OneWorld® Security

An Overall Strategy

By Alex Rippingale, QS Software International Ltd.

Introduction

E1 With the onset of Application Security in OneWorld, JDE® has gone a long way towards enabling a totally secure system, which, it could be argued, was virtually impossible using the tools available in WorldSoftware. Using Application Security in OneWorld enables you to deny access to any application (both Interactive and Batch) with a simple Y/N lock.

The requirement for a security strategy in World meant taking a large number of security features into account to develop a comprehensive security strategy. This is still the case in OneWorld. However, due to the ability to deny or grant a user access to an application, the basis for two different approaches to security becomes immediately apparent.

Your Security Officer can adopt a strategy of locking the whole system down with one value, so that it is totally secure, and then granting back the necessary applications to the relevant users. Or they can maintain the JD Edwards policy of allowing access to the whole system and securing critical applications individually or via access control (using custom menus and blocking hyper exits) in a similar vein to World. The advantages and disadvantages of the two strategies are discussed below, as well as other areas for concern that are irrelevant to which security strategy your organisation wishes to adopt.

1. Application Security – Off (Secure All Applications)

Securing all applications and then granting access to only those applications required by a user seems like a very simple solution to anyone who has considered security. It is an attractive strategy to those users who have used World and who are security conscious. There are, however, drawbacks in using this solution which will be discussed in detail below.

The value required to apply this method is Application Security *ALL NN applied to the *PUBLIC profile. This will effectively not allow any users to employ any applications throughout JD Edwards. For users to be able to work with JDE means that each user needs to be given Application Security YY for each application that she needs to do her job. Your Security Officer will need to have a matrix/list of all programs that all users or user groups require.

Advantage

The benefit of this strategy is that wherever users go on your system they cannot use applications to which they have not been specifically granted authority. This makes Access Control virtually redundant, as it is irrelevant which Menus and/or Exits a user can employ. There are limitations

to this, as some applications have a number of forms, some of which are sensitive and access to which you would want to restrict. If a user has been given authority to an application like this, then he can get to all of its forms unless application security is applied to specific forms. This will not be a global problem, however, as in the vast majority of situations this is not the case.

Another advantage of this approach is the simplicity of an audit. Due to the fact that the entire system has been locked and access may only be granted explicitly, an audit would entail listing all the security settings applied at the *PUBLIC, group, and user levels. The auditor would know that there would be no danger of a user getting access to critical applications by way of unsecured exits.

Disadvantage

Difficulties come in the actual use of the system, as there are many hidden programs that run behind the main JDE applications. Unless access to these is granted, some processes will either fall over or do not complete properly, sometimes without notifying the user, which could lead to integrity issues as a result.

Action Code Security

Action Code security is familiar to World users and is essentially the same within OneWorld with the addition of the Copy, OK/Select, and Scroll to End options added to the Add, Change, and Delete options.

Inquire Only

A *ALL Inquire only (NNNYNY) value can be applied to the *PUBLIC profile so that no user can employ an Interactive Application to update. Those users that require the Update capability can then be given it where necessary. Confidentiality issues still need to be dealt with via Row Security or denying access to sensitive applications.

The benefit of this is that, if you are using *ALL Application NN, you only need to grant Action Security to a portion of those applications that you have already granted back to your users. Therefore, from a security standpoint it is very secure, and from a maintenance angle it is relatively simple to implement. Problems come in a few instances where some applications (such as confirmation windows) need to have Action code YYYYYY granted where it is not immediately obvious for you to do so. These become apparent when using the system, however, and should be picked up in testing.

All Update

Leaving JDE without any Action security or by placing a *ALL Update (YYYYYY) value against *PUBLIC will have the same effect and mean that any user who can reach an interactive application will be able to use it to update, which is not a secure methodology. If you have used the Secure All Applications methodology and then allowed full access to all actions, the security officer would need to restrict the actions of all the applications where the user is only permitted to inquire. This approach leaves a lot of room for error and could be time consuming.