SAVIYNT

SAVIYNT FOR MICROSOFT DYNAMICS GP

COMPREHENSIVE SOLUTION FOR ACCESS COMPLIANCE AND SOD MANAGEMENT

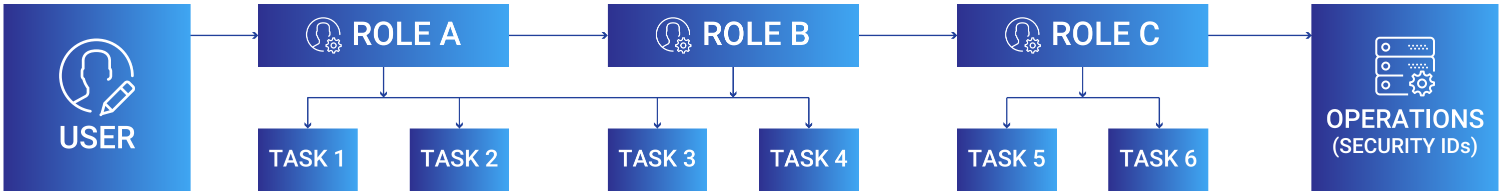
Microsoft Dynamics GP enterprise resource planning (ERP) software is a solution typically leveraged by mid-sized businesses. Dynamics GP focuses on solutions for companies that require in-depth solutions for Financial Accounting and Reporting, Payroll, Purchasing, Inventory, Project Manufacturing, Sales, and more. In addition to these series of modules, a community of Independent Software Vendors (ISV) have developed many add-ons, generally referred to as Third Party applications (e.g., Cashflow Management or Analytical Accounting).

The wide range of these capabilities that 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. Dynamics GP has a complex security model to govern access. If not configured adequately, a company could be left with significant security gaps.

UNDERSTANDING DYNAMICS GP SECURITY:

Ensuring security and compliance in Dynamics GP is a complex task. Users are provided access via Security Roles. The Security Roles are configured with Security Tasks that enable the user to perform specific business functions. Security Tasks are a group of operations required to transact different business functions.

- **Operation:** The Operation component is the base level element of security for accessing "windows" necessary to transact activities in Dynamics GP. There are several distinct types of operations: Reports, SmartLists, Series Posting Permissions, Customization Tools, etc.
- **Task:** The Task component is the group of operations that are needed to complete a business task. For example, the business task can include both the Enter Customers operation and the Post Sales Transactions operation.
- **Role:** The Role component is a group of tasks that are logically combined to define different job responsibilities within a company.



SAVIYNT APPLICATION GOVERNANCE RISK AND COMPLIANCE (GRC) SOLUTION:

Saviynt's solution for Microsoft Dynmics GP provides much-needed visibility into user access. The Dynamics GP ruleset comes with risks or toxic combinations of fine-grained entitlements incorporating such items as security roles, security tasks, operations, security types, third party apps, 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 Dynamics GP by offering one of the most advanced Application GRC solutions that includes 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 lack of 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 Microsoft Dynamics GP. 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 that 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 Microsoft Dyanmics GP 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 controls

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

Saviynt USA / Headquarters, 5777 W Century Blvd
Suite 370, Los Angeles, California 90045, USA

info@saviynt.com
sales@saviynt.com

310-641-1664

Saviynt is a Cloud Access Governance and Intelligence company that focuses on providing simple, fast and cost effective solutions for organizations to manage security of their critical assets in the Cloud and Enterprise.