

SECURITY MANAGER PRO

Managing security in JD Edwards EnterpriseOne can be extremely complex and time-consuming, with lots of repetition and duplicated effort.

In an attempt to overcome this, many organizations use spreadsheets to manage Task Views, Roles and Security, but this approach is also beset with problems. Spreadsheets are notoriously prone to errors and it can be difficult to monitor changes made and be sure that you have the correct version, leading to the risk of inadvertently building problems into your live security table.

One of the main reasons for investing in an ERP system was to consolidate your enterprise data into a single environment. It doesn't make sense to manage security – critical to protecting your business and preserving the integrity of your data – by means of external, potentially unreliable spreadsheets.

SECURITY MANAGER PRO IS COMPLETELY INTEGRATED INTO THE JD EDWARDS ENVIRONMENT. IT COMPRISES A SET OF CUSTOM PROGRAMS AND TABLES THAT ENABLE YOU TO MANAGE YOUR SECURITY VERY EFFICIENTLY AT THE ROLE LEVEL.

You can import spreadsheets, but the data is then held in custom programs and tables that enable you to manage your security very efficiently at the Role level.

- Access to security programs and tables can be restricted to authorized users
- Any changes made are fully auditable
- Everything you do is stored in tables within your ERP system and can be reported upon using our tools or your preferred reporting solution
- There's never a need to search for the right spreadsheet or worry about version control.
- You can be confident in the integrity of your security and in the knowledge your reports are always based on accurate information rather than exported spreadsheets

Whether you are implementing JD Edwards EnterpriseOne 9.x from scratch or upgrading from an earlier release, Security Manager Pro can help you manage your security more efficiently yet more rigorously. You can:

- Implement new security from scratch, automatically generating security from your Task Views for rapid implementation and easier ongoing management
- Import existing security from your current F00950
- Import existing Task View information from spreadsheets
- Manually enter security into a standard JD Edwards grid

Whichever method you choose, you then:

- Refine and/or rework the security as appropriate using our productivity tools
- Check for Segregation of Duties or Multiple Role conflicts to eliminate potential loopholes BEFORE you build your new security table
- Set defaults for Exits, Associated Objects, Hidden Programs and UBEs



BENEFITS

- Easy to use
- Align security to your Task Views to make it easier to manage
- Automatically generate security to match your business processes
- Simplified, seamless management of all security types, including User Defined objects
- Import your existing security or spreadsheet data
- Proactive Segregation of Duty checks
- All security changes are fully auditable

MAIN FEATURES

PREBUILD SECURITY

In the same way that you test new programs before deploying them live, we believe that you need chance to validate security settings before writing them into your live F00950 table.

With **Security Manager Pro**, all security settings are stored in a PreBuild table – a custom table held within your JD Edwards environment. This allows you to run automated checks to identify Segregation of Duties or Multiple Role conflicts that would be introduced by the proposed access permissions.

As you refine your security settings you can build the live security Role by Role or for a group of Roles. When settings are updated, profiles are flagged to show whether the latest changes have already been built into live security or not.

With **Prebuild** you can validate security changes and be confident they won't disrupt operations or create loopholes in your live security.

SECURITY COMPONENTS

We believe that Roles Based Access Control is the most efficient way to manage security – and we allow you to take it one stage further.

Many processes (eg. Address Book Maintenance) need to be made available to several different Roles. With Security Manager Pro you can define such processes as Security Components then add them to as many Roles as required. If the process needs to be changed, you simply update the Component and all the affected Roles are automatically flagged. You can then check for conflicts before you commit the changes to live security to avoid unintended consequences.

Security Components enable you to:

- Set up new users very rapidly
- Make security changes in minutes
- Reduce the workload and complexity of defining and managing security.

USER DEFINED OBJECT (UDO) SECURITY

New security types were introduced in JD Edwards EnterpriseOne to support UDOs such as E1 Pages, One View reports, Grid Formats and Watchlists. Security records for these UDOs are held in a second security file (F00950W), making security management even more complex.

In QSoftware V5.2, we have introduced a UDO Component type, so that users can set up reusable UDO Security Components and add them to Roles and/or Users alongside standard Security Components. All the security records are automatically written to the correct tables.

The Component approach makes security management seamless for **all** security types.

ROW SECURITY

You can also use Components to manage Row Security very efficiently. Each location or business unit can be set up as a Component and attached to relevant Roles/Users, removing the need for it to be repeated and maintained within every Role.

Defining Row Security as Components makes it much easier to manage.

SEGREGATION OF DUTIES (SOD)

We supply pre-seeded "Top Ten" SoD Rules, as recommended by leading auditors, which you can adapt to reflect your own SoD policy. The rules can be as granular as you need and there is a rule type that allows you to monitor access to Critical Objects, which are particularly risky processes in their own right.

To reduce the number of false positives, you can apply mitigations, with start and end effective dates, when you need to make temporary exceptions to cater for vacations or other absences.

Proactive SoD Management:

- Reduces the risk of unauthorized access going undetected
- Reduces the workload and complexity of achieving compliance.

APPLICATION SECURITY NET EFFECT ENQUIRY: ROW SECURITY NET EFFECT ENQUIRY

These queries enable you to quickly find out whether a user can access particular applications or data items, and at what level the prevailing security is held.

They display the applicable security settings at all levels (ie *Public, Role and User) and calculate the Net Effect to show you whether the User can access the specified item or not.

IMPORT FROM SPREADSHEETS

If you currently hold Task Views in spreadsheets, you can import them into the Prebuild table.

Native JD Edwards functionality validates the data on import, reducing the risk of carrying errors into your live security.

SINGLE EASY-TO-USE CONSOLE

Security Manager Pro's user interface makes it very easy to view and manage Task Views, Security and Profiles all in one place – so you no longer need to keep jumping between different programs to check settings and apply changes.

Depending on your preference, you can manage the elements in a tree structure or a grid.

Managing security, Task Views and Profiles in one place is much quicker and easier.