Saviynt

SOLUTION GUIDE

Saviynt for JD Edwards

Comprehensive Solution for Access Compliance and SOD Management

JD Edwards enterprise resource planning (ERP) software is a well-known solution leveraged by companies that require in-depth solutions for industrial manufacturing, engineering, natural resources, construction, real estate, consumer products, distribution, as well as many others.

JD Edwards offers significant out-of-box capabilities to provide solutions for financial accounting, order processing, supply chain execution, manufacturing and distribution. These capabilities, to provide such diverse competencies, introduce several challenges in ensuring users are provisioned effectively with adequate and appropriate access; always being mindful of access to sensitive data (PII), least privilege and the potential for segregation of duty (SOD) conflicts.

JD Edwards has a complex security model to govern access and is not secured by default. If not configured adequately, a company could be left with significant security gaps.

Understanding JD Edwards Security:

Ensuring security and compliance in JD Edwards is a complex task, as access can be configured in several ways. It is possible to set up security for a role, user, or both. JD Edwards also incorporates *PUBLIC and *ALL to universally apply security configurations. The system applies security in the following order: User --> Role --> *PUBLIC. Security can be configured to grant or deny access to *ALL for users, roles and *PUBLIC. Access provided to specific functionality will take precedence over *ALL configurations. An example of the hierarchy is as follows:

A user is given specific write authorization to a JDE program, but *ALL dictates that no write access is provided to all programs. The specific authorization given to the user will take precedence.

By default, JD Edwards is delivered with wide-open access. It is important to first configure *PUBLIC and *ALL to deny access by default and follow by granting access back to users as needed.

There are also several other access rights that are incorporated into what level of access a user might have once they are provided access to an application. Items such as Application Security and Action Security further secure how users can access or perform specific actions on different applications. Items such as Exit Security and Solution Explorer Security that allow users to move quickly among menus and applications. Row Security and Column Security determine a user's access to view and transact on specific sets of data.

Saviynt Application Governance, Risk, and Compliance (GRC) Solution:

Saviynt's solution for JD Edwards provides much-needed visibility into user access. The JD Edwards ruleset comes with risks or toxic combinations of fine-grained entitlements incorporating such items as roles, ability to run applications, action security, etc. to provide an assessment of entitlements that should not belong to the same user.

Saviynt automates and enables organizations to satisfy compliance requirements by offering a comprehensive, cutting edge capability in all areas of Application GRC including: SOD Analysis, Role Engineering & Management, Emergency Access Management, Compliant Provisioning, Access Certification and Transaction Monitoring.

Protecting Sensitive Data and Meeting Compliance Needs:

Saviynt automates and enables enterprises to meet compliance mandates for JD Edwards by offering one of the most advanced Application GRC solutions that include features such as SOD management, continuous compliance framework, risk-based certification and emergency access management. The platform enables internal audit and security teams to define business rules, identify SOD violations and remediate them, monitor critical transactions and assess their impact via an intuitive workbench.

Identify and Monitor Risks in Real Time:

Saviynt enables internal security teams and auditors to determine SOD violations and remediate them using an intuitive workbench and offers a mitigating controls library to accept or manage risks.

Unified Compliance Framework:

Many organizations struggle to build a library of controls that can automate compliance processes due to lackof resources or time and difficulty in gaining expertise in all the applications. Saviynt empowers security teams with over 200+ security controls mapped to industry domains and applications such as JD Edwards. Saviynt also provides a flexible framework to create organization specific controls that can later be contributed to the controls exchange.

Privileged Access Management:

One of the key benefits of Saviynt is that companies can manage emergency, break-glass procedures to provide time specific, privileged access on demand. When privileged access is granted, Saviynt can provide visibility into transacted activities to provide assurance nothing inappropriate was transacted.

Key Benefits

Continuous Compliance

- Prioritized, real-time risk dashboards for actionable investigations
- Interactive drag and drop Link Analysis for rapid investigation on high risk events
- Ability to configure real-time alerts, reports
- Controls reporting mapped to SOX, PCI, FedRAMP, HIPAA, etc.

Role Design & Management

- Automated security group design and management
- User and Role security group provisioning
- Role impact simulation and assessment
- Attribute based Access Rules (ABAC) combined with Roles to create highly flexible / event driven access management

SOD Management

- Out of box rulesets for JD Edward with mapping to business functions and granular application entitlements
- Integrated with online Controls Exchange for contribution from customers and partners
- Cross application SOD evaluation
- Investigation workbench including actual vs. potential classification
- Detective and preventive control enablers

Emergency Access Management

- Easy shopping cart based approach
- Access recommendations / certification decisions empowered via usage activity, peer requests, business policies / attributes
- Flexible enterprise grade workflow designer
- Preventive checks for SOD and security policy violations
- Automated provisioning to target systems

ABOUT SAVIYNT

Saviynt empowers enterprises to secure their digital transformation, safeguard critical assets, and meet regulatory compliance. With a vision to provide a secure and compliant future for all enterprises, Saviynt's cutting-edge solutions have been recognized as industry leaders. For more information, please visit www.saviynt.com.

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com