



WHITE PAPER

Managing JDE security Compliance in World

“Automate your audit with SOXLock”

Table of Contents

PART 1: SOXLOCK - THE “ACE IN THE HOLE FOR SOX”	3
PART 2: SOX COMPLIANCE IN 4 EASY STEPS.....	3
PART 3: ADDITIONAL BENEFITS OF THE ALL OUT SOLUTION AND SOXLOCK SECURITY.....	4

INTEGRATED WITH



JD EDWARDS WORLD

This paper focuses on the requirements of the Sarbanes Oxley legislation as it affects users of JD Edwards.

Part 1 introduces the ALL Out World product and the concept of Application Security (SOXLock) – the ability to lock all types of individual programs – particularly the ones that JDE does not lock. It also discusses the importance of “Deny ALL” and shows how SOXLock security enables its implementation.

Part 2 shows you how you can achieve SOX compliance in 4 easy steps –

1. Discovery
2. Lock using the SOXLock
3. Report –
 - a. Base Compliance Report – “Who can access what and what can they do when they get there?”
 - b. Segregation of Duties rules and report
4. Resolve – taking away SOXLock and Action security so you can easily sign-off with no outstanding issues

Part 3 discusses additional benefits of the system-

- Applying “Deny ALL” security for action code in a day.
- Implementing simple change control procedures
- Managing application and action security in one place
- Implementing Group level security and managing variations

Part 1: SOXLock – the “Ace in the Hole for SOX”

People familiar with EnterpriseOne or SAP will have heard of Application Security and know that it is the cornerstone of a security implementation in those environments.

You set up a list of programs that a user is authorized to access and then you lock them into the list.

It is simple, effective and addresses all the fundamental control issues in an ERP system such as “Deny ALL”, change control, access reporting and segregation of duties.

The SOXLock feature of ALL Out Security delivers application security for World.

What is more – it sets itself up automatically – you just turn it on in discovery mode and in a few weeks you can start locking users down.

You have one *PUBLIC *ALL “N” setting (the “Deny ALL”) and all the rest are “Y” settings.

No wonder customers call it - “Ace in the Hole for SOX”.

And this is why a “Deny ALL” strategy puts you ahead of the Auditors. Many haven’t realized yet but all those massive reports you produce of menu access or function key routes are meaningless.

With SOXLock you can produce a short, reliable and instant report and be 100% confident they will not be able to question its veracity.

Part 2: SOX Compliance in 4 easy steps

You don’t need to change your menus, worry about function key exits, or who has menu travel fast path, hidden selections or any of that complexity.

Just leave your existing system as it is.

From now on the foundation of your security is going to be SOXlock Application Security and standard Action Code security.

Step 1 – Discovery mode - when you load SOXLock into your system it immediately starts to operate in Discovery mode. It looks at all the programs your users are accessing and builds a permissions list.

Step 2 – Lock – after a few weeks you can start to lock users down and begin producing the SOX reports.

Step 3 - Report – you will need two SOX compliance reports

Base Compliance Report - “All programs a user can access and what action code security they have when they get there.” This report will be from one to a few pages long.

Segregation of Duties Rules and Reports – you will review the sample rules (37) delivered with the product and start to apply them to the permission lists and assess their impact. These reports will, hopefully, be short. Eventually you want them to be blank!

Step 4 – Resolve – if you find issues you are going to want to take away SOXLock security and action code security. You may have to review your internal procedures and re-assign some tasks but you have at least achieved the first hurdle of reporting the issues and having the tools to start doing something about it.

Part 3: Additional Benefits of the ALL Out solution and SOXLock Security

Applying "Deny ALL" security for action code in a day.

It sounds impossible, but, with care, it is easy. Customers have implemented the global *PUBLIC *ALL NNN setting for 700+ user environments in a day with no complaining phone calls!

The problem with implementing the global lock-out for action security is knowing which programs users are actually accessing so that you can convert default "Y" into an actual "Y". ie - you need to create records in the F0003 file for each user/program combination with an actual "YYY" setting.

With SOXLock you know the programs people are using and so creating the "YYY" settings is easy.

Implementing simple change control procedures.

Put a stop to random program creation or version creation. SOXLock global lock-out makes it easy to insist a user gets management approval before a new program or DreamWriter version is created.

And we have a new feature that grants temporary access to a new object so you do not disrupt operations while the required authorizations are obtained.

Managing application and action security in one place.

You will use a single screen to manage both SOXLock Application and standard JDE Action Security. The screen shows actual settings and inherited settings and is color coded so it is easy to see inheritance and make the necessary changes either at user, group or *PUBLIC in one place.

Implementing Group level security and managing variations.

In large organizations where many users conform to standard procedures you will want to manage security at a group level. When doing this many JDE users have a "Group Level Only" policy. SOXLock security management screens make it very easy to manage changes at a user level that do not conform to a group. In this way you can reduce the number of group profiles with one user in.

THE ALL OUT FAMILY FOR JDE WORLD	
SOXLock	Critical process lists and SOD rules set up and reporting and security management.
STARGROUPS	Functional and business unit security groups. Links users to multiple groups.
PROFILE+	Copy, change and delete profiles "in one click".

For more information:

sales@ALLOutSecurity.com

or visit www.ALLOutSecurity.com