AutoSecure for JD Edwards EnterpriseOne

The fast route to compliant, Role-based Security
Import, customize and be ready to test within hours

Implementing or overhauling the security in your JD Edwards system can be a daunting task.

Whether you're concerned about the ongoing cost of security management, or worried about potential weaknesses, the answer usually involves implementing an efficient, sustainable Role-based Security Model.

But designing Roles from scratch can take a lot of effort and time, and it's crucial to collaborate with the Business – after all, they need to decide which users need to access which tasks.

AutoSecure harnesses the knowledge of security and audit experts to reduce the effort needed. It populates Security Manager Pro (SMP) with predefined Roles and Segregation of Duties (SoD) Rules, reducing security implementation costs by automating around 80% of the workload.

Efficient, sustainable, scalable security with minimal effort upfront

AutoSecure is an automation tool which enables customers to create a Best Practice, compliant Role-based security model very quickly, using Seeded Roles and SoD Rules.

The base model can be enhanced to include security for custom applications and checked for SoD conflicts before deployment, then tested and tuned to your own business processes during user acceptance testing.

It offers a pragmatic yet scalable solution for companies who just want to get effective, manageable security in and working as quickly and easily as possible, including:

- New JDE users implementing for the first time
- Existing JDE users who want a security redesign.

To find out more or request a demo, email sales@qsoftware.com or visit www.qsoftware.com

Benefits

- Very rapid implementation of Role-based security – be ready to test within a few hours
- Don't reinvent the wheel – use Best Practice Roles and SoD Rules designed by experts
- Roles are automatically selected for all the JDE modules you use
- Involve the business - meaningful names give all users a clear view of the tasks within the Roles
- Implement sustainable internal controls from the start, with built in SoD and Sensitive Access rules
- Proactive compliance – identify and resolve conflicts before you deploy the security
- Security can be fully tested and refined as part of your system/user acceptance testing process
- Minimal risk of access problems at go-live
- Holistic, efficient risk management – integrated solutions available for User Provisioning, SoD/Audit Reporting, Periodic Access Review and Fraud Detection.

Features

AutoSecure comprises:

- Seeded Roles covering a wide range of job functions. The Roles have been created by experienced JDE security and audit consultants
- Predefined Industry-specific Roles for Real Estate, Manufacturing and Distribution
- Security Components with business-friendly names. These contain the detailed security settings for all the tasks within the Roles
- Seeded SoD and Sensitive Access Rules created by experienced JDE audit consultants (optional)
- QCloud: the Cloud-based system behind AutoSecure. It provides the dashboard, manages the automation, and holds the Seeded Roles, Rules and Security Components.
- Security Manager Pro (SMP), co-located with your JDE system (i.e. on-premise, hosted, on OCI, AWS, etc). SMP builds the live security file which manages access to JDE applications. It also provides many utilities to help you manage security very efficiently throughout the lifecycle of your JDE system
- Optional consultancy to help you tailor the Roles to meet your specific needs.

How does AutoSecure work?

1. **Log in to QCloud to request Seeded Roles and Rules**
2. **Import**

- AutoSecure analyzes your ERP usage to identify which JDE modules (SKUs) you're currently using, or you can select all the modules that you plan to use from a list of all JDE modules.
- Next, you'll see a list of all the Roles available for the modules you selected. Accept all the recommended Roles or deselect any that you don't need.
- AutoSecure then fetches the required Roles, Functions and Components from QCloud and sets them up in SMP.
- (Optional) You can also request Seeded SoD Rules for the Roles you have selected, and push them to SMP.

3. **Customize**

- Add security for any custom developed applications and custom created versions.
- If required, create data security components to define rules for which data Users can access (for example, data belonging to a specific business unit or location).

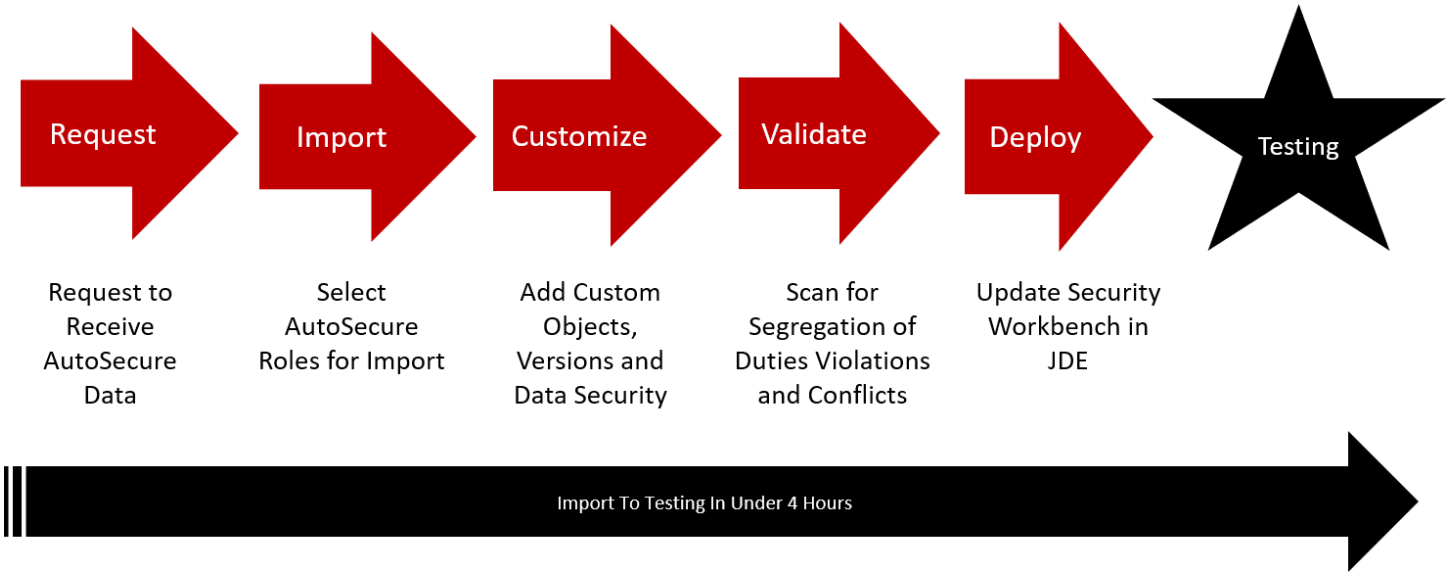
4. **Validate**

- The next step is to create test User IDs and assign appropriate Roles to them.
- Use SMP to scan for SoD violations or other security conflicts that need to be resolved prior to deployment.

5. **Deploy**

- Then you're ready to deploy the Roles to the JDE Security Workbench. This step populates the live JDE security file (F00950) with all the required records.

To complete your security model, it's important to test and tailor your Roles to reflect your specific organizational structure and business processes, ready for go-live. We can offer advice and guidance to help you to do this.



QSoftware

US Headquarters
5889 Greenwood Plaza Blvd, Suite 401
Greenwood Village, CO 80111
Tel: (720) 390 7970

UK & EMEA Headquarters
Connect House, Kingston Road
Leatherhead KT22 7LT United Kingdom
Tel: +44 (0)1372 700850

Integrated with ORACLE Cloud

ORACLE Gold Partner

www.qsoftware.com