SafePaaS Roles Manager™

Roles Management: Square Peg in a Round Hole?

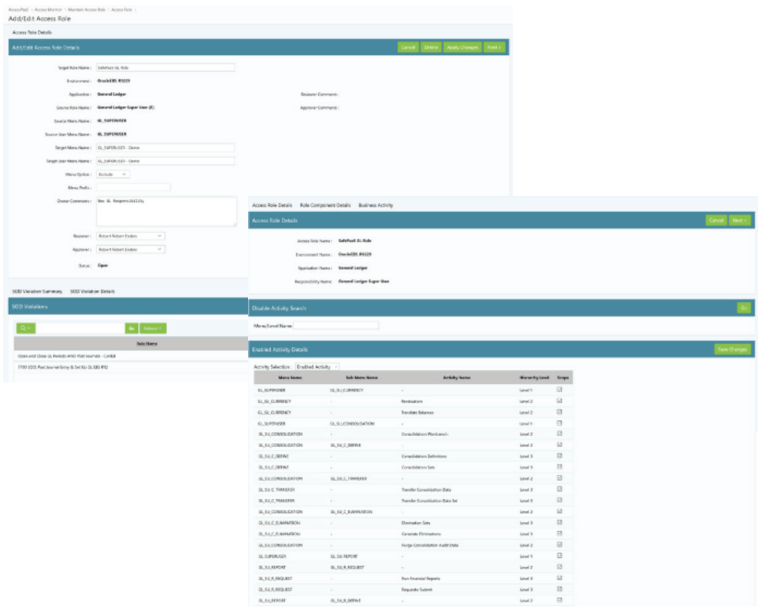
Many organizations face challenges in granting business application roles that fit the user access responsibilities and rights to comply with enterprise information policies. Provisioning user access to roles supplied with enterprise business applications can impede user productivity and increase risk of unauthorized access to sensitive information as well as the likelihood of erroneous transactions.

A "One size fits all" approach can result in higher IT maintenance costs and audit fees when users, irrespective of their job position and responsibilities, are granted roles to access sensitive business information such as transactions, master data and system configurations. For example, a user with a "Super User" Role assignment in the Payables application may enable a user to Update Supplier Bank Accounts, Create Invoices, Change 3-Way Match configurations and Pay Invoices.

Application Administrators often address these risks by customizing the role template delivered with the business application. However, with hundreds of access rights available in complex applications and a lack of formal role design process that includes business control owners, some role misconfigurations are never discovered until operational loss event is reported or a material audit finding is issued. The impact and likelihood of access control failure risk is rapidly growing as user access points into enterprise data is accelerating through the proliferation of mobile devices connected over the cloud

Discover User Activities and Improve Productivity

Well-designed roles not only improve user productivity but also mitigate enterprise information risks. You can gain instant insight by using Roles Manager to discover user access rights within your business applications. Next, you can correct mismatched roles by browsing through a catalog of role templates based on job positions available in the Roles Manager. You can tailor the role template using the role design workbench to select the access rights within your business application to meet the functional requirements, as well as comply with policies that restrict and segregate user access.



You can maintain change controls over the roles to ensure that the process owners can review and approve Roles based on privileges, organization structure, data security rules and job position. Once the roles are approved, you can automatically generate the role configuration file and deploy the roles into the business application. You can also use these techniques to migrate roles from one instance to another.

SafePaaS™

www.safepaas.com

SafePaaS Roles Manager™

Analyze Role Entitlements

Discover role entitlements by scanning access to application privileges and data using the security structure of your business application. Identify issues in access rights based on role assignments. Download analysis results in Microsoft Excel and determine remediation plan.

Detect risk of fraudulent, unauthorized, unusual and erroneous transactions within your business application to monitoring user activity. Audit database and application activities of all users granted privileges to perform critical business tasks such as maintain master data, update system configurations or access restricted information.

Design User Roles

Improve application security and user productivity with effective role design. You can start by browsing through the catalog of role templates available in Roles Manager to select a template as a source and create a target role tailored for each job position. Each target role includes application specific access rights such as menus, functional and forms to deploy the target role.

Configure Role Entitlements

Configure application security components by including new access rights to excluding existing security rights. Extend and customize security components such as menus, and permissions assigned to users within a role.

Control Data Access

Limit user access to data by applying security rules, profile options and personalization based on data role, privileges , organizational unit and other security attributes available within the business application. Roles Manager can also be integrated with on-premise and Cloud ERP applications to deploy approved roles into the target systems, thereby reducing security design and risk remediation efforts.

Deploy Role Configuration

Generate Role configuration report to ensure that the target role meets business requirements. Submit the final role design to business application manager and access control owner for final review and approval. Execute role deployment steps to automatically load the role configuration into the business application.

Maintain Roles

It is important to maintain change controls over the business application security model to ensure that the application control owners can review and approve any changes to roles based on business needs, organizational structure and user job positions. Roles Manager includes change control workflows to ensure that any changes to role design are reviewed and approved by authorized manager before releasing those changes for user assignment. Reports are available to track all changes to the role design as well as compare roles across application environments, business units, etc.

Provision Roles to User

Streamline and control user-provisioning process to assign business application roles to users. Roles Manager enables self-service provisioning for new, as well as existing users. A user can request access to one or more roles online by select the application environment and submitting a workflow request to the pre-assigned role approver. The approver can receive the request via email with the option to approve or reject the request. The provisioning request and approval action are logged for audit reporting.

Grant Emergency Access Roles (Fire Fighter)

Certain users require emergency access to sensitive functions to resolve technical problems such as errors in the financial close process. Users can request such access through the provisioning process. Once the access is granted, the user activity audit is activated automatically through approval of requested access via configurable workflow. Once active, all user activities are captured and stored as a complete audit trail. As needed, control owners, compliance managers and internal auditors are notified of any violations based on pre-defined thresholds. This control monitor mitigates privileged user access risks while maintaining flexibility and responsiveness required for business performance.

Certify User-Role Assignment

Improve application security with periodic user access review and verification process. Roles Manager can send a user-role certification request via email notification to application access control owners to review active users and roles assigned to those users. You can detect and prevent any unauthorized user access rights and quickly correct any conflicts. A compressive report of the review and verification process is generated as evidence to support the effectiveness of your user access controls.

SafePaaS™

www.safepaas.com