

Is Your SAP System Secure During Emergency Access?



*The Advantages of Security Weaver™
Emergency Repair™*



THE NEED FOR GREATER CONTROL WITH EMERGENCY SYSTEM ACCESS

With any sophisticated business system such as the SAP enterprise software environment, performing routine maintenance to correct software-related problems is considered part of standard operations. The majority of these maintenance tasks are duties such as fixing errors due to incomplete debugging, making modifications to existing business functions, or adding enhancements that expand capabilities.

Under normal operating circumstances, software maintenance is usually restricted to IT and/or development personnel. But when system problems related to mission critical business functions are identified outside of routine maintenance schedules, access to the system must be granted to appropriate available support personnel so that software glitches can be quickly corrected. The process of authorizing short-term access to the system for after-hours maintenance purposes is referred to in this paper as “*emergency access*”.

The manner in which emergency system access is granted can lead to regulatory compliance problems, especially if authorization is granted without appropriate controls on the viewing of sensitive information. For example, for enterprises in the health care, pharmaceutical, or public securities sectors, the assignment of temporary system access can allow unauthorized access to protected information such as medical or financial records. As a result, any IT department that does not place sufficient controls on user access to sensitive information risks non-compliance with federal regulations such as Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), or the Gramm-Leach-Bliley Act (GLBA). This non-compliance can result in substantial fines and/or legal penalties to the enterprise.

In light of potential liabilities, enterprises must now maintain highly detailed and audited documentation on each support user who is granted emergency access to the enterprise business system. Records must show a complete transaction history of all access sessions in order to provide substantiated evidence that the user did not access or modify any unauthorized or sensitive information.

This white paper will identify the many challenges that SAP customers face by granting emergency access privileges within their enterprise information environments, and will detail the way that existing solutions fall short in effectively managing and auditing user information during emergency access sessions. Existing approaches will be compared to the **Security Weaver™ Emergency Repair™** solution, and we will show how this alternative provides superior advantages that facilitate the management, auditing, and reporting of emergency access information to better serve the needs of today’s enterprise organizations.

Security Weaver is a leader in the area of enterprise information security, offering innovative industry control and compliance solutions for the SAP software environment. With the release of the innovative **Emergency Repair™** solution, Security Weaver once again reinforces its technical leadership by providing a highly effective, real-time, all-in-one compliance solution that enables advanced reporting, auditing, and management of emergency access information for the entire SAP enterprise software environment.

The manner in which emergency access to the SAP system is granted can lead to subsequent compliance problems, especially if the authorization is performed without appropriate controls.

THE PROBLEM: SYSTEM ACCESS WITHOUT ACCURATE DOCUMENTATION

As an ongoing means of improving SAP system security to meet internal security control requirements, support users who have been granted temporary access to sensitive information are later removed from the system access lists by the administrative support staff. Unfortunately, when a critical production issue arises in areas of sensitive information, the support staff will be unable to troubleshoot and resolve the issue without undergoing a time consuming and complex re-authorization process.

To date, IT managers have deployed two different approaches to provide emergency access to the system while attempting to retain appropriate internal security controls, each of which has its own set of challenges. These two approaches are: 1) *granting temporary access* to the system and 2) *creating multiple, generic maintenance IDs* to provide emergency system access.

Traditional Method #1: Granting Temporary Access to Existing User IDs

With this approach, the system administrator provides emergency access authorization to an existing user ID for a limited amount of time. However, this temporary access is not always accomplished in a timely and efficient manner, as it often requires completing a number of complex and time-consuming steps, or is fraught with pitfalls, like the following:

- **A Cumbersome Approval Process** - When temporary access to the system must be granted, several established security protocols must be followed. These often require the involvement of several levels of system administrators and multiple IT managers. Most approval processes also assume that managers are available when needed. If one or more managers in the approval chain are unavailable, valuable time is lost while a backup administrator with a similar level of authorization can be located to grant authorization.
- **Live Administration and Monitoring** - With most enterprise systems, there is typically a limited number of system/user administrators who have the authority to grant system access privileges. As a result, these administrators must be available on a 24 x 7 basis. When emergency access is needed after normal business hours, they must be contacted to grant the authorization. Some companies even require that their administrators return to the data center and stand over the shoulder of the support user so they can witness that the temporary access isn't being abused. This process does not always guarantee complete security control since the administrator performing the live monitoring must have an equivalent level of system familiarity as the support user, and must be able to correlate that knowledge along with the specific areas within the SAP system that will be accessed to resolve the problem.
- **Inaccurate or Incomplete Documentation** - When a system problem is identified, the support help desk responsible for initiating the corrective action should provide all the details about the software problem and the specific action steps taken to resolve it. This information should be recorded to provide corporate accountability for future compliance audits and to provide detailed instructions for resolving the problem if it reoccurs. If the help desk fails to completely document the problem, its circumstances, and all the details of the resolution activities, then when the same or a similar problem arises in the future, the resolution process must be initiated all over again, resulting in added effort and costs for the IT department.
- **Lack of Automated Reporting and Tracking** - By default, an SAP system does not provide a permanent process of tracking and saving all the detailed activities associated with a specific user ID or the information that was viewed during the emergency access session. While SAP systems can temporarily save some of the basic transaction details to a temporary system file, in most cases this information is retained by the system for no more than a few weeks. If this information is not permanently saved to another location after this period of time, the temporary file is overwritten with new information and the older transaction information is lost. To obtain a more permanent record of these transactions, the IT department must create a custom reporting function to store the details contained in the temporary files, which requires a substantial amount of programming, and adds additional cost for the enterprise.

By default, an SAP system does not provide a process of tracking and saving user IDs or the information that was viewed during an emergency access session.



The Security Weaver ER solution for SAP enterprise software environments provides an automated and secure means of ensuring emergency access to sensitive information

CONCLUDING SUMMARY

Providing emergency access to the SAP system is a necessity, especially when critical software modifications are needed after normal business hours. However, in gaining emergency access, temporarily authorized users may also have the opportunity to access and/or modify sensitive financial, personal, or health-related information. Protection against unauthorized access must be secured with appropriate controls, and must be accompanied by detailed documentation in case of compliance audits regarding federal regulations such as SOX, HIPAA, or GLBA.

The Security Weaver ER solution for SAP enterprise software environments solves these security issues by providing an automated and secure means of ensuring that emergency access to sensitive information can be fully controlled, documented, and audited. ER also leverages existing SAP interface resources in a way that facilitates IT support effectiveness while reducing operating costs at the same time.

In summary, Security Weaver ER provides four important business benefits for emergency access to an SAP enterprise system:

- **Provides Greater Control** - Since all system activity is based on the user's ID and SAP roles, Security Weaver ER provides management with complete visibility into "high risk" system support activities.
- **Ensures Regulatory Compliance** - Use of Security Weaver ER ensures that enterprises can maintain full federal regulatory compliance with all pertinent laws that apply to the access of sensitive information.
- **Reduces Operating Costs** - Since support is decentralized and tied to specific support events, Security Weaver ER decreases the related administrative overhead and costs by streamlining the process for resolving IT production problems, thereby eliminating the need for full-time, live support for maintenance user access.
- **Creates More Efficient and Effective Audits** - Security Weaver ER's stronger process-related controls create more efficient audit trails, providing corporate auditors with readily available information and substantiation for regulatory compliance.

For more information on
Security Weaver ER, as well as
other Security Weaver solutions
for SAP enterprise software,
please visit our website at:
www.securityweaver.com



Security Weaver, Inc.

28102 S. Montereina Drive
Rancho Palos Verdes, CA 90275-1202
Phone: 800-620-4210
Fax: 888-538-0634
Email: infoER@SecurityWeaver.com

