



Product Family for JD Edwards EnterpriseOne

Q Software Security and Audit Solutions for JD Edwards EnterpriseOne

Your JD Edwards system is one of your most valuable assets, so it's important to protect it.

But with many business-critical demands on IT resources, we often find that security initiatives are continually postponed – until either auditors intervene, or fraud happens.

You need security to be efficient and reliable, so that it does its job with minimal burden on your IT team.

With almost 3 decades' experience in JDE security and audit, our solutions are designed to help you manage JDE risk and fulfil your audit obligations efficiently.

Our Business-friendly solutions also promote better collaboration between IT, Audit and the Business, empowering all staff to exercise their expertise and get the job done quicker.

Here's a brief overview of our integrated suite of on-premise and Cloud-based risk management solutions, which enable you to cut the cost and effort of managing security and audit.

Security Audit & Analysis

QCloud Security Audit

If you're unsure about the effectiveness of your security, or if you suspect there are weaknesses, but find it difficult to pin them down, QCloud can quickly and easily give you the information you need to find and fix the problems.

It's a Cloud-based audit service which analyzes your JDE security and Segregation of Duties (SoD). Simply log in to QCloud, request an audit and the results are delivered within hours. The only technical effort needed is around 30 minutes for installation, followed by a half hour training session

for users to find their way around, and then you can receive accurate results and insights whenever you need them.

It reports on:

SoD violations: View by user or by SoD rule, with interactive queries so you can drill down to find the details of what's causing the violations.

Critical Master Data: Shows users who can access master data or key system configuration data, where inappropriate changes could enable fraudulent activity or jeopardize the integrity of your system and result in financial misstatements.

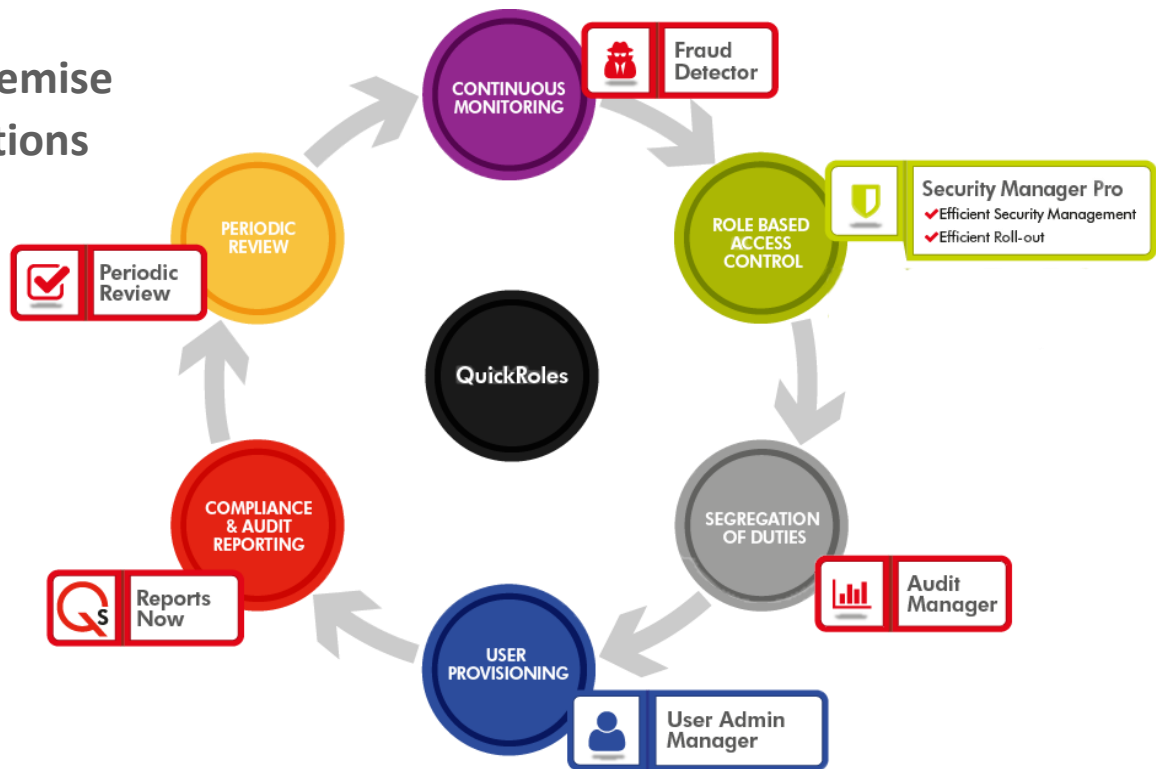
General Security: Provides metrics on the state of your security and helps you to clean up by identifying redundant items that could be hijacked and abused.

Data Security: Metrics about Row and Column security help you to identify excessive use, which could impact system performance.

QCloud analysis and reporting encapsulates our deep experience of working with JD Edwards security. It shines a light on vulnerabilities that many people overlook.



On-Premise Solutions



Security Management / Role-based Access Control

Organizations have different security needs and priorities. However you prefer to manage your security, our solutions help you to cut cost and effort.

QuickRoles:

Many JD Edwards clients understand the efficiency benefits of Role-based security, but designing Roles from scratch can take a lot of effort and cost.

QuickRoles is a new automation tool which captures the knowledge of security and audit experts to help you get up and running very quickly.

It provides predefined Roles and Segregation of Duties (SoD) Rules, creating up to 80% of your security within a few hours, ready for you to test and tailor.

QuickRoles offers two alternative routes to Role-based security:

QuickRoles for F00950

For users who like the simple grid approach of Security Workbench, QuickRoles writes Role security records directly to the F00950 security table.

It's bundled with our new QuickSecure solution, which gives you productivity and troubleshooting tools to manage security directly on the F00950 much more efficiently.

QuickRoles for Security Manager Pro

For users who want to take advantage of advanced tools for ultra-efficient security management and proactive SoD checks, QuickRoles populates Security Manager Pro's PreBuild tables.

Security Manager Pro

Designed for organisations who need to:

- Minimize the cost and effort of ongoing security management
- Reduce risk and remediation effort by running preventive Segregation of Duties checks to identify SoD conflicts before security is assigned.

Key benefits and features include:

Ultra-efficient security management - Components

Where you have common processes that need to be carried out by many different users, it can be tempting to define them as a Role, which is then assigned to all the relevant users.

This can mean that users end up with many roles, making it difficult to ascertain exactly what access rights they have, as well as to identify SoD and role sequence conflicts.

SMP allows you to define security in Components, which can then be included in all the relevant Roles. If the process changes, you only need to edit the Component, then deploy security for the affected Roles.

Better Visibility

SMP organizes your security in an expandable tree structure, giving you a much clearer picture of a Role or User's access rights, with interactive views so that you can drill down to the details.

Test and validate before you assign live security - PreBuild Security

Just as you test new applications before deploying them, we believe it makes sense to validate security before you write it to your live F00950 table.

As you design your security, it is stored initially in PreBuild tables (custom tables which are held within your JD Edwards environment). This allows you to validate security changes before you deploy them, and avoid the risk of disrupting operations or creating loopholes in your live security.

Avoid introducing unidentified risks - proactive SoD checks

Integrated SoD rules and our PreBuild approach mean that you can run automated checks to identify any Segregation of Duties conflicts that would be introduced by security changes before you deploy them.

Spend less time managing security - advanced productivity and troubleshooting tools

SMP includes many tools and utilities to help you manage security and investigate problems more efficiently. For example, the Net Effect enquiry rapidly gives you a definitive answer on what access a user has to a particular object, taking all their roles into account.

QuickSecure

QuickSecure is designed for JDE customers who like the Security Workbench grid approach, but need utilities and automation to reduce the workload and potential for errors and omissions.

It uses a simplified grid system to write standard security records directly to the live F00950 security table and UDO security records to F00950W. It also provides productivity and troubleshooting tools so that security administrators can do a thorough job with a lot less hassle.

Key benefits and features include:

- Familiar approach, but much easier to navigate and use

- Huge time savings
- Much less repetition
- Easier to see the important info without constant scrolling
- Powerful utilities reduce the manual workload
- Better visibility over what a Role or User can access
- More reliable security – less prone to human error or omission
- Easier, quicker problem investigation and resolution
- Full audit trail of who changed what and when.

Watch a video on how QuickRoles works with SMP and QuickSecure [here](#)

Segregation of Duties

Audit Manager

However you manage your security, Audit Manager analyzes your live security table to identify SoD violations that exist in your system – i.e. users who have access rights which enable them to violate your SoD policies.

Where violations are found, you can drill down to investigate them and, if appropriate, apply fully documented mitigating controls.

Supplied with seeded SoD rules which you can customize to meet your needs, it enables you to maintain your SoD model securely within your JDE environment.

Key benefits and features include:

- Automated SoD analysis and reporting saves time and improves accuracy
- Regular detective SoD reporting reduces the risk of fraud or costly error
- Pre-seeded rules speed up the implementation process
- Mitigations eliminate many false positives
- Helps you keep your system in good shape, reducing the time needed to prepare for audits.

User Provisioning

User Admin Manager

User Admin Manager (UAM) enables users to submit requests for Roles and it uses a configurable workflow to automate the process of approving and provisioning them, reducing the workload and paperwork involved.

It can prevent SoD violations by checking for conflicts before Roles are assigned, where required, and it keeps a full audit trail of activity as evidence for your auditors.

UAM also includes productivity tools which:

- Make routine User and Role administration and clean-up tasks much quicker and easier
- Provide a much faster way of setting up large numbers of users and assigning Roles during implementation or acquisition projects.

Key benefits and features include:

- Automation reduces the turnaround time for Role requests and eliminates paperwork
- Proactive SoD checks avoid unintended SoD conflicts, reducing risk and remediation work
- Enables the Business to take ownership of User Provisioning:
 - They specify and approve the Roles their users need
 - They control the timing of the request/approval/assignment process
- Less work for technical IT staff
 - No need for them to be involved in Role requests
 - User set-up, maintenance and clean-up tasks take much less effort and/or can be delegated
- Audit trail provides evidence that all provisioning activity is appropriately authorised
- Empowering the Business leads to a better relationship with IT.

**Watch a short demo of
User Admin Manager [here](#)**

Access Reviews

Periodic Review

Our Periodic Review module enables users to conduct regular access reviews with a fraction of the time and effort. It provides evidence to auditors that access has been reviewed and signed off by the Business.

It enables you to conduct reviews of:

User Profiles

Review information about Users and their Roles. You can:

- See which roles are assigned to Users and check that they are appropriate (P95921)
- Find out which Users were added, changed or deleted, and ensure that the User ID aligns with the full name from the Address Book (P0092)
- Confirm that the User's status (enabled/disabled) and the proxy ID is correct (P98OWSEC).

Security Workbench

Review information from the live Security Workbench (F00950) and User Defined Objects (F00950W) tables, to check that the security granted to Roles/Users is appropriate.

Key benefits and features include:

- Produce review reports with the touch of a button
- Present business managers with clear information which they can understand and review much more easily
- Capture data on approvals, rejections and explanatory notes directly into your JDE system
- Quickly and easily produce evidence for your auditors
- Simplifies the process and saves effort for both technical staff and business reviewers
- Speeds up the review process
- Works independently of security tools; you can use it however you manage your security.

**Watch a short demo of
Periodic Review [here](#)**

Continuous Monitoring

Fraud Detector

Fraud Detector gives you powerful monitoring tools which can alert you instantly to suspicious changes to critical or master data, and make it easy for you to view and investigate them promptly.

It works with the Data Change Tracker (21CFR11) in JD Edwards, which allows you to specify exactly which tables and columns you wish to audit. Every time those columns are updated, the audit details are automatically logged.

With Fraud Detector you can set up alerts to notify relevant people of significant changes that may need to be investigated – for example, changes to bank account details or system configuration files.

Audit data can be viewed through easy-to-use enquiries and reports, with filters that allow you to pinpoint significant events, investigate changes and add explanatory notes where needed.

Key benefits and features include:

- You decide exactly what to audit and monitor
- Instant notification of changes to critical data greatly reduces the risk of fraud
- Quickly and easily see all audited data in one place
- Detailed audit trail of who changed what and when, including before and after values
- All changes to audited data are logged, even if made by programs external to JDE.

Compliance and Audit Reporting

ReportsNow

We've partnered with ReportsNow to provide a comprehensive set of predefined interactive reports that complement our solutions. They give you dashboards and summarized information to help you keep your finger on the pulse of your security, as well as detailed reports where you can drill down to investigate specific issues.

You can report on:

- Your Security Model (Security Manager Pro)
- Your SoD Rules, Violations and Mitigations (Audit Manager)
- Audited Data and Alerts (Fraud Detector)
- Approvers, User Profile Reviews and Security Workbench Reviews (Periodic Review)
- Role Request Status, User Provisioning activity (User Admin Manager).

License Management

QCloud License Audit

As your business grows and changes, it's important to ensure that your JDE licensing is compatible with your current needs.

QCloud License Audit is a Cloud-based service which analyzes your actual JDE usage and provides accurate statistics and detailed forensic evidence about user activity in each module (SKU or SKU suite), within hours and with no technical effort. The results can be viewed through interactive enquiries, and you can also download the details in a spreadsheet for further analysis.

Key benefits and features include:

- Get an accurate view of actual usage over 3, 6 or 12 months, as required
- Detailed forensic evidence helps you understand your licensing needs and supports your negotiations with Oracle
- Find out if you are under-licensed
- Optimize license usage by identifying redundant access rights
- Identify users with unused access so you can tighten up security.

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



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

ORACLE

Partner

ORACLE

Build
Partner

Expertise in
Validated Integration for Oracle
JD Edwards EnterpriseOne

www.qsoftware.com

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.