WHITE PAPER

# Project+ & Menu Management

## Implementations, Upgrades Conversions and Much More

## Table of Contents

PROJECT+ .....................................................................................3

THIS IS THE PROJECT+ "FRONT DOOR" ...............................................3

MENU SET-UP AND MANAGEMENT ....................................................3

PROFILES – USERS AND ROLES ...........................................................4

AUTOMATIC SECURITY SET-UP - ALLOUT DISCOVERY ...............................5

NEW SITE SECURITY SET-UP – DENY ALL – FROM MENUS – BASED ON YOUR OWN MENUS. .......................................................................5

NEW SITE – STARTOUT – STANDARD MENUS, TAB PAGES, ROLES AND SECURITY .....................................................................................6

EXISTING SITE OPEN TO CLOSED – DENY ALL..........................................6

EXISTING SITE OPEN TO CLOSED – DENY CRITICAL ..................................8

APPLICATION "DENY ALL" BUT ACTION CODE SECURITY OPEN. ...................9

ROLE OR USER LEVEL *ALL Y SETTING – HOW TO REMOVE THEM ................9

EXCLUSIVE TO INCLUSIVE ROW SECURITY CONVERSION ...........................9

Q SOFTWARE TO STANDARD E1 CONVERSION ..ERROR! BOOKMARK NOT DEFINED.

CONCLUSIONS AND RECOMMENDATIONS .........................................10

APPENDIX A: GLOBAL LOCK-DOWN STRATEGY ....................................11

INTEGRATED WITH

ORACLE

JD EDWARDS ENTERPRISEONE

### Scope of this paper

This paper focuses on how to use the ALLOut Methodology and toolset to enable you to deliver your project on-time and within budget by taking tasks, that typically take days or weeks, and automating them so they take days –

- Menu set-up – you can't go live without them
  - Menu export to a spreadsheet
  - StartOut – automatic set-up from a spreadsheet
  - Menu management in a grid
  - Menu-filtering in a grid
- Users and Roles set-up and management
  - StartOut - automatically set-up profiles from a spreadsheet
  - User and role management in a grid
  - Convert from Groups to Roles in a grid
- New site security set-up – Deny ALL
  - Menus – automatically generate Application, Action and Processing Option security
  - StartOut - 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

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
- **OneWorld Xe** – OneWorld Menus

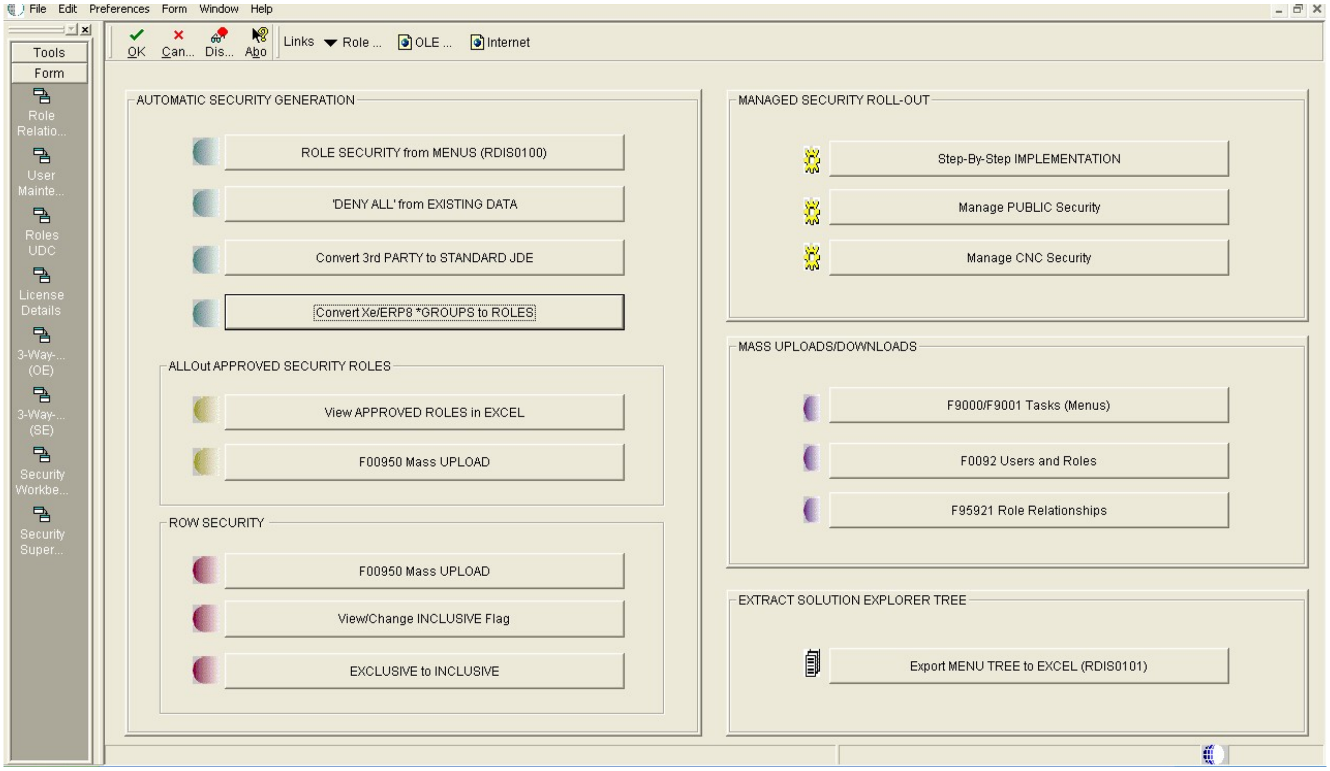
## Project+

The ALLOut Project+ module has been developed using the standard E1 toolset and consists of Event Rules and UBEs that you use to meet your specific objective.

Only E1 files are used.  When you see data in a Project+ grid then it is your data.  When you click “update” – you are given a warning message – but then it will directly update your data.

If data is environment specific, such as role relationships, it will update the data in the environment into which it is loaded.  You then promote changes in the normal way.

## This is the Project+ “front door”


File
Edit
Preferences
Form
Window
Help
OK
Can...
Dis...
Abo
Links
Role ...
OLE ...
Internet
Tools
Form
Role Relatio...
User Mainte...
Roles UDC
License Details
3-Way-... (OE)
3-Way-... (SE)
Security Workbe...
Security Super...
AUTOMATIC SECURITY GENERATION
ROLE SECURITY from MENUS (RDIS0100)
'DENY ALL' from EXISTING DATA
Convert 3rd PARTY to STANDARD JDE
Convert Xe/ERP8 *GROUPS to ROLES
ALLOut APPROVED SECURITY ROLES
View APPROVED ROLES in EXCEL
F00950 Mass UPLOAD
ROW SECURITY
F00950 Mass UPLOAD
View/Change INCLUSIVE Flag
EXCLUSIVE to INCLUSIVE
MANAGED SECURITY ROLL-OUT
Step-By-Step IMPLEMENTATION
Manage PUBLIC Security
Manage CNC Security
MASS UPLOADS/DOWNLOADS
F9000/F9001 Tasks (Menus)
F0092 Users and Roles
F95921 Role Relationships
EXTRACT SOLUTION EXPLORER TREE
Export MENU TREE to EXCEL (RDIS0101)

## Menu Set-up and Management

All E1 sites need menus.  You have got to have them to go live.  Setting them up can be a slow job and if you are up against a tight deadline then the job could delay your go-live.

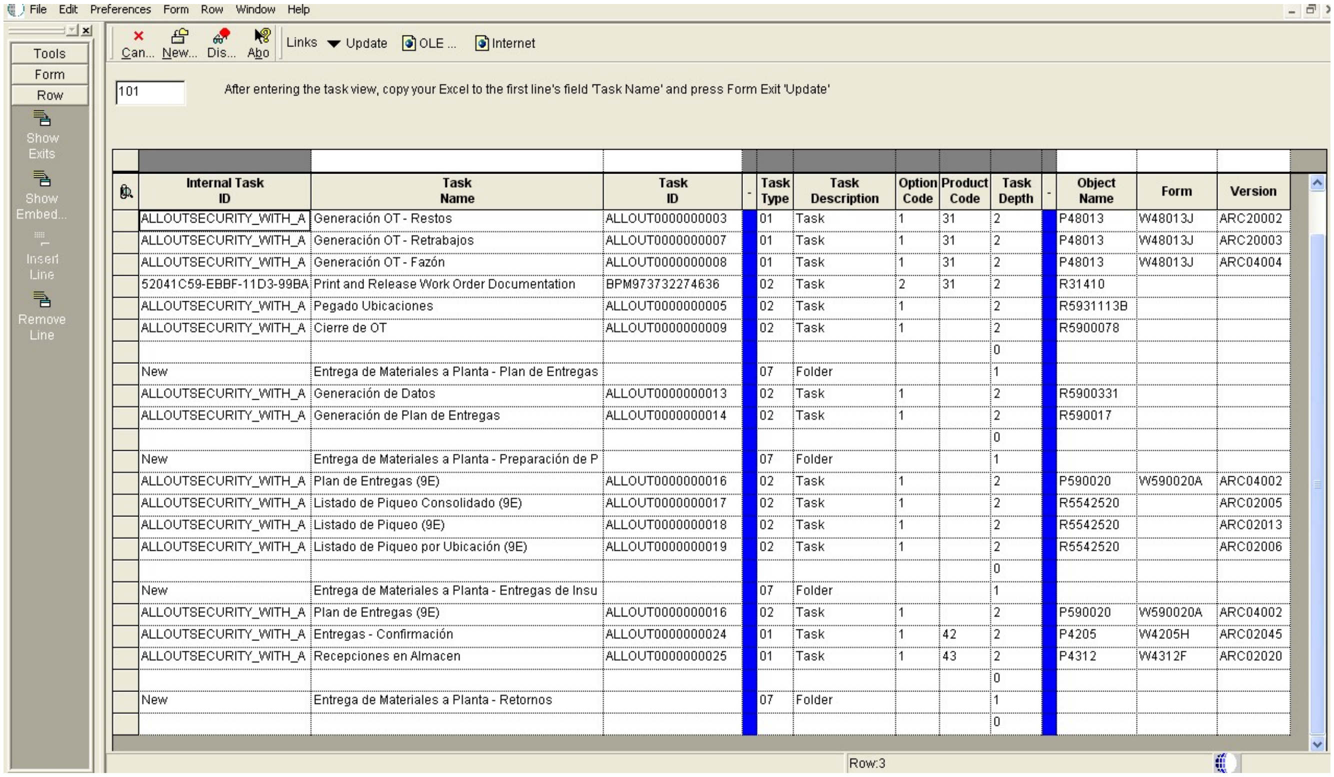
With the Menu Management Module you can create a menu tree in Excel and import it into E1 using the grid.  It will create Task IDs and you will be able to immediately see the new menu structure.

If you are an international company then getting them translated and setting them up can be a tedious task.  You can create a Master Menu, use this module to export it to Excel, have it translated, and then re-import it back into E1.

If you are upgrading from the old OneWorld menus to Solution Explorer, then Menu Management provides an alternative method to using the standard E1 Menu Conversion program.

The “MenuPlus” module enables you to revise menus quickly and easily.

And finally, there is the 3WaySuperGrid where you can see roles, menus and security in a grid and make changes to Menu Filters and security.



101

After entering the task view, copy your Excel to the first line's field 'Task Name' and press Form Exit 'Update'

| Internal Task ID | Task Name | Task ID | Task Type | Task Description | Option Code | Product Code | Task Depth | Object Name | Form | Version |
|---|---|---|---|---|---|---|---|---|---|---|
| ALLOUTSECURITY_WITH_A | Generación OT - Restos | ALLOUT0000000003 | 01 | Task | 1 | 31 | 2 | P48013 | W48013J | ARC20002 |
| ALLOUTSECURITY_WITH_A | Generación OT - Retrabajos | ALLOUT0000000007 | 01 | Task | 1 | 31 | 2 | P48013 | W48013J | ARC20003 |
| ALLOUTSECURITY_WITH_A | Generación OT - Fazón | ALLOUT0000000008 | 01 | Task | 1 | 31 | 2 | P48013 | W48013J | ARC04004 |
| 52041C59-EBBF-11D3-99BA | Print and Release Work Order Documentation | BPM973732274636 | 02 | Task | 2 | 31 | 2 | R31410 | | |
| ALLOUTSECURITY_WITH_A | Pegado Ubicaciones | ALLOUT0000000005 | 02 | Task | 1 | | 2 | R5931113B | | |
| ALLOUTSECURITY_WITH_A | Cierre de OT | ALLOUT0000000009 | 02 | Task | 1 | | 2 | R5900078 | | |
| | | | | | | | 0 | | | |
| New | Entrega de Materiales a Planta - Plan de Entregas | | 07 | Folder | | | 1 | | | |
| ALLOUTSECURITY_WITH_A | Generación de Datos | ALLOUT0000000013 | 02 | Task | 1 | | 2 | R5900331 | | |
| ALLOUTSECURITY_WITH_A | Generación de Plan de Entregas | ALLOUT0000000014 | 02 | Task | 1 | | 2 | R590017 | | |
| | | | | | | | 0 | | | |
| New | Entrega de Materiales a Planta - Preparación de P | | 07 | Folder | | | 1 | | | |
| ALLOUTSECURITY_WITH_A | Plan de Entregas (9E) | ALLOUT0000000016 | 02 | Task | 1 | | 2 | P590020 | W590020A | ARC04002 |
| ALLOUTSECURITY_WITH_A | Listado de Piqueo Consolidado (9E) | ALLOUT0000000017 | 02 | Task | 1 | | 2 | R5542520 | | ARC02005 |
| ALLOUTSECURITY_WITH_A | Listado de Piqueo (9E) | ALLOUT0000000018 | 02 | Task | 1 | | 2 | R5542520 | | ARC02013 |
| ALLOUTSECURITY_WITH_A | Listado de Piqueo por Ubicación (9E) | ALLOUT0000000019 | 02 | Task | 1 | | 2 | R5542520 | | ARC02006 |
| | | | | | | | 0 | | | |
| New | Entrega de Materiales a Planta - Entregas de Insu | | 07 | Folder | | | 1 | | | |
| ALLOUTSECURITY_WITH_A | Plan de Entregas (9E) | ALLOUT0000000016 | 02 | Task | 1 | | 2 | P590020 | W590020A | ARC04002 |
| ALLOUTSECURITY_WITH_A | Entregas - Confirmación | ALLOUT0000000024 | 01 | Task | 1 | 42 | 2 | P4205 | W4205H | ARC02045 |
| ALLOUTSECURITY_WITH_A | Recepciones en Almacen | ALLOUT0000000025 | 01 | Task | 1 | 43 | 2 | P4312 | W4312F | ARC02020 |
| | | | | | | | 0 | | | |
| New | Entrega de Materiales a Planta - Retornos | | 07 | Folder | | | 1 | | | |
| | | | | | | | 0 | | | |

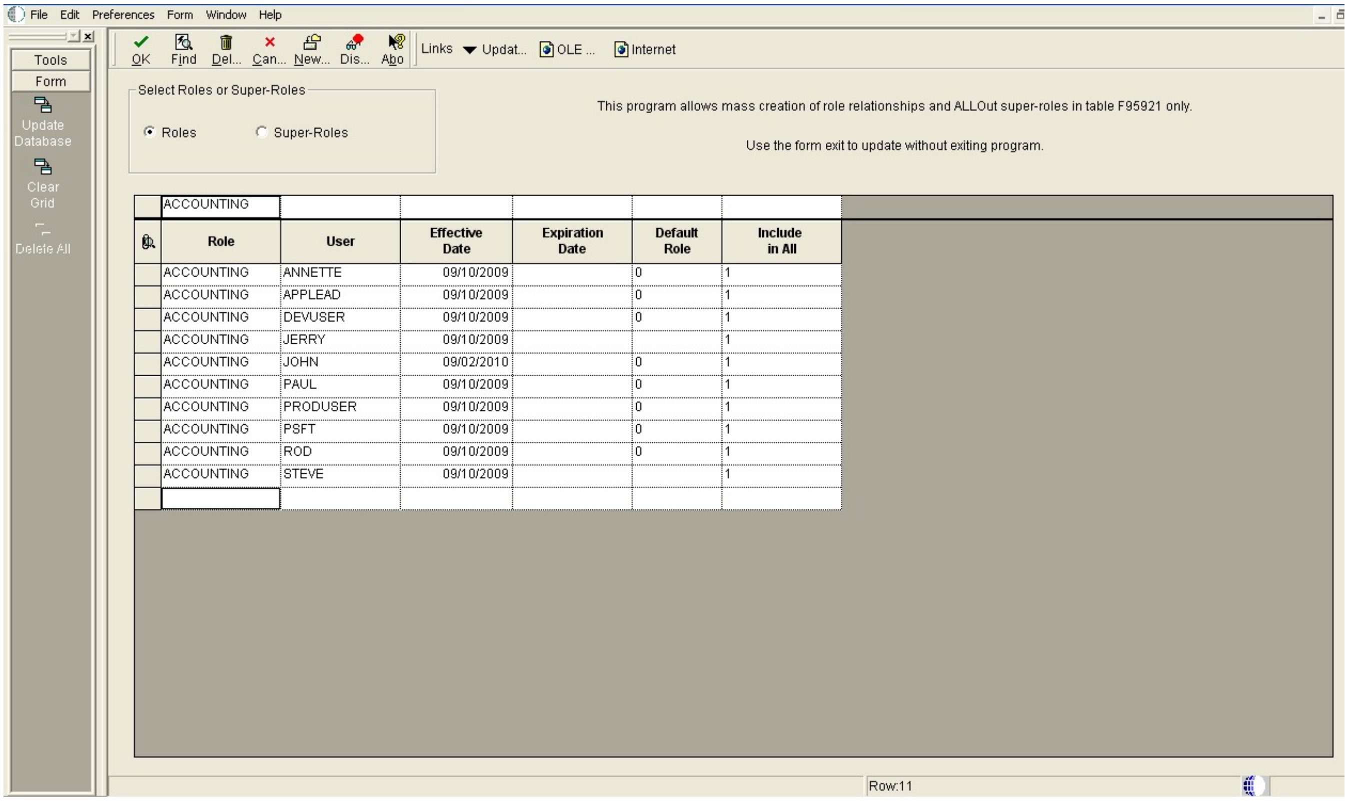
## Profiles – Users and Roles

All E1 sites need User and Role profiles.  You can’t go live without them and setting them up, particularly for large sites, can take a long time and potentially delay a go-live date.

Project+ has a grid that you can use to import large volumes of profiles from a spreadsheet.

You can use the program as an alternative to the P0092 standard E1 program.

You can also set-up and manage role relationships in a grid.  This program is a replacement for the standard P95921 program in E1 where you can only see and work with one user profile at a time.



Select Roles or Super-Roles

● Roles ○ Super-Roles

This program allows mass creation of role relationships and ALLOut super-roles in table F95921 only.

Use the form exit to update without exiting program.

|  | ACCOUNTING |  |  |  |  |
|---|---|---|---|---|---|
| Role | User | Effective Date | Expiration Date | Default Role | Include in All |
| ACCOUNTING | ANNETTE | 09/10/2009 |  | 0 | 1 |
| ACCOUNTING | APPLEAD | 09/10/2009 |  | 0 | 1 |
| ACCOUNTING | DEVUSER | 09/10/2009 |  | 0 | 1 |
| ACCOUNTING | JERRY | 09/10/2009 |  |  | 1 |
| ACCOUNTING | JOHN | 09/02/2010 |  | 0 | 1 |
| ACCOUNTING | PAUL | 09/10/2009 |  | 0 | 1 |
| ACCOUNTING | PRODUSER | 09/10/2009 |  | 0 | 1 |
| ACCOUNTING | PSFT | 09/10/2009 |  | 0 | 1 |
| ACCOUNTING | ROD | 09/10/2009 |  | 0 | 1 |
| ACCOUNTING | STEVE | 09/10/2009 |  |  | 1 |

## Automatic Security set-up - ALLOut Discovery

ALLOut supports the implementation of a “Deny ALL” strategy for Application, Action and Processing Option security.

Appendix A discusses the importance of this strategy.

ALLOut supports a number of strategies for security implementation –

- New-site – security implementation from scratch using menus
- New-site – security implementation from scratch using standard roles
- Existing site – implementing “Deny ALL without the Pain!”
- Existing site – implementing “Deny Critical” – ie – only locking critical programs, not all

## New site security set-up – Deny ALL – from Menus – based on your own 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.

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 Discovery 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 Discovery Grid to load the *PUBLIC *ALL N settings plus all objects that need to be used by all users.
- For each role – use the Discovery 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 – StartOut – Standard Menus, Tab Pages, Roles and Security

StartOut is a spreadsheet with embedded macros that you customize so that you can automatically generate the following –

- Tasks
- Task Views
- Roles
- E1 Pages
- Menu Filtering
- Security – Application and Action security
  - Programs on Menus
  - Programs behind exits

It enables you to follow an "implementation process" so a Project Manager can allocate work to the appropriate application and technical resource and ensure the project progresses in a structured way.

### 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 Discovery 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 Discovery to create the new PUBLIC role
    - Set up Deny ALL for PUBLIC - use the Discovery 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 Discovery 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 supplied) SOD rules into ALLOut.
- For each role – run the Discovery 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 breached 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 Discovery 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. By the way – 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.  The solution is quoted for on a fixed price basis.

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.

## 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:-

Lock-down - users can only access applications that they are authorized to use

Reporting – you can now produce definitive reports of access and update authority

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.