ALLOUT Security

WHITE PAPER

Implementing Multiple Security Tables in JD Edwards E1

INTEGRATED WITH
ORACLE
JD EDWARDS ENTERPRISEONE

Abstract

The JD Edwards EnterpriseOne product suite is delivered with a single security table (F00950) that is utilized across all environments. This provides for a simple and consistent means of controlling access to objects regardless of the environment being used. However, there are instances where having multiple security tables would be advantageous. We will discuss the process for implementing multiple security tables.

Scope

This document is intended as a high-level overview of the concepts, processes, and options involved in implementing multiple security tables. This process is platform and database agnostic. This document is NOT intended as, and should not be used as, a detailed guide to this process. If you are considering implementing multiple security tables you should engage the services of an experienced CNC technical professional.

Multiple Security Tables

JD Edwards EnterpriseOne has undergone many name changes over the years, but one thing has remained constant: the use of a single security table to control access to all of the E1 objects and data. Wouldn't it be nice to let your Business Analysts log in to Development with full access and then log in to Production with different access that is limited to the specific areas they are responsible for supporting?

Security by environment

The process to create a second or even third security table is relatively simple and straightforward. The basic process is this:

1. Backup your existing F00950
2. Generate the F00950 in your desired datasource (NOT System)
3. Copy the F00950 from System to your desired datasource
4. Create & activate OCM entries to point to the 'new' F00950

Generate the F00950

The first step in this process is to create an empty F00950 and associated index files in your target datasource. You will need to determine where this new security table will reside. If you are implementing the secondary table for Development only, the logical choice is in DV Business Data. However, if you do this, be aware that you will need to backup the table prior to any data refresh activities and then restore it after the data refresh is complete. A better location for the new security table is in the Central Objects since they are not typically refreshed.

To generate the F00950, go into OMW and add the F00950 to your default project. Go into the design tools and then into table operations, and select ‘generate table’.

CAUTION

When you select 'generate table', the existing System datasource is pre-filled in the form. DO NOT click OK until you have changed the datasource to your new table location.

Once you have entered the appropriate datasource, click OK. This process will generate the table and indexes. Verify this has completed successfully by opening UTB and opening the new table.

Copy the F00950

Now that you have a valid F00950 in your new location, you can utilize your Database tools to copy the data from your original table to your new table. Contact your DBA to schedule this work. Performing this copy at the DB layer is much faster than utilizing the E1 copy table UBE.

Create OCM

You will now need to create the OCM entries for users/roles to be able to utilize this new security table. OCM entries are required for the System map as well as for each Server Map included in your installation. The method to create the entries is the same whether being created for system or server map tables. To create the entries required to utilize this new security table, go into OCM and click add. Fill in the appropriate values for Environment, Object Name (F00950), Primary Data Source (DV Central Objects is recommended), System Role (this can be either the E1 user or the Role). Select OK when complete. Once all of the required entries have been created, find the new entries and activate them.

CAUTION

You must create matching entries for both System and server map OCM tables or you will get unexpected results when users are logged in.

If you are creating OCM entries at the role level, be careful of assigning roles that are using the original F00950 as well as roles that are using the new F00950 as this will result in unexpected results while users are logged in.

Things to Consider

Before embarking on a journey with multiple security tables you need to be aware of a few things. Your end users that are logging into Production and non-production will need to understand that they may be looking at different security tables for each of their logins.

Dual Maintenance

Once you have implemented multiple security tables and you want to make changes to either of the security tables, you will need to be logged in with a role/user ID that is pointed to the version of the F00950 you want to modify. You will not be able to modify both tables from a single login. If you are using a single ID and constantly switching your own OCM mappings on and off, you need to be careful about which mappings are active when you make specified changes to security. This effectively means you are performing dual maintenance of your security tables when moving changes from one table to

the next. ALLOut Security provides several options that can assist in this manner to streamline, but not eliminate, the dual maintenance requirements. Please contact Sales@ALLOutSecurity.com for more information.

Open to Closed

If you are implementing dual security tables to assist in going from open to closed security, ALLOut Security has an entire suite of products and methodologies designed to assist in this effort. By utilizing a combination of security change control as well as other features and methodologies, you can easily transition your users to a closed system in a controlled process with little or no disruption to their daily activities. Please contact Sales@ALLOutSecurity.com to schedule an online overview of our capabilities.

Change Control

If you are implementing dual security tables to provide security change control for your company, you could end up in a situation where you are performing dual maintenance of your security tables. This can be a cumbersome and time consuming process, even when utilizing the ALLOut tools to streamline the process. Rather than performing dual maintenance, ALLOut Security offers E1 clients Security Change Control. When utilizing Change Control from ALLOut, you make changes to security in one environment and promote it to production. You also end up with a record of the changes made as well as the date of the change. For more detailed information, including a whitepaper, contact Sales@ALLOutSecurity.com

Conclusion

Implementing multiple security tables or security by environment is a relatively straight forward proposition and can be easily accomplished. You will need to decide for yourself if the additional maintenance and troubleshooting outweighs the benefits gained by being able to make changes to security and test before impacting your production users. As with any technical undertaking that affects your business users, it is imperative that you open a dialogue with your business users and explain the pros and cons of the approach and gain their buy-in before starting the process. Done properly, security by environment will go unnoticed by your end users.

Customer notes

If you are implementing multiple security tables it is highly recommended that you make and secure a backup of your F00950 table before beginning the process. It is also highly recommended that customers engage the services of an Oracle certified partner that specializes in CNC work.

For a list of partners that ALLOut Security recommends and works with, please review our website: www.alloutsecurity.com