Solving SAP® Application Access and Security Challenges with an Identity-Infused Enterprise

Introduction

Today's computing era introduces a number of challenges for SAP® application owners and IT groups. A constantly changing user base needs access to mission-critical SAP applications hosted internally, on the Web and in the cloud. Yet ensuring user access can be time-consuming and labor-intensive, especially when running multiple instances of SAP applications across a large enterprise.

At the same time, through the normal course of business, organizations collect large amounts of valuable information about their employees, customers and partners, and that data must be protected. As governments around the world are regulating how that data should be safeguarded, companies are seeking ways to combat business and IT risks, including enterprise risk mitigation and controls; identity and fraud management; and governance and compliance. As a result, organizations must balance appropriate access with uncompromising security.
As companies work to upgrade their controls over sensitive information, identity plays an increasingly critical role. With it, they can manage access policies, improve their security posture and simplify regulatory compliance efforts.

This paper explains how organizations running SAP applications can provide appropriate, secure access by infusing identity throughout their environments, without adding to their daily workload.

The Challenge of Providing Secure Access to SAP Applications

The SAP Business Suite consists of several modules that encompass a wide range of business functions, from human resources and accounting to customer and supply chain relationship management. Oftentimes, the central point of access for the modules is SAP NetWeaver®, a Web-based front end for the entire SAP system.

Even with a rich portal interface, enterprise-wide identity and access management for SAP and other applications presents several challenges. The foremost of these is managing user accounts across SAP modules.

Many enterprises running SAP applications rely on manual processes to grant application access. Employees requiring access often need to track down the application owner, fill out paperwork, and submit it for approval and processing. With different groups managing and granting application access—sometimes across far-flung offices—organizations often lack a central record of all access rights associated with any single employee. This lack of centralized records makes it difficult for IT to enforce security policies when employees change positions or leave the company.

In a word, this time-consuming, expensive and often inaccurate process involves entering, modifying or deleting user information—repeatedly—in multiple systems across the enterprise. Moreover, it’s difficult to determine which employees have access to which applications at any given time.

As the enterprise grows and changes to meet market demands, the challenges of quickly and accurately granting and revoking access rights grow with it. In addition, monitoring processes to ensure compliance with corporate and governmental regulations only add to the burden and costs.

The Advantages of Operating with Identity at the Core

When an organization decides to manage and monitor identity and access management policy in a coherent, centralized fashion, the first step is to automate user account management and related business processes. This automation begins by making the identities stored in SAP ERP systems available to other enterprise applications. The essential role of SAP applications such as SAP ERP Human Capital Management (HCM) and SAP Customer Relationship Management (CRM) in the overall lifecycle of an identity makes them a critical starting point and a key success factor in many identity management deployments. In these areas, ERP software provides the starting point for creating user identities for new employees, customers and partners alike.
With identity at the core, organizations can enable a number of capabilities that ultimately make administrative tasks easier, help improve security and support regulatory compliance efforts. For instance (starting at the top left and moving counterclockwise in Figure 1):

1. **Defining who can do what:** Organizations can define what each user can do within SAP applications and other enterprise systems and applications.

2. **Controlling resource access:** Organizations can assign users to resources and SAP applications based on their role or relationship with the organization.

3. **Identifying who is doing what:** Based on the applications and systems that users have access to, organizations can monitor what they are doing within those systems, and if it’s risky or out-of-policy activity, remediate that activity as soon as it occurs.

4. **Remediating security risks:** Organizations can identify and remediate security risks as they occur, not days or months after the fact.

5. **Certifying user access:** Organizations can certify that users have appropriate access by infusing identity into systems and processes.

6. **Proving compliance:** With insight into who is doing what and the ability to control and certify resource access, organizations can confidently prove to auditors that they are in compliance with regulatory requirements.

Moreover, organizations can ensure all of these capabilities regardless of whether their SAP and other enterprise applications reside in physical, virtual or cloud environments.

**Figure 1.** Identity at the core streamlines tasks and strengthens security measures.
The Identity-Infused Enterprise in Action

In this section, we’ll explore four scenarios in which organizations can benefit tremendously by infusing identity throughout their environments:

- User lifecycle management
- Password management
- Continuous controls monitoring
- Access management

User Lifecycle Management

Let’s start with a common use case: managing the identity of users throughout the lifecycle of their relationship with an organization—from the time they are hired (zero-day start) to the time they leave the company (zero-day stop). To do that, the company needs to establish various roles that specify different sets of entitlements so employees get immediate access to resources based on need. If employees change roles or leave the company, their access needs to be changed based on those events.

In this scenario, we’ll see how a large retailer greatly simplified the overall user-lifecycle management process—even with a constantly changing user base—by using SAP ERP HCM as the authoritative source for identity information.

The retailer’s rapid growth had led to a proliferation of operating systems and applications, accessed by over 36,000 employees in 68 locations. Specifically, the company was running multiple instances of SAP and non-SAP applications, including SAP ERP HCM, SAP CRM, SAP ERP Financials, e-mail, file storage and homegrown custom applications.

To support its sprawling employee base, the retailer maintained multiple identity stores. Because of constant staff changes, it was continually updating these stores. But with no automated method for user provisioning and management, the IT team spent countless hours manually adding, modifying and deleting users—tasks that were slow, costly and difficult to manage.

To enable efficient application access control and free up its IT staff, the company implemented an identity management solution that enabled it to manage users—including revoking application access—centrally from a single point of control. By allowing the retailer to create enterprise roles with specific entitlements and access rights, the solution empowered the company to provide users with role-based access to applications.

Using authoritative identity data stored in master employee records within SAP ERP HCM, the solution monitors the company’s other applications for any lifecycle changes, such as change of role, title, base location or employment status. As these organizational changes occur, the solution automatically grants and removes individuals’ IT account names and IT resource access rights, depending on the entitlements attached to the employee’s job role. In addition, any employee information change is reflected across all of the applications where that information is stored, including SAP ERP HCM, SAP CRM and homegrown applications. By synchronizing identity information across multiple platforms and automating user administration, the retailer was able to increase security while cutting manual administration.

>> SAP ERP HCM is a logical place to focus an identity management project, since it’s often the hub of employee records.
After deploying the solution to manage enterprise-wide account deletion in a single step, the retailer then rolled out identity management across other business-critical systems, including network access, e-mail and personal file storage. Now the company can provide role-based access for users, creating standardized sets of permissions and access rights that can be changed centrally for groups of people, according to business policy. This enables fast and flexible response to new business requirements, and minimizes the administrative burden.

**Password Management**

Now let’s take a more granular look at this issue by seeing how one organization addressed password management. Though the majority of companies use a username/password combination to secure access to their applications, it’s not an ideal solution. Problems arise when users have dozens of unique usernames and passwords to remember. With so many credentials to remember, they may resort to writing them down or calling the helpdesk to reset them—which places a huge burden and cost on the helpdesk.

Managing the user throughout the lifecycle of their relationship with the organization involves assigning users one or more passwords that are synchronized across the connected systems in the identity management environment. While this helps reduce the number of passwords users must remember, it’s not a foolproof approach, since passwords themselves are not compatible from system to system.

This was exactly the challenge facing one of the largest independent banks in the U.S. To support the firm’s nearly 150,000 users—including both employees and customers—IT staff manually managed access to dozens of systems and applications, including SAP ERP HCM, SAP ERP Financials, e-mail and the company’s intranet, to name a few. In addition to IT employing inconsistent means to manage user credentials, users had to remember multiple IDs and passwords.

Moreover, because the bank operates in a highly regulated industry, it needs to ensure the security of confidential customer information. But managing customer information across multiple systems increases the potential for data inaccuracies and poses security risks.

The firm implemented a single sign-on solution, covering identity and access management. With identity management, it synchronized user information across multiple systems, replacing silos of user data with a single repository for user identity information. By integrating its customer-facing applications for online banking and online cash management, the bank can now provide thousands of retail and commercial customers with a holistic view of their accounts.

With centralized user identity management, customers no longer need to remember multiple IDs and passwords to access their many different services with the bank. Now customers can use single sign-on to access all applications via a portal. Plus, by creating federated identities across many internal systems and using SAP ERP HCM as the authoritative source for 3,500 employee identities, the IT team can provision new users with same-day access to applications based on their role in the organization.

Providing single sign-on access for customers and employees reduced the number of passwords by 75% and reduced password-related helpdesk requests by 30%. Plus, centralized user management lowered IT administration time by 25%, while greatly improving data accuracy.
and security, making it possible for the bank to complete its audits significantly faster and react quickly to new regulatory requirements.

**Continuous Controls Monitoring**

Identity information enables continuous controls monitoring—a combination of identity and access management policies (who *should* have access to applications) with security management data (who *is* accessing organizational resources). This blend helps close the gap between what should be happening based on established controls and what is happening. With this insight, organizations can stop users who try to circumvent established organizational policies and controls, and maintain compliance.

Gaining a complete picture into who is doing what activity is an especially useful approach for detecting and remediating risky activity. By determining whether a user should be engaged in a particular activity based on policy, organizations can stop unwanted behavior and satisfy compliance requirements.

Let's look at a use case involving an IT service provider for the German insurance industry, which continuously monitors user activity to achieve better security and support its compliance initiatives.

In its work with large insurance companies, the company needs to provide over 22,500 users with reliable, secure access to business-critical systems, including SAP HCM, SAP CRM, IBM Lotus Notes, Oracle and custom applications. Some of the organization’s clients run more than 200 different applications, which made managing and securing user identities and access rights a complex task.

The company was relying on manual, paper-based processes for user administration. As the number of users, systems and companies grew, it was spending too much time on basic tasks like creating new user accounts and resetting forgotten passwords. Moreover, in 2009, the German government released a new directive on risk management in the insurance industry, which increased the need for a more auditable approach to IT security and access management.

Using identity management and a solution that automates the security monitoring of IT systems and controls in real time, the organization was able to create a centralized identity and security management solution that automates most user management processes and provides greater insight into which users are accessing which systems. Because the solution is flexible enough to work with a range of applications, the company gained a single method of managing user identities regardless of its clients’ specific infrastructure.

Now, when a new employee is created in a client’s HR system, the solution automatically creates the appropriate user accounts in other systems, based on the employee’s role. Plus, the solution consolidates access logs from all the different systems for real-time analysis and reporting. This provides a full audit trail and helps to reduce the risk of unauthorized or malicious users accessing systems. If unusual activity is detected, the system can take immediate action, such as immediately revoking access privileges.

By automating the creation and deletion of user accounts, and providing a self-service portal that allows users to reset their own passwords, the organization reduced the amount of time spent

---

**Best Practices for User Lifecycle Management**

- Automate user management tasks to efficiently address zero-day starts and stops
- Centralize user identity information in a single identity vault
- Use an HR application (like SAP ERP HCM) as the authoritative source for identity information
- Manage users consistently across SAP and non-SAP applications
- Harmonize usernames to gain a consolidated view of user access
- Leverage roles to make sure users get appropriate access to resources
- Synchronize passwords to eliminate password headaches
- Allow users to manage and change their own passwords
on basic user management work. Just as important, the combination of identity management and security monitoring makes it easier for the service provider to demonstrate compliance with IT security and risk management legislation, and provides greater visibility into user activity.

**Access Management/Web Single Sign-on**

Access management is critical to ensuring that users have appropriate, role-based access to applications. Let’s see how one company used identity and access management to more quickly and efficiently manage identities, enhance security and ensure that IT is more responsive to requests from the business.

The company, the official Caterpillar equipment distributor in Italy, uses a mix of SAP and non-SAP Web-based applications—including SAP ERP HCM, SAP NetWeaver, Lotus Domino and non-SAP applications—distributed across two autonomous divisions.

With approximately 1,350 employees across its two divisions, the company found it challenging to manage user identities and access rights across dozens of different corporate applications and databases. Updating a user’s profile to reflect a change in personal information or provide access to new applications was a slow, largely manual process that required significant effort from the IT department. This created delays and left users frustrated, since requests could take several days to execute. Equally, users needed multiple, separate logins for the applications, and spent significant amounts of time logging in and out of systems.

The company now uses an identity management solution to centrally control user identities and largely automate the provisioning of new user accounts. It uses that solution in combination with access management to extend authentication seamlessly over the Web, simplifying and securing remote work via the SAP NetWeaver Portal. Once users log into the SAP NetWeaver portal, they have role-based access to the company’s various SAP and non-SAP applications. Any changes to user information are automatically synchronized across all connected directories and systems.

By housing these applications within a secure enterprise portal, the IT group can be certain that systems are protected from non-authorized access. Plus, with greater clarity into who is accessing systems, the organization has gained enhanced security. In fact, this transparency empowers the IT department to provide better information to the business and enables greater responsiveness to change requests. It also resolves potential security issues around expired users still having access to some corporate systems.

**Novell® Identity, Security and Compliance Solutions for SAP®**

Now organizations can tightly integrate SAP applications—like SAP ERP HCM, SAP CRM and the SAP BusinessObjects GRC suite—with Novell technologies that are ideally suited for enhancing identity, security and compliance controls in the SAP business environment:

- **Novell Identity Manager®**. Ensure efficient, consistent, secure and compliant access to corporate assets across physical, virtual and cloud environments.
- **Novell Access Manager®**. Provide secure, hassle-free access for all types of users—including employees, customers and partners—regardless of location or time of day.
- **Novell Sentinel®**. Ensure security and compliance with proven policy monitoring, enforcement and reporting.

**Best Practices for Continuous Controls Monitoring**

- Centralize user management for SAP and non-SAP applications
- Leverage identity to enrich security and reporting
- Integrate identity management with the security infrastructure to:
  - Understand who is accessing applications and whether that access is authorized
  - Remove inactive accounts and save licensing costs
  - Stop potentially harmful activity as it occurs

**Best Practices for Access Management**

- Protect all Web-based applications behind a portal interface
- Use an identity vault to deliver consistent role-based access
- If needed, federate identities between internally hosted and externally hosted applications
Because these solutions are fully certified by SAP Labs, organizations can seamlessly integrate the security and identity information in their SAP solutions with other business applications. As a result, business policy becomes an automated IT practice, regardless of the systems involved.

Novell technologies create an automated link between the SAP authoritative source—such as SAP ERP HCM—and the identity vault. This link enables data flow within a business based on its unique requirements, and eliminates the labor-intensive and error-prone practice of re-entering the same data into multiple databases. As new records are added, modified or deactivated/disabled in the authoritative source, network tasks associated with these events can be processed automatically.

Tapping into the authoritative SAP source of personnel information, the data can be propagated to other non-SAP business applications and databases without the need for custom integration solutions. Administrators can decide what data will be shared and how data will be presented within their organizations.

**Bridge the Gap Between Business Processes and IT Security and Controls**

In many organizations, business and IT groups have different mind-sets when it comes to application access and controls. This misalignment leads to inconsistency across the enterprise for user provisioning, identity management and security management.

Even when dealing with a fluctuating user base, an identity-based foundation enables organizations to confidently grant user access to SAP applications—regardless of where the users or applications reside. While SAP NetWeaver enables application-to-application processes, business-to-business processes and business process management and inserts real-world awareness into businesses processes, Novell provides a unique capability to inject identity throughout these processes.
As a result, companies can extend and leverage SAP roles to provision the enterprise and provide automated, secure access to critical applications. By automating and centralizing user management for SAP and other applications, organizations can better secure their applications and ensure that the right people have the right access. Moreover, they can better understand what’s happening at the application level, specifically who is accessing applications and whether or not they are in compliance with internal policies.

Taking this approach allows companies to implement a more holistic security strategy across the enterprise, for stronger security and lower operational costs. Best of all, by leveraging identity, organizations can automate the entire process and minimize administration time.

**The Novell identity and security management stack** is the first to achieve SAP-certified integration with SAP NetWeaver and SAP Business-Objects Governance, Risk and Compliance (GRC) solutions. SAP certification proves that Novell user provisioning, access management and security event monitoring technologies can integrate seamlessly with your SAP infrastructure.