

Automated, Continuous Compliance

With an integrated solution from Sun and SAP



Analysts confirm that today, enterprises everywhere face unprecedented demands to comply with strict requirements governing the security and integrity of critical business applications and information. To meet these requirements, an organization must be able, at any given time, to ascertain who has access to specific information resources, monitor changes in access control while assuring compliance, report results, and provide an historical record of changes and activity. Corporations need to provide complete visibility throughout the entire enterprise as well as comply with internal and external auditor requirements.

Highlights

- Helps provide continuous compliance through transparent ERP auditing and identity management
- Enables real-time risk analysis and remediation throughout the employee life cycle
- Enables enterprise-wide and centralized auditing and reporting
- Offers cross-platform, cross-process, and cross-function compliant identity management for ERP and non ERP applications
- Helps reduce risk, time, and cost of compliant user provisioning
- Enables efficient complaint provisioning processes

To ensure compliance with legislative and international requirements, organizations must add staff, hire consultants, and implement processes that are often manual and complex. A great deal of manual effort is required to prevent users from erroneously accumulating conflicting privileges. The challenge is to find manageable, repeatable, sustainable, and cost-effective alternatives to accomplish security and compliance objectives over the long term.

The solution

Through the combined integration of Sun's identity management solutions and SAP GRC Access Control, enterprises can finally achieve the arduous goal of compliant provisioning. The integration provides automated, system-wide auditing and reporting capabilities to assist with streamlining corporate policy and legislative compliance for mission-critical Enterprise Resource Planning (ERP) applications and other enterprise IT resources.

The industry-leading Sun Java™ System Identity Manager software employs a variety of capabilities, features, and tools to help ensure that access to sensitive information is subject to the most secure control possible by enforcing security policy and global standards through repeatable and sustainable processes.

SAP GRC Access Control provides the functionality to create an end-to-end compliant provisioning solution with features such as risk analysis and remediation, compliant user provisioning, enterprise role management, and superuser privilege management capabilities.

The scalability of provisioning from Java System Identity Manager software, combined with the risk analysis and remediation of SAP GRC Access Control, is designed to prevent cross-application provisioning conflicts. For example, it could prevent someone from creating a vendor in one system and paying the same vendor in another system. Automated and continuous monitoring of user access reduces risks to systems caused by subsequent rule changes or unauthorized provisioning. In addition, the combined solution automatically detects and reacts to potential risks, such as dormant accounts, while providing a central point to instantly revoke user accounts. This prevents the risk of erroneously aggregated privileges, and reduces the time spent auditing and fixing access control. SAP GRC Access Control simulates compliance issues in the production system before approving a request, and automatically pulls information from within ERP identity sources and checks for security violations.

Together, Java System Identity Manager software and SAP GRC Access Control provide complete visibility throughout the enterprise, enabling control over network resources, ERP applications, and other mission-critical business applications. The solution helps meet corporate security policies and regulatory requirements by enabling:

- Compliance with national and international regulations governing privacy, security, and financial integrity
- Enterprise-wide identity auditing and reporting
- Repeatable, auditable, enforceable security processes through a role- and rule-based approach
- The ability to review the status of access privileges at any time
- The ability to analyze risks and simulate mitigating controls before provisioning
- Automated mandatory checks for separation of duties (SoD) violations, and access to critical transactions prior to provisioning identity as well as access into ERP and other IT resources
- Compliance with regulatory requirements to periodically review and document user access assignments
- Accountability for who has access to what and who approved what, and when
- Easy viewing for auditors and process owners

How does it work?

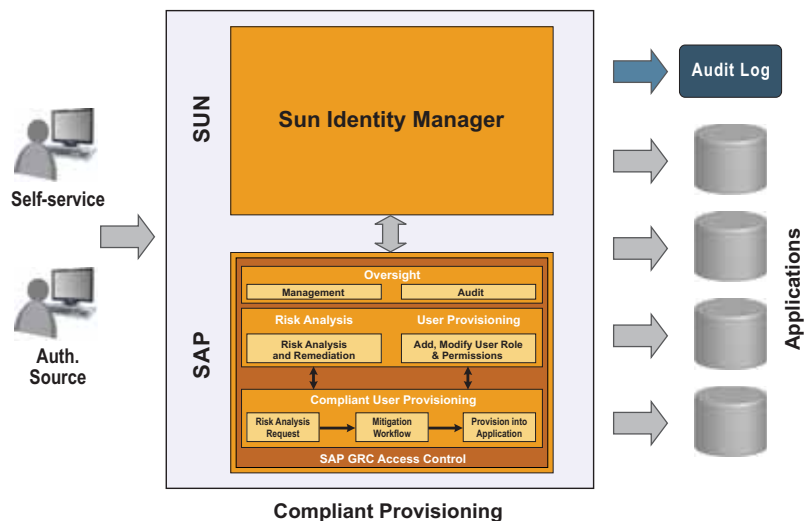
The integrated solution provides continuous compliance by automating provisioning and auditing of user access across enterprise IT resources, including custom and Web applications, mainframes, directories, databases, operating systems, and ERP applications.

The process can start with the Java System Identity Manager or SAP GRC Access Control and follows these steps:

- A user’s enterprise role is set up or automatically detected in an authoritative source
- The user’s virtual identity is created, tying the user to accounts, entitlements, and authorizations across the enterprise
- A risk analysis of the request is performed to check segregation of duties or privileged access violations
- Mitigating controls are provided through automated workflow
- A role is assigned to the user in the ERP system
- User accounts are automatically provisioned and deprovisioned across the enterprise based on compliance policy
- Documentation of provisioning controls and reports for periodic access reviews are generated for auditable evidence
- Ongoing, activity-based monitoring of ERP system transactions is provided

Conclusion

To stay competitive, companies must open up their networks to a global, online economy, while facing increasing regulatory and legislative mandates. In an age of information security audits, internal and external security threats, and regulatory and government privacy mandates, protecting sensitive enterprise resources is a vital necessity. The integrated solution of Java System Identity Manager software and SAP GRC Access Control provides complete visibility throughout the enterprise to help meet corporate security policies and regulatory requirements. The integrated solution helps reduce risk by shifting focus from after-the-fact reactive compliance to preventive compliance.



Integrated continuous compliance solution from Sun and SAP