

SOLUTION BRIEF

Improving SAP Security with CA Identity and Access Management

# improving SAP security with CA Identity and Access Management

we can





**The CA Identity and Access Management (IAM) suite can help you increase the security of your SAP environment, streamline management, and simplify your compliance efforts.**



# executive summary

---

## Challenge

The SAP Business Suite and the vast breadth of its capabilities have moved SAP into a leadership position in business application software. However, there are significant security and compliance challenges in managing these complex SAP business applications. These challenges make overall management difficult and expensive, introduce potential security vulnerabilities, and make compliance an ongoing concern.

---

## Opportunity

The CA Identity and Access Management (IAM) suite is perfectly suited to help meet and solve these challenges. It can improve the overall security of your SAP environment by helping to mitigate risks and automate manual processes that exist in most SAP environments. It helps to eliminate improper use of information by controlling what users can do with the information that they obtain. It also simplifies user provisioning management and centralizes some key security and identity-related information, thereby helping to eliminate security “silos” across the organization.

---

## Benefits

Beyond these important benefits for SAP installations, CA IAM can provide very important additional benefits for your enterprise. It helps reduce risk and improve the security of your SAP and non-SAP applications and data. It simplifies compliance and reduces the costs and efforts for compliance audits. It can also enable new business opportunities by enabling the quick and secure deployment of new online services so that you can react quickly to market and competitive events. Finally, by automating and simplifying key security processes, it can improve your operational efficiency and reduce your total costs for security and compliance management.

---

## The CA Technologies advantage

The CA Content-Aware IAM suite offers a broad set of capabilities that can significantly improve the security of your SAP deployment. In addition, our extensive experience and expertise in successful customer IAM deployments enable us to reduce your time-to-value, and to give you the confidence to adopt new technologies in order to drive your business forward.

## Challenge

### Security challenges in SAP environments

SAP AG is the largest business software company in the world, and its suite of software applications is supporting core business processes of some of the largest companies in the world. The SAP Business Suite consists of five major areas, including:

- **Enterprise Resource Planning (ERP)** helps many organizations within an enterprise manage information and processes related to marketing and sales, production and inventory control, human resources, finance and accounting, and other areas.
- **Customer Relationship Management (CRM)** helps companies acquire and retain customers, and gain marketing and customer insight.
- **Product Lifecycle Management (PLM)** helps manufacturers with product-related information.
- **Supply Chain Management (SCM)** helps companies with the process of resourcing its manufacturing and service processes.
- **Supplier Relationship Management (SRM)** enables companies to streamline and improve management of procurement processes.

The breadth of capabilities provided by the SAP Business Suite is outstanding. However, with these capabilities come significant challenges in managing and securing the entire IT environment. The areas that have posed management difficulties for many companies include:

- **Identity and role management** There are typically many application roles within a large organization with a high degree of overlap. Manual management of these decentralized identities and roles becomes burdensome and expensive. It also introduces security and compliance problems because it is difficult to determine the exact entitlements that each user has across all applications.
- **Access management** SAP provides limited user authentication capabilities in the product itself, and there is little ability to tailor the authentication method to the sensitivity of the application or resource. In addition, the SAP authorization model is focused on transactions, and does not provide sufficient capability or flexibility to accommodate the complete scope of business application needs of most large enterprises.
- **Privileged user management** SAP provides some basic capabilities to control what their administrators can do while they are managing the SAP applications, but it isn't available under the standard license. Also, if these administrators are privileged (Administrator or Root) users on the servers that are hosting the SAP applications, they can perform actions that could have disastrous effects on the security of these SAP servers. Since SAP does not provide any capabilities for protecting the critical SAP infrastructure of application and database servers, these resources are subject to attack, breach, or inappropriate disclosure. Therefore, an ability to harden all IT servers, including those that are hosting SAP applications, is absolutely essential to help ensure the security of the entire SAP environment.

- **Protecting critical business information** SAP environments include large amounts of information, much of which is critical to the organization. Once users have gained appropriate access to this data, many organizations have little or no control over what those users can do with it. These organizations often are not fully aware of all the places their sensitive information is stored, and have no protection against this information being exposed or disclosed to unauthorized people, either internally or externally.
- **Log management** SAP log management capabilities are limited to SAP applications, so administrators cannot flexibly aggregate, filter, and analyze log files from all the various systems and applications in their environment. This makes it hard to identify emerging security threats or trends, an absolutely essential requirement both for overall security and for simplifying compliance audits.

Despite the enormous capabilities of the SAP Business Suite, the above security and compliance challenges should be mission-critical for most organizations.

The CA Identity and Access Management (IAM) suite provides capabilities that can not only help solve these problems, but can also simplify management and increase security in a number of ways for SAP deployments. This paper highlights these key areas and illustrates how CA IAM can significantly improve the overall security of your SAP environment.

---

## Opportunity

### Leveraging CA IAM to improve SAP security

The SAP Business Suite is a set of very large and complex applications. Few organizations deploy these applications all at once, but rather adopt a phased approach to limit risk and improve the probability of a successful deployment. As these complex deployments evolve, management of the SAP environment becomes more and more difficult in certain areas.

But, more importantly, in a large ERP environment, the problem of security risk becomes magnified and more difficult to manage. For example, data loss from a warehouse management system is not as risky as data loss from a large ERP system in which all the business and administration processes are managed, and where all the related data is stored. This data would range from HR records all the way to sales results and financial ledgers. When all the business processes in the organization are managed in one place, and all the data to support that operation is stored in one large database, security risk management becomes absolutely critical to the business. This is another reason that additional approaches to reducing security risk are needed.

Although we touched on these areas above, let's explore them in more detail and highlight areas where CA IAM can provide significant security and compliance benefits for SAP environments.

### Identity and role management

**The challenge** The management of user identities and roles within an SAP environment is a significant challenge. In most organizations, roles are created within separate environments (for example,

development, test, production, etc.) without any central coordination or oversight. And, considering the often large numbers of transaction types and business processes that are defined within most SAP environments, management of these user roles quickly becomes unwieldy. Decentralized role creation and user management result in very large numbers of roles and a high degree of overlap among the roles.

Potentially worse, though, is the problem of inconsistent entitlements for users with multiple roles that often result when the SAP role model gets out of hand. Segregation of duties (SoD) violations can go undetected, resulting in increased risk of fraud or inadvertent security policy violations.

The largest challenge related to SAP role management is that the problem only gets worse over time. As roles multiply and overlap increases, management of the entire environment becomes extremely difficult and expensive. In addition, as undetected SoD violations start to arise, management is unaware that the level of risk has risen to unacceptable levels.

**The benefits of CA IAM** The CA IAM suite provides full Identity Lifecycle Management, which is provided by:

- **CA Role & Compliance Manager** leverages analytics and workflow to automate identity governance processes, including entitlements cleanup, certification, segregation of duties, and role management. By automating these processes and controls, it helps you reduce risk, improve compliance, and increase operational efficiency.
- **CA Identity Manager** provides identity administration, provisioning/deprovisioning, user self-service, and compliance auditing and reporting. It helps you establish consistent identity security policies, simplify compliance, and automate key identity management processes.

CA Role & Compliance Manager can add significant value to any SAP environment that has challenges with managing its SAP roles. First, it can discover roles that exist through a detailed analysis of the entitlements that your users already have. Next, it centralizes the management of your roles, which simplifies your role model and reduces the cost of managing excessive numbers of roles.

It also generates customizable reports that enable you to simplify role definitions and identify and remove unnecessary ones. Removing unnecessary role definitions and removing unneeded roles from specific users has a monetary benefit also, because it might enable you to save money on software license fees that you might be paying for these users.

CA Role & Compliance Manager also helps you strengthen security for your SAP environment by enabling you to identify and correct SoD violations. It can generate reports that help identify improper access rights based on your SoD policies. But, it can also help prevent SoD violations because it can check dynamically for these violations when processing requests for access rights. In both cases, potentially significant security and fraud risks that would be extremely hard to identify through manual inspection are reduced.

In addition, CA Identity Manager enables you to centralize the creation and management of user identities and accounts throughout the enterprise. It also provides extensive user provisioning that automates processes for on-boarding, modifying, and off-boarding users and their associated access.

For an improved user experience, it also provides self-service capabilities that enable end users to initiate provisioning actions, password management, and related processes.

In summary, managing SAP roles can lead to high administrative costs, highly manual processes, and increased security risk. The addition of CA Role & Compliance Manager helps bring order to SAP role management by simplifying processes, reducing administrative costs, and reducing SoD security risk.

### Access management

**The challenge** The SAP Business Suite provides capabilities for controlling access and for single sign-on (SSO) for the applications within the Business Suite. When using the SAP Web Application Server and the SAP Enterprise Portal, for example, users are strongly authenticated and have SSO to other SAP applications.

However, the inability to extend these access management capabilities beyond SAP applications has important drawbacks. For example, it:

- Limits authentication methods to those supported by SAP applications.
- Increases support costs as users struggle with inconsistent authentication methods and interfaces across applications.
- Reduces the quality of the user experience due to this inconsistency of the interfaces.
- Hampers compliance due to decentralized authentication, auditing, and reporting.

In effect, the existence of separate access management (authentication, authorization, and reporting) capabilities for both SAP and non-SAP environments creates significant administrative and security problems. A better approach is a common way of controlling access across the entire IT environment.

**The benefits of CA SiteMinder®** CA SiteMinder is the industry leader in centralized Web access management. It enables IT organizations to centralize Web access management so as to protect access to all applications in their environment, both SAP and non-SAP. In addition, it helps strengthen overall security due to the breadth and flexibility of the user authentication capabilities that it supports. Specifically, CA SiteMinder can provide the following security enhancements for SAP environments:

- Improved authentication capabilities—support for a wide variety of authentication methods, which can be combined for even stronger security for high-value applications.
- SSO across both SAP and non-SAP Web-based applications
- Integrated session management to reduce the likelihood of unauthorized user access
- Standards-based support for federated networks, enabling you to provide secure online services to your business partners
- Centralization and simplification of password management, reducing Help Desk costs and improving the user experience
- Improved auditing and reporting of Web access, helping you to more easily prove compliance with regulations and policies

**The benefits of CA Single Sign-On** CA Single Sign-On (SSO) is a solution for enterprise single sign-on that can also increase security in SAP environments. In most IT environments, various applications and systems have their own authentication procedures, which often require users to enter a different user ID and password. In many cases, users resort to insecure practices such as writing down passwords or using the same password for multiple applications. This defeats the purpose of requiring a secure log on in the first place. These vulnerabilities are amplified in situations where workers share workstations or work areas with one another, such as hospital or help desk environments.

CA SSO consolidates application access into a single login while providing a superior level of application security. It offers comprehensive support for resources requiring a login, including mainframe, email, database, ERP, and custom applications, with the flexibility to accommodate any login process. It allows you to improve application access security without incurring the cost of modifying each individual application. Using CA Single Sign-On, you can centrally manage user application access privileges, audit this access, and add comprehensive password policies to existing applications.

CA Single Sign-On also provides out-of-the-box support for a broad range of strong authentication options, including biometrics, PKI digital certificates, tokens, and keystroke analysis. Multiple forms of strong authentication can be simultaneously deployed, giving users the option of using the most convenient form of authentication while maintaining increased security.

The result is increased employee productivity, improved responsiveness to customers, reduced Help Desk costs, and elevated protection for sensitive application data.

In summary, the SAP access management capabilities can be reasonably effective in pure SAP environments, but cannot provide robust capabilities across SAP and non-SAP applications. CA SiteMinder provides an integrated approach to Web access management that helps you reduce risk, simplify the creation and enforcement of access policies, and streamline administration. It also improves your business agility, because you can more easily deploy new online services so that you can respond quickly and securely to new market, competitive, or technology trends.

### **Privileged user management**

**The challenge** SAP provides some control over what users, including SAP administrators, can do while they are accessing the applications in the SAP Business Suite. However, this does not provide any protection at all from either malicious or inadvertent destructive acts (attacks) from outside the SAP environment. For example, a rogue system administrator could corrupt one of the SAP databases or could attack the application itself. He could also potentially turn off the system logging process, perform an unauthorized action, and then turn it back on again, in the hopes of covering his tracks.

Organizations are also vulnerable to careless mistakes by a privileged user. Because these users tend to have Administrator or Root access, they can do virtually anything they want to on the systems for which they are privileged. A simple mistake can result in significant data loss that can have disastrous effects.

In addition, systems administrators often share (and sometimes lose) their system passwords, leading to an even larger risk of policy violations. And, when these users all log in as “root” or “admin,” their

actions, as reported in the log file, are essentially anonymous. These conditions not only pose a significant security risk, but make compliance extremely difficult because improper actions cannot be prevented nor associated with the offending person. This is particularly important in an outsourced environment.

What is needed is very granular access control on privileged users. Unfortunately, native server operating system security does not provide sufficient control over who can access what resources, nor does it provide the granular auditing generally needed to meet compliance requirements.

**The benefits of CA Access Control** The CA solution for Privileged User Management, **CA Access Control**, provides extensive capabilities to limit what administrators can do on your critical SAP systems. It secures servers by providing more granular entitlements for administrators across platforms than are offered by native operating systems. This facilitates easier compliance through improved granularity of policy-based access control and enforcement that includes segregation of duties. The solution controls who has access to specific systems, resources on those systems, and critical system services (as in our previous example, it is important that administrators do not have the ability to turn off the system logging process in order to hide any inappropriate activity). It also can simplify management through a single user interface to manage all your server platforms.

CA Access Control also supports extensive privileged user password management (PUPM), which helps provide the accountability of privileged access through the issuance of passwords on a temporary, one-time use basis, or as necessary while providing user accountability of their actions through secure auditing. This is effective at helping to reduce the common problem of shared administrator passwords that can either get into the wrong hands, or may provide one administrator with more entitlements than is required for their job role.

By deploying CA Access Control on your critical SAP systems, you effectively harden the operating system on those servers, thereby creating a much more secure platform on which you run the SAP applications that your business depends on. You also eliminate the problem of shared administrator passwords for your critical systems, and ensure that all administrators are individually identified within the system event logs. The result is greatly improved security for your SAP applications.

### Protecting critical business information

**The challenge** The information used by SAP applications is critical to your business. However, many organizations don't actually know where all their sensitive information is stored, and have no way to enforce policies over use of that information. For example, you have employees who are authorized to get access to that information, but only for legitimate business purposes. Unfortunately, some employees can be either malicious or careless, and in both cases, the results can be disastrous. Something as simple as a Social Security number can have significant negative impacts if disclosed inappropriately. In short, you need an effective way to discover, classify, and control the use of sensitive information such as financial records, health information, customer records, intellectual property, source code, and the like.

**The benefits of CA DLP** The CA Technologies solution for data discovery, classification, and control, **CA DLP** helps you get control of your massive amount of information, and most importantly, protect sensitive data from inappropriate disclosure or misuse. CA DLP identifies sensitive data across the

enterprise in real time and determines whether or not end users are using that data in accordance with various security and regulatory mandates. It identifies and classifies all sensitive data; examples include personally identifiable information (PII), intellectual property (IP), and non-public information (NPI). It controls sensitive data at all locations: at the endpoint, on the server, on the network, or stored across the enterprise.

CA DLP enables you to define policies that determine which action should be taken if inappropriate usage of the data is detected. For example, it can prevent users from emailing sensitive information outside the company, moving it to a local storage device, storing it on publically accessible share devices, and other improper operations. Your policies can also define a range of actions when disclosure is detected, ranging from warnings to administrator alarms. It also includes a collection of pre-built policies based on real business use cases that make quick deployment much simpler.

CA DLP provides for the classification of your sensitive information and the enforcement of your information usage policies, so as to help prevent inappropriate use or disclosure of this critical information. The result is reduced IT security risk and easier compliance with mandates that dictate information usage requirements.

### Log management

**The challenge** Effective management of system audit logs is essential not only for overall security, but for compliance with external regulations and internal policies. The log management capabilities provided by SAP are basic in scope, and become particularly difficult to manage as the size of the SAP environment expands. Log files cannot be effectively aggregated across systems for easier analysis, and the filtering capabilities are quite limited. This fact alone makes it challenging to identify emerging or existing security threats, because important events become lost in a mass of unimportant system event information. It is very difficult to create customized queries on this information in order to eliminate all uninteresting events so that you can focus on what's really important for your environment. In fact, many SAP installations download this log information into an Excel spreadsheet and attempt to manually filter it according to whatever criteria are important for them. Although this is an improvement, it does not scale to large amounts of log records, still requires significant manual effort, and leaves you vulnerable to human error that might leave a significant event unrecognized.

There are three primary disadvantages of this approach to SAP log management. First, it is an intensely manual process, thereby leading to high costs and unacceptable human error rates. Second, it makes it more difficult to really understand what is going on in your systems and to identify security events before they become critical. Lastly, because it is difficult to prove that your security controls are working effectively on the basis of the system log files, compliance becomes more difficult and expensive. Compliance audits that are based on these limited capabilities are not for the faint of heart!

**The benefits of CA Enterprise Log Manager** The CA solution for log management, **CA Enterprise Log Manager (ELM)**, can provide important efficiency and security benefits for SAP environments. It allows organizations to identify internal and external threats to enterprise systems and business operations by collecting and analyzing distributed log data to look for suspicious activity and finding the root cause of operational problems. CA Enterprise Log Manager aggregates log files, normalizes events into a common format, and classifies them into more intuitive and organized event structures, facilitating quick analysis and reporting from its Web-based dashboard. Most importantly, it provides quick

time-to-value for compliance because it can be quickly installed and can provide immediate value by reporting events with hundreds of out-of-the-box, ready-to-use reports covering all major regulations and standards, such as SOX, PCI, and others.

With CA ELM, you can:

- centrally manage and view log data across your enterprise
- schedule or run queries, reports, and policy violation alerts
- generate predefined and customizable reports with trending information
- create compliance reports using regularly updated compliance reporting templates
- launch an event investigation using its interactive graphical event viewers
- and much more

It also comes with a large number of predefined report templates so that reporting on compliance for a specific area, or a specific regulation, becomes much simpler than the ad hoc queries and filtering of Excel files that many SAP customers use.

---

## Benefits

### Leveraging CA IAM for additional benefits

We have seen above how some of the specific challenges of managing large SAP environments can be met using the CA IAM solution components. These products can simplify how you manage your SAP roles, improve overall security of your Web resources, improve management of your system logs, and reduce the risk associated with privileged users.

However, because of the breadth and the integration of the CA IAM suite, there are other significant benefits that it can provide to any environment, including SAP deployments. The most important benefits of CA IAM include:

#### Reduced security risk

CA IAM helps ensure that your critical IT resources are protected, and that only properly authorized users can access them, and only in approved ways. It protects your critical Web applications, Web services, federation networks, and all the systems in your IT environment. It also allows you to manage and analyze security information to quickly identify and remediate potential security issues, including improper disclosure or use of sensitive corporate or customer information.

#### Control over information use

The information processed by SAP applications is critical to the operation of the business. CA DLP helps protect against improper disclosure or use of sensitive information either in transit, at rest, or in use. It thereby reduces information security risk and makes it easier to establish compliance with certain security-related regulations and best practices.

### Improved regulatory compliance

CA Technologies' IAM products provide your organization with the tools necessary to support continuous compliance with automated and centrally managed capabilities that help reduce costs while strengthening IT security controls. With comprehensive auditing, your compliance challenges can become much simpler because you can provide proof of your controls and validate to auditors the effective operation of your security controls.

### Reduced administrative expense and improved efficiency

Manual, time-consuming security processes are a drain on IT resources and costs. CA Technologies' IAM products can help automate many of your key IT security processes, especially those related to managing user identities and access rights. Along with automated filtering and analysis of security log information, these capabilities can bring significant administrative efficiencies, thereby reducing your overall IT costs.

CA Technologies IAM can also improve the productivity of your employees since it helps eliminate manual, time-consuming processes. It enables new users to be productive quickly without waiting long periods to be provisioned with accounts and applications. It also reduces the time required for management access request approvals and enables them to focus on more important activities—like growing the business.

### Improved secure business enablement

Customers and partners will only do business with your organization if they believe that you can provide a secure environment for their personal information. CA Technologies' IAM products can help your organization secure their applications, as well as deliver new applications and services more quickly to your customers and partners. Because deploying new services becomes easier, you can respond more quickly to competitive, market, and technology trends to help protect and grow your business.

## Next steps

If you are experiencing difficulty in managing any of the following in your SAP environment:

- User identities and roles
- Access entitlements
- Actions of privileged users and SAP server security
- Control of information use
- System log files

then consider some of the CA Technologies IAM solutions that can simplify your SAP security management, improve overall security, simplify compliance, and help automate and streamline your key security procedures.



To learn more about CA Content-Aware IAM, visit [ca.com/iam](http://ca.com/iam).

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and physical to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies' innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at [ca.com](http://ca.com).