems and use CD's for install
 - iii) Don't share help files
 - iv) Do not place shared services such as printing or DNS services on this host
 - v) Only run OneWorld on this machine for installs and upgrades
 - vi) Do not create user accounts on this machine,
- b) Enterprise Server
 - i) Do not allow users to log onto this machine
 - ii) Do not give users job control authority or system administration privileges
 - iii) Do not share or give general access to the OneWorld code and work directories
 - iv) Do not allow users to access or read the server .ini files
 - v) Do not allow users to start, stop, or configure OneWorld services
- c) Workgroup Servers
 - i) Do not allow users to log into workgroup servers
 - ii) Do not allow users access to the file system that supports OneWorld services
- d) Workstations – considered UNSECURE hosts
 - i) Users can access all information on their machine
 - ii) All validation and control records should be kept off of the workstations
- e) Windows Terminal Server (TSE) and Web Server
 - i) Treated like workstations
 - ii) Do not store any information on these servers
 - iii) Users should only be able to log onto these servers to run OneWorld and nothing else

2) Database Management Systems.

- a) OneWorld uses third party Databases to store all data records
- b) Must be accessible via network services such as ODBC and OCI
- c) Databases that are shared or exist on any Server must be secured
- d) Three Security models exist
 - i) Use system ID's so that users do not have the ability to log directly into the dB. Secure the dB with OneWorld object security.
 - ii) Allow user ID's access to the dB. Implement the entire data security model within the dB.
 - iii) Treat the dB as unsecure.

3) Networks

- a) Servers, Workstations, Printers, Storage Devices
- b) File Sharing, File Transfers

- c) ODBC, OCI
- d) Remote Login Sessions
- e) Printing
- f) Use network domains to restrict user access
- g) Use IP filtering to restrict users from overall access to remote networks and network segments

User Profiles

*OneWorld checks for security by USER ID first. If not found then Group ID is checked. If security for the Group ID is not found, then all records with *PUBLIC in Group ID field will be checked. If no security is found, then the user has all access.*

COEXISTENCE

In a coexistence environment, security profiles must be maintained on World and OneWorld.

Security Strategies

- OPEN/RESTRICT
 - Users have access to all OneWorld Objects (JDE default)
 - Objects are restricted one at a time from users
 - Most Work
- RESTRICT/OPEN
 - Restrict access to all applications
 - Access is granted to one object at a time
 - Safest

Following are 8 generalized groups that are not necessarily all-inclusive and will vary based on client's needs and business requirements.

1. Application User Group

This group consists of end-users based on a specific application (Purchasing, A/R, etc.) This group has the tightest security level. Security for this group should be set up to allow access to a custom initial menu and disable fast path.

2. Application Super User Group

This group consists of team leads or supervisors of specific Application Groups. Security for this group should be the same as the Application User Group as well as the ability to create new versions, move or copy versions between pathcodes, create new menus, and add new UDC values.

3. **Workflow Administrator**

Only applicable is using OneWorld workflow. This role can be shared between various Application Team Leads.

4. **Data Dictionary/UDC/Menu Administrator**

Responsible for making changes to the Data Dictionary, UDC's and OW menus. Application Team Leads can be responsible for this, but we would recommend having a single person responsible for all changes.

5. **Third Party Report Writer**

Third Party Report Writers need to provide a USER ID and Password. This grants report access to all data. Row and Column level security should be defined for these ID's.

6. **Product Version Control Group**

This group ensures timely package builds and deployments of Updates and is responsible for keeping track of numerous objects and operations.

7. **Developer**

Developers need special access to certain directories on the Deployment Server for checking objects in and out. They also need all OneWorld programs necessary to modify and create applications.

8. **MIS/DB/OW Administrator**

Responsible for managing the servers, backups, databases, printer setup, general maintenance. This group has all authority both I OW and in the OS and dB.

Security Checklist for Limiting Access to Applications		
Technical Application Name	Program	DO NOT Permit Access
Network Monitor (A)	N/A	1,2,3,4
Universal Table Browser (A)	N/A	1,2,3,4
All *.exe programs under System on the deployment server (A)	N/A	1,2,3,4
UDC	P0004A	1,3,6
Host Configuration	P00053	1,2,3,4,6
Menu Design	P0082	1,3,6
User Profiles	P0092	1,2,3,4,6
Work with Environments	P0094	1,2,3,4,6
Release Master	P00945	1,2,3,4,6
Security Workbench	P00950	1,2,3,4,6
Machine Identification	P00960	1,2,3,4
Queue Properties	P01133P	1,2,4,6 B

Queue Security	P01135	1,2,4,6 B
Work with Queues	P012501	1,2,4,6 B
Group Revisions	P02150	1,2,4,6 B
Start Escalation Monitor	P9000020	1,2,4,6
Data Dictionary	P92001	1,2,3,6
Error Messages	P92002	1,2,6
Cross Reference	P980011	1,2
Business Function where used	P980012	1,2,3,4,6
Path Code master	P980042	1,2,3,4,6
Batch Versions	P98305	3,4,6
Interactive versions	P983051	1,3,4,6
PO Text Translation	P98306	1,2,3,4
Installation Planner	P9840	1,2,3,4,6
Table Conversion/Merge Log	P984052	1,2,3,4,6
Installation Workbench	P9841	1,2,3,4,6
Table Conversion Scheduler	P98430	1,2,3,4,6
Object Librarian	P9860	1,2
Promotion Manager	P98603	1,2,3,4
Object Transfer	P98604	1,2,3,4
OCM	P986110	1,3,4
Data Sources	P986115	1,3,4
Work with Servers	P986116	3,4
Build Debug Info	P98615	1,2,3,4,6
Server Package Installs	P986150	1,2,3,4
B732 Printer Application	P98616	1,2,3,4,6
Record Copy	P9864	1
Process Master	P98800	1,2,3,4,6
Checkout Log	P9882	1,2,3,4
Work with Packages	P9885	1,2,3,4
Process Activity Monitor	P98860	1,2,4,6 B
Advanced Analysis	P98870	1,2,4,6 B
Spec Merge logging Info	P98881	1,2,3,4,6
Translation	P988830	1,2,3,4,6
Deployment Locations	P9889	1,2,3,4
Optional Tables Workbench	P98920	1,2,3,4,6
User Overrides	P98950	1,3,4,6
Business Function Documentation	P98ABSFN	1,2,3,4
Data Replication	P98DREP	1,2,4,6

Media Object Queues	P98MOQUE	1,2,3,4,6
User Security	P98OWSEC	1,2,3,4,6
JDE Licensing Security	P98SRV	1,2,3,4,6
Media Object Templates	P98TMPL	1,3,4,6
System Control	P99410	1,2,3,4,6
Workflow Data Consolidation	PH9001	1,2,4,6 B
Create User Profiles from Address Book Records	R0092	1,2,3,4,6
Summarize Group Profile Information	R00921	1,2,3,4,6
Create Publisher and Subscriber records	R00960	1,2,3,4,6
Purge completed Tasks	R01131P	1,2,3,4,6 B
Update display decimals	R9200100	1,2,3,6
Replicate Data Dictionary Changes	R92001T	1,2,3
Recreate Replicated Data Dictionary	R92TAM	1,2,3
Installation Planner Report	R9840A	1,2,3,4,6
Plan validation	R9840B	1,2,3,4,6
Installation Plan Copy	R9840C	1,2,3,4,6
OCM Mapping Comparison	R986101	1,2,3,4,6
Data Source master report	R98611	1,2,3,4,6
OCM global update	R986110	1,2,3,4,6
Data Source Master Comparison	R986112	1,2,3,4,6
Verify OCM	R9861130	1,2,3,4,6
Object Configuration delete	R986120	1,2,3,4,6
Object Configuration copy	R986121	1,2,3,4,6
Check out and Purge Report	R982000	1,2,3,4,6
Process Activity Print	R98860	1,2,3,4,6
Purge Completed Processes	R98860P	1,2,3,4,6
Multi-tier package deployment	R98892B	1,2,3,4
Generate Business Function Documentation	R98ABSFN	1,2,3,4

A. Place NT Security on these files when they reside on the deployment server. On client workstations, the security can be controlled in NT by limiting access for those executables on the deployment server. Grant permission only to certain users in NT for Read/Write or Execute permission.

B. This responsibility can be assigned to each Application lead instead of a Workflow Administrator.

Deployment Server Directory Security

Use the following NT Security:

Directory	CNC Administrators (CNCADMIN) (8)	Production Users (PRODUSER) (1)	Development Users (DEVUSER) (7)	Application Super User Groups (APPLEAD) (2)
Client Jdeclnt.ddc Jdeclnt.xdc Odbcdatasource.inf All other files	Read/Write Read/Write Read/Write Read/Write	Read/Write Read/Write Read/Write Read Only	Read/Write Read/Write Read/Write Read Only	Read/Write Read/Write Read/Write Read Only
Pathcode /package all other subdirectories	Read/Write Read/Write	Read/Write Read Only	Read/Write Read/Write	Read/Write Read/Write
Database	Read/Write	No Access	No Access	No Access
Datadictionary	Read/Write	No Access	No Access	Read/Write
Helps	Read/Write	Read Only	Read Only	Read Only
Hosts	Read/Write	No Access	No Access	No Access
Mediaobj	Read/Write	Read Only	Read Only	Read/Write
Planner	Read/Write	No Access	No Access	No Access
Printqueue	Read/Write	No Access	No Access	No Access
System	Read/Write	Read Only	Read Only	Read Only

Different OneWorld Security Types

Cost Center Security

This is implemented using Row Security. This allows access to certain Cost Center records. This applies when using the Universal Table Browser Program. This does not combine Group Profile Security with User Security. User Security overrides Group Security.

Row Level Security for Specific Records

Same as Cost Center Security and prevents access to particular records in a database.

Form Level Security for Interactive Applications

Should be implemented when you need to limit particular user or group access to part of an application. Similar to Application level security except it is more form specific.

Security Workbench (P00950)

You need to limit access to the Security Workbench except for one or two individuals. All changes should be routed through these individuals. Make sure that these individuals don't secure themselves out of the program.

Menu Security

Limits users to specific, usually custom, menus. This is done by specifying opening menus for the group in the User Profile Revisions program. At this point the administrator has the ability to allow Fast Path to other menus.

- Custom menus can be created to restrict users from accessing other menus
- Fast Path, New Tab, Menu Search (binoculars), and File Open must also be restricted from the user for this to be effective.

Fast Path

Typically allowed for application team leads but not end users.

UDC/Menu/Data Dictionary Security

Application team leads should have access to UDC's and Menu revisions, while most users should not. For Data Dictionary, the DD administrator should be the only one making changes.

Scroll to Bottom on a Grid Security

This can significantly affect performance. Most groups should not have access to this.

Media Objects Security (Adding or Changing)

This is set at application design time. Allows any user to change or delete a Media Object.

Processing Options Security

Typically set for end user groups who are only allowed a predefined set of Processing Options for an Application.

Object Level versus Version Level Security

Object Level 'Update' allows an unsecured user to view Processing Options values for any object version. Object Level 'Prompt for Values' bars unsecured users from viewing Processing Options. Version Level security greater than 0, bars all users from viewing Processing Options values. Object Level 'Prompt for Versions' security bars unsecured users from viewing any Oexplore or batch versions for an object.

Workflow Security

This should be enabled when implementing Workflow. (Workflow automates business process such as PO Approval routing.)

Using NT Defined Groups Names for your OneWorld Group Names

This is for ease of maintenance.

SQL *NetSecurity

Limit access to the Query Tool. The database password is stored in the JDE.ini file in plain text. : Limit access to the jde.ini file.

Security and the JDE.INI File

Limit users access to the jde.ini file on their desktop

Server INI File Security

As previously mentioned, the server JDE.ini file contains the database USER ID and password. This file needs to be secured using NTFS security, Unix Object Security, and AS400 object security.

Workgroup Server Security

Workgroup servers use the same security as the deployment server. Replicated databases need to be secured and use of SQL query tools needs to be restricted.

Database Security on the F98OWSEC

Contains the OneWorld and database USER ID's and password. No one should be locked out using native database security.

File Security

BSFN Security

Business Functions need to be kept secure. Checking in and out can be controlled by only granting NT security to the development group for the deployment server directory structure.

Spec Security

Environmental files, access should be limited to the OneWorld kernel processes. Permissions should be read/write only for the user, and the group should not be classified as executables.

INI File Security

Access should be restricted to all except the USER ID and password returned from the security server. If security server is not running, then all users would need access to the INI file on the security server to run.

UBE Security

Starting and Stopping OneWorld Security

Only certain users should be given this authority.

JDE Default User and Password

The default user JDE with password JDE needs to be changed. There are multiple places that this must occur for the program to function appropriately. Also ensure that you can't log on the databases using this ID and Password.

Security Server Error Matrix

Security Server Required or Not	Enterprise Server INI file	Workstation INI file	Description of Result
Security Server Required	Security Server ON	Security ON	No error message
		Security OFF	Error: Must Authenticate to Security Server
	Security Server OFF	Security ON	Error: Unable to locate Security Server
		Security OFF	Error: Must Authenticate to Security Server
Security Server NOT Required	Security Server ON	Security ON	No error message
		Security OFF	Database Password Entry screen
	Security Server OFF	Security ON	Error: Unable to Locate Security Server
		Security OFF	Database Password entry screen

UNIFIED LOGONS

You have to change the SQL datasource to use NT authentication instead of SQL authentication and create the matching user id in OneWorld.

OneWorld Object Security

1. **Application**
Secures users from executing an application or form within an application
2. **Action**
Secures users from adding, deleting, Revising, inquiring, or copying a record
3. **Row**
Database level security
Secures users from accessing a particular range or list of data in a table
Must be enabled in Data Dictionary
4. **Column**
Secure users from viewing or changing a value for a field
This can be a database or non database field
5. **Processing Options**
Secure users from viewing or changing the values of processing options, or from prompting for versions in specific applications
6. **Tab**
Secures users from tab pages on a form
7. **Exit Row**
Secure users from form and Row exits
8. **Exclusive Application**
Temporarily gives a user access to an application or UBE that had been previously restricted in Exclusive Application Security
9. **External Call Security**
Secures users from Non-OneWorld applications that can be accessed from within OneWorld
Will secure a user out of the executable if trying to access within OneWorld

Approach for User Security

Must determine if client is using **User based security** (every user has an individual logon for every system) or **System based security** (each user has a unique ID only within OneWorld.)

USER BASED SECURITY

- Journaling can track all activities at the user level
- Remote processes can be traced to individuals
- User specific security models can be created within the database and host operating systems.
- Users can bypass OneWorld to directly access database systems
- Changes to the security model are cumbersome
- OneWorld does not support sharing of ID and password information

SYSTEM BASED SECURITY

- Security administrator efforts are simplified

- Users are not allowed to directly access non-OneWorld components
- Ability to track processes by individual user is restricted.

SECURITY GOTCHAS

- Missing line in server.ini [Security] section “SecurityServer=enterprise_server_name”
- Mismatched case-sensitive enterprise server names
- Passwords incorrect or case-mismatched
- Security sections of client and/or server jde.ini files not turned on
- Passwords do not match in DB/2 and SQL Server (or Oracle)