



ProjectPlus

Implementations, Upgrades Conversions and Much More

Table of Contents

SCOPE OF THIS PAPER.....	2
PROJECTPLUS.....	3
MENU SET-UP AND MANAGEMENT	3
PROFILES - USERS AND ROLES	4
AUTOMATIC SECURITY SET-UP - ALL OUT DISCOVERY ...	5
NEW SITE SECURITY SET-UP - DENY ALL - FROM MENUS.....	5
NEW SITE SECURITY SET-UP - DENY ALL - FROM ALL OUT STANDARD APPROVED ROLES (TEMPLATES).....	6
EXISTING SITE OPEN TO CLOSED - DENY ALL	7
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	10
CONCLUSIONS AND RECOMMENDATIONS	10
APPENDIX A: GLOBAL LOCK-DOWN STRATEGY	11
THE ALL OUT FAMILY.....	12

INTEGRATED WITH



JD EDWARDS ENTERPRISEONE

Scope of this paper

This paper focuses on how to use the ALL Out Methodology and Tool-set 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
 - Automatic menu set-up from a spreadsheet
 - Menu management in a grid
 - Menu-filtering in a grid
- Users and Roles set-up and management
 - 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
 - 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 EI 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 B9 – it is the focus of our business and is why we are called "ALL Out".

JD Edwards Versions Supported

The following versions are supported –

- **EnterpriseOne 8.9 to B9**
- **OneWorld Xe and ERP8** – with Solution Explorer
- **OneWorld Xe** – OneWorld Menus

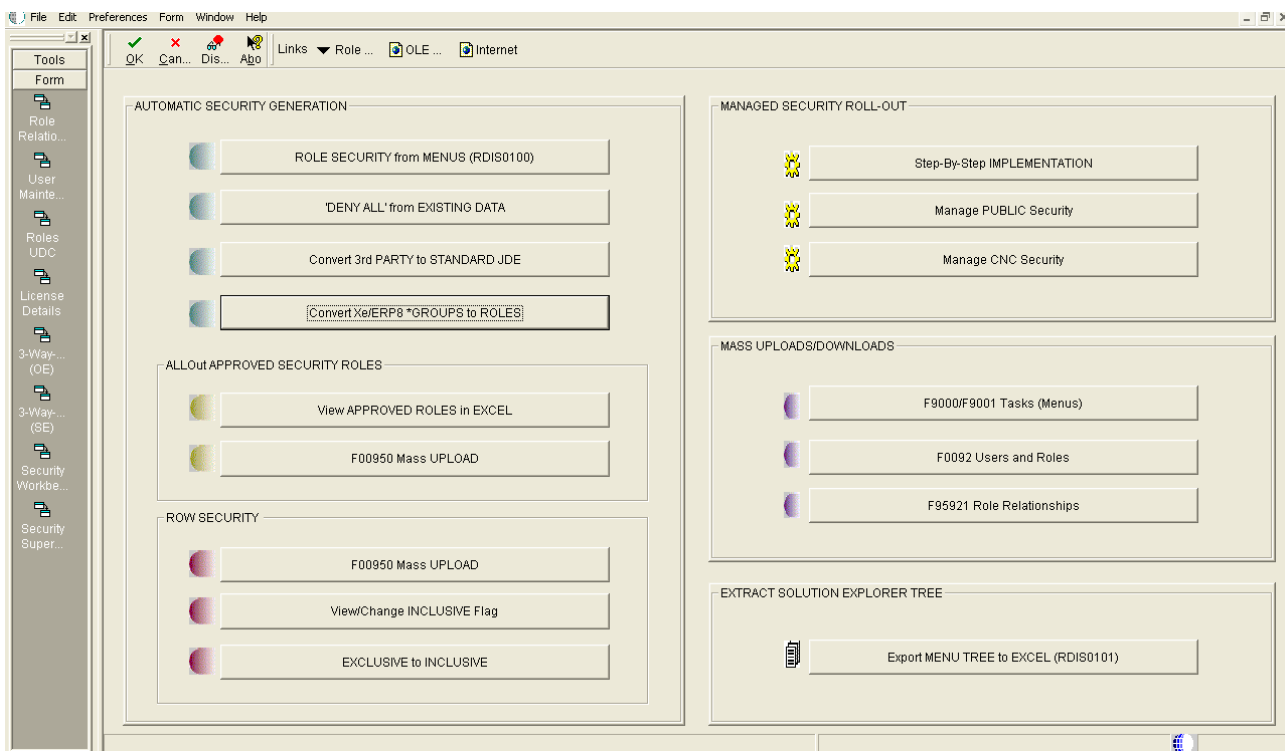
ProjectPlus

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

Only EI 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"



Menu Set-up and Management

All EI 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 Project+ you can create a menu tree in Excel and import it into EI using the grid. Project+ 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 Project+ to export it to Excel, have it translated, and then re-import it back into EI.

If you are upgrading from the old OneWorld menus to Solution Explorer, then Project+

provides an alternative method to using the standard EI Menu Conversion program.

There is also a new "Menu Management in a Grid" feature that 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.

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 EI 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 EI program.

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

File Edit Preferences Form Window Help

Tools
Form
Update Database
Clear Grid
Delete All

OK Find Del... Cant... New... Dis... Ago Links ▼ Updat... OLE ... Internet

Select Roles or Super-Roles

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

Roles Super-Roles

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

Row:11

Automatic Security set-up - ALL Out Discovery

ALL Out supports the implementation of a "Deny ALL" strategy for Application, Action and Processing Option security.

Appendix A discusses the importance of this strategy.

ALL Out 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

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

The next step is to define roles that correspond to each of the business processes. The standard EI 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 EI program is adequate – the ALL Out 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 ALL Out 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 ALL Out Risk Reporting module can be used to achieve this.

New site security set-up – Deny ALL – from ALL Out 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 Discovery.

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.
- Create roles using standard E1 – P0092 program
- Use the Discovery 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 ALL Out 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 ALL Out 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 EI (or for Xe and ERP8 sites, the ALL Out 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 EI 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 ALL Out 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 ALL Out 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, PD4012 (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.

ALL Out 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 ALL Out supplied) SOD rules into ALL Out.
- 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 ALL Out 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 EI 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 ALL Out 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 ALL Out Consultant.

The client needs to send ALL Out 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.

Q Software to standard EI conversion

The Q Software product maintains security in external security tables.

The product was developed in the days of Xe – one user one group.

Most of the functionality of the product is now handled in the later releases of standard EI.

If there is any functionality that cannot be handled by standard EI, then ALL Out has equivalent functionality that can handle the task much more simply than the Q product – such as -

- Row security multiple role enablement

- Roles within Roles

- Action code conflict management

ALL Out has a program that will do a mass conversion of Q components and functions to standard EI roles (or ALL Out Roles within Roles).

These programs will be run by an ALL Out Consultant.

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 EI 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 – **ALL Out 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 **ALL Out 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 ALL Out Security for product information and to register for a public webinar.

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

Email: Hazel@alloutsecurity.com

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 EI 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.

Product briefs are available for each of the ALL Out Modules listed

The All Out Family	
Risk Reporting	Addresses access reporting & creates segregation of duties rules
3 Way SuperGrid	Fine tunes role based security & reviews/resolves complex multiple roles
950 SuperGrid	Replaces standard P00950 program and allows easy update of F00950 table settings
ProjectPlus	Automatic generation of menus, profiles and security settings & customization of action security
Risk Management	Creates rules for SOD between roles and keeps track of role allocation
CombiRoles	Identifies conflicts for a user and combines small roles into Super Roles

For more information:

sales@ALLOutSecurity.com

or visit www.ALLOutSecurity.com