WHITE PAPER

Managing JDE security Security Conversions "Open to Closed without the Pain"

Table of Contents

INTEGRATED WITH

ORACLE

JD EDWARDS ENTERPRISEONE

This paper focuses on how to use the ALLOut toolset to enable you to set-up and convert security in a number of ways –

- New site security set-up – Deny ALL
  - Menus – automatically generate Application, Action and Processing Option security
  - Standard approved roles (templates) – automatically load Application and Action security.
- Existing site - Open to Closed
  - Deny ALL
  - Deny Critical
- Application "Deny ALL" but Action Code open – convert to Action Deny ALL
- Role or User level *ALL Y settings – how to remove them
- Exclusive to Inclusive Row Security conversion
- Q Software to standard E1 conversion

The core of the solution is the Project+ program that will create 95+% of the settings automatically in the time it takes to run the UBE.

Many projects we can support via the web and do not require an on-site visit.

If your project is more complex, our consultant will attend on-site for 2 or 3 days, agree the procedure with you, run the programs and then cut-over at least one user from the old set-up to the new one. You will then transfer over the rest of the users in the following days.

We have completed the project for all versions of JD Edwards from Xe thru to 9.1 – it is the focus of our business and is why we are called "ALLOut".

JD Edwards Versions Supported

The following versions are supported –

- **EnterpriseOne 8.9 to 9.1**
- **OneWorld Xe and ERP8** – with Solution Explorer – the process is the same but you will be creating security for Group profiles not roles.
- **OneWorld Xe** – OneWorld Menus – the software will create security at the Group level using your OneWorld Menus.

JD Edwards Security Table

The ALLOut Project+ process populates the standard E1 security table F00950. There are no external tables involved.

The conversion process, even in an existing live site, does not require a second security table.

Global lock-down strategy

The importance of a “Deny ALL” global lock down strategy is discussed in Appendix A.

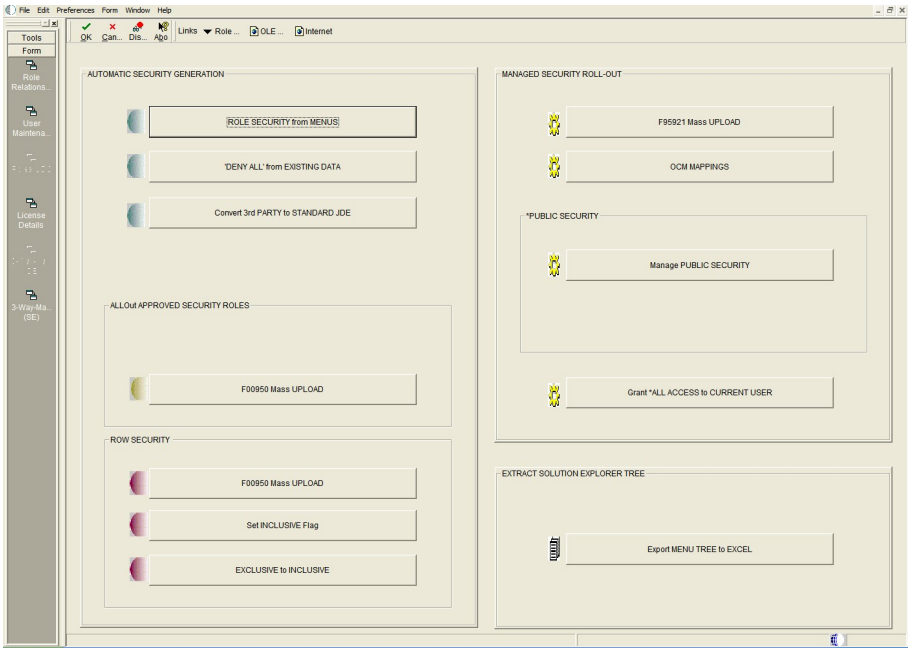
The alternative “Deny Critical” is being used by E1 customers that focus on Segregation of Duties (SOD) for their reporting. SOD rules are based on critical programs and if these are locked then it is easy to demonstrate that the rules are not breached.

ALLOut Project+

Initially this was a UBE that created “Y” settings from menus so that a Deny ALL set up could be implemented in a few hours.

The program is now a family of UBEs and interactive grids that address all the set-up and conversion requirements needed by JDE sites.

This is a screen shot of the “front door” –



Each button leads to programs that support the processes described below.

New site security set-up – Deny ALL – from Menus

Most E1 implementations start by the applications team creating a menu (Task View) structure that support all the business processes. The standard E1 programs enable this to be achieved easily.

The next step is to define roles that correspond to each of the business processes. The standard E1 program (P0092) enables this to be achieved easily.

The third step is to use the Menu Filtering (Fine Cut) tool to create a specific view of the menus for each role. The standard E1 program is adequate – the ALLOut 3WaySuperGrid is better as it enables you to achieve this for multiple roles at the same time.

The fourth step is to create security – particularly application, action and processing option security.

The ALLOut Project+ family of programs and spreadsheets enable you to achieve this in a matter of a few hours.

The process is –

- Set up *PUBLIC Deny ALL - use the Project+ Grid to load the *PUBLIC *ALL N settings plus all objects that need to be used by all users.
- For each role – use the Project+ UBE to
    - Create default application, action and processing option "Y" settings based on the Menu Filter.
    - Embedded programs – for each UBE – create application "Y" settings
    - For programs behind each exit – create application "Y" settings
- Fine tune – use the 3WaySuperGrid to –
    - Fine tune action security
    - Fine tune programs behind exits
    - Export to spreadsheet for off-line review
- The security is now ready to be handed over for testing and fine tuning.
- Part of the process is to check each role does not breach SOD rules. The ALLOut Risk Reporting module can be used to achieve this.

New site security set-up – Deny ALL – from ALLOut standard approved roles (templates)

Some sites do not use Menu Filtering.

In this case you will need to use the standard role templates provided as part of Project+.

The process is -

- Set up *PUBLIC Deny ALL - use the Project+ Grid to load the *PUBLIC *ALL N settings plus all objects that need to be used by all users.
- Create roles using the standard E1 – P0092 program
- Use the Project+ Grid to load each of the standard roles into the security table.
    - Security settings are for application and action security

    - These have all the programs required to support the process, including programs on the menus, hidden programs and programs behind the exits
- Use the 3WaySuperGrid to load the role, menu and security settings. There is an option to see the menu and programs as seen by the role. Use this option to:-
    - Fine tune action security
    - Fine tune programs behind exits
    - Export to spreadsheet for off-line review

The security is now ready to be handed over for testing and fine tuning.

Part of the process is to check each role does not breach SOD rules. The ALLOut Risk Reporting module can be used to achieve this.

Existing site Open to Closed – Deny ALL

If you use menus for security, then converting from open to closed is very easy.

The process described here will work for the old OneWorld menus, Solution Explorer, Task Views, Web Menus etc.

The ALLOut Project+ program will identify all the programs on the menus and create the application and action security "Y" settings they are currently receiving by default.

Any existing application and action security will not be changed – **all your existing investment in application and action security will be preserved.**

You can then apply the Deny ALL setting – with care!

The challenge when implementing a Deny ALL strategy in a live site is to avoid disrupting the day-to-day operations of existing users.

To achieve this you need to –

- Create a new, temporary role called PUBLIC and use this role to apply the settings that would normally be applied at *PUBLIC.
- For each role (either existing or new) – create the required "Y" settings.
- Assign multiple roles to users - use the multiple roles capability of standard E1 (or for Xe and ERP8 sites, the ALLOut CombiRole module) to assign the PUBLIC role to each user in turn – in addition to their standard roles.
- Once the conversion is complete, the *PUBLIC settings can be created and the PUBLIC role removed.

Taking each step in detail -

1. Create a new, temporary role called PUBLIC
    - Use Project+ to create the new PUBLIC role
    - Set up Deny ALL for PUBLIC - use the Project+ Grid to load the *ALL N settings plus all objects that need to be used by all users.

2. For each role (either existing or new) – create the required "Y" settings.
    - Create default application, action and processing option "Y" settings based on the Menu Filter.
    - Hidden programs – for each UBE – create application "Y" settings
    - For programs behind each exit – create application "Y" settings
    - Fine tune – use the 3WaySuperGrid to –
        - Fine tune action security
        - Fine tune programs behind exits
        - Export to spreadsheet for off-line review
3. Assign multiple roles to users
    - In standard E1 you can very easily assign the new PUBLIC Deny ALL role to a user and they will not see any difference to their day-to-day operation.
    - In Xe and ERP8 you will use ALLOut CombiRoles to assign the PUBLIC Deny ALL role plus the standard roles to a user and they will not see any difference to their day-to-day operation.
4. Once the conversion is complete –
    - Create the *PUBLIC Deny ALL settings.
    - Remove the PUBLIC Deny ALL role from each user and delete the PUBLIC role.

Part of the process is to check each role does not breach SOD rules. The ALLOut Risk Reporting module can be used to achieve this.

Existing site Open to Closed – Deny Critical

Segregation of Duties – locking the critical programs that make up the rules!

If you are in the situation of having an open system – and your auditors require you to produce Segregation of Duties reports – the SOD rules will be program based.

For example, P04012 (Vendor Master Maintenance) and P4310 (Purchase Order) is a forbidden combination.

If you are relying on menus for security, when you run the reports – every user will be in breach of every rule!

What you need is a quick but effective way of identifying all roles that currently use these critical programs.

ALLOut Project+ uses your SOD rules as the basis for creating "Y" settings for application and action security.

It is then a very easy step to create *PUBLIC "N" settings for these programs.

The "Deny Critical" project consists of the following steps.

- Load your (or the ALLOut rules) SOD rules into ALLOut.
- For each role – run the Project+ program against the menu and create "Y" settings for action and application security if none currently exist.
    - Action and application "Y" settings are created for critical programs only.
    - Embedded UBEs are identified
    - Programs behind exits are identified.
- For each program in turn
    - Create application and action security "N" settings at *PUBLIC.
    - Do this relatively slowly to avoid disruption to users just in case some programs have been missed.

You are now ready to re-run your SOD reports and all the breaches will disappear.

Application "Deny ALL" but Action Code Security open.

This is a program run by an ALLOut Consultant.

It creates an action code security "Y" record if there is no action code security record for the role or at *PUBLIC.

Once complete the *PUBLIC *ALL "N" setting can be applied.

The project will not result in any disruption to day-to-day user activity.

Role or User level *ALL Y Setting – how to remove them

We see these at so many E1 sites.

There is a Power User that is getting hindered in their day to day work and so they ask (demand) access to everything. They are given *ALL Objects "Y" and the problem is gone!

Now you need to get rid of the setting. If you delete it then they will be complaining again about being locked down.

What you need to do is discover all the objects the user is getting to through their menus, exits and hidden program and create the appropriate "Y" settings.

The ALLOut Project+ program will create all the required "Y" settings for Application and Action security. It will not change any existing security that may have been in place.

Once complete you can remove the *ALL Y setting.

The process will run at either the user or role level – however we recommend you run it at the role level – creating a new role just for the power user if necessary. Removing redundant or duplicate roles is the subject of our Multiple Roles Management white paper.

Exclusive to Inclusive Row Security conversion

This is a program run by an ALLOut Consultant.

The client needs to send ALLOut a large sample of the existing row security so the complexity of the conversion can be assessed.

A temporary second security table needs to be created.

The program will create a “Y” setting to replace all the existing “N” settings.

Some fine tuning may need to be applied.

The project will not result in any disruption to day-to-day user activity.

Conclusions and recommendations

The procedure for implementing a closed system is now well proven and can be achieved quickly and with minimal disruption for end users.

The cost of the solution is minimal compared to the time, effort and disruption for end users when doing the lock down using standard E1 features.

Once complete you will be in a position to undertake effective compliance reporting and segregation of duties reporting – **ALLOut Risk Reporting Module** will assist with this.

If you find that you are having segregation of duties issues with your role structure then you will need to re-structure your roles using the **Supergrid** and the **ALLOut CombiRoles** module.

The **Risk Management Module** takes role assignment to the next level. You can use it to stop a role being allocated that will cause a SOD breach. It also has advanced audit trail and reporting features.

Contact us at ALLOut Security for product information and to register for a public webinar. sales@alloutsecurity.com

Currently setting up security? Talk to us about an evaluation.

Appendix A: Global lock-down strategy

Early implementations of EnterpriseOne took the view that it was sufficient to identify sensitive programs and restrict access to them via menus. All the project team needed to do was to create custom menus and security was available as a by-product. In this way it was possible to implement "security" with the minimum of effort.

Auditors have now come to realize that this approach has several major shortcomings:-

Default setting for a new program is "open access" – this means that any new program (or version) will automatically be open until someone does something to limit access

Default setting for a new user is also "open-access" and specific action is required to make sure that a new user's access is restricted

Back-doors – there are so many routes through E1 that it is impossible to block access to any program effectively

Because of these limitations a more controlled environment is essential.

Fundamental to any effectively controlled environment is the ability to put into place a "global lock" that ensures users can only access the programs, forms and versions (collectively known as "applications") they are authorized to use. The implementation of this lock provides three essential benefits:-

1. Lock-down - users can only access applications that they are authorized to use
2. Reporting – you can now produce definitive reports of access and update authority
3. Change control - all new applications are totally protected until someone takes positive action to grant permission for their use.

It is only through the implementation of effective controls that these objectives can be met.