

**Solution in Detail**  
SAP NetWeaver  
SAP Single Sign-On

# Cybersecurity and Secure Authentication with SAP® Single Sign-On



---

# Table of Contents

- 3 Quick Facts**
- 4 Remember One Password Only**
- 6 Log In Once to Handle Job After Job Securely with No Interruptions**
- 8 Profit from Three SSO Scenarios for High Security**
- 10 Make an Effective Long-Term Strategic Investment**
- 11 Gain Greater Productivity and Security with SSO**



# Quick Facts

---

## Summary

The SAP® Single Sign-On application gives users a better experience by providing access to all IT systems needed with one password. It protects users and businesses from many cybersecurity threats by using smart cards, two-factor and risk-based authentication, digital signatures, and encryption of communication channels. It adds vital security functionality to your SAP and non-SAP software landscapes and has made SAP Single Sign-On a best-practice security solution across industries and regions.

---

## Objectives

- Protect individuals and business from identity theft, computer crime, industrial espionage, and cyberattacks from both inside and outside the business
- Support strong password policies
- Eliminate the need for insecure memory aids for passwords
- Ensure authenticity and integrity of documents and nonrepudiation
- Lower help-desk costs

---

## Solution

- Single user login for secure access to all the software a user requires throughout the day across companies, domains, and devices
- Dynamic adaptation of authentication requirements based on risk, including support for two-factor authentication
- Cryptographic features certified by computer security standard FIPS 140-2, including integration with hardware security modules
- Digital signature support

---

## Benefits

- Higher authentication security
- Greater data security by encrypting data in transit
- Lower help-desk costs due to significantly fewer calls for recovering passwords and unlocking accounts
- Higher user productivity by eliminating the need to perform separate login procedures for each software application

---

## Learn more

To find out more, please visit [www.sap.com/pc/tech/security/software/single-sign-on/index.html](http://www.sap.com/pc/tech/security/software/single-sign-on/index.html).



# Remember One Password Only

With the SAP® Single Sign-On application, you set the stage for a significantly higher level of data security. You can implement reliable, efficient encryption for all communication between your user and your server systems based on the application's FIPS-certified cryptographic features. You can enforce a strong password policy by giving your employees only one password to remember – which also helps to [reduce help-desk costs](#).

Although your company's system landscape may be highly heterogeneous, comprising a multitude of solutions from nearly as many different providers, you can maintain high security for your employees and your business. Employee workstations may be running different operating systems, and users may rely on different devices. Your employees most likely have access to different central business applications to perform their highly specialized work. They access systems from both inside the corporate network and from their home office or while traveling. Despite this variety of software and access requirements, you can provide every user with access to his or her personal data quickly and securely, including access to e-mail clients, employee portals, and directory services. To accomplish this, you focus on:

- **Authentication service:** This service identifies users based on unique characteristics. All of the activities within a company can then be assigned to individual employees through a detailed log, which also prevents misuse of IT resources.
- **Identity management:** Every user needs a digital identity that is valid and unique throughout the company. IT then manages these identities for individual systems by means of user accounts.

- **Authorization management:** Every employee requires the access rights sufficient to carry out his or her tasks, but no more. Whenever these tasks change, the management system must make immediate adjustments to provide the corresponding rights.

Authentication service is the area that concerns your employees directly. Logging in to each of the individual systems they need every day can become a frustrating time sink and a hindrance to productivity. Too many authentication procedures can easily disrupt an employee's individual workflow. To access operating systems, portals, and e-mail accounts, employees usually need a unique form of identification – generally a user name and password. Meanwhile, security standards often impose strict constraints, requiring complex combinations of numbers, letters, and special characters, which employees can all too easily forget. Naturally, employees like to keep complex passwords written down in places they think are secure, but they may misplace those lists. This exposes your systems and your employees to unnecessarily high risks and renders role management and segregation-of-duty concepts useless. And, of course, help desks come into play. In other words, this loss of productivity entails additional costs.



It's clear that easing circumstances to support the human factor is just as critical as having a sophisticated security concept. These are the specific areas the SAP Single Sign-On application is designed to address. With the application, you can delight your employees by providing user-friendly access to your systems, simplify your employees' daily work, and achieve sustainable cost advantages in IT support.

Identity management and authorization management are the areas the SAP Identity Management (SAP ID Management) component covers. With

this software, you can maintain a reliable overview of the entire user lifecycle – from the day you hire an employee to the day he or she leaves your organization – even in heterogeneous software landscapes. SAP ID Management aids you in overseeing across multiple systems all roles and authorizations your company offers its employees. When you combine this software with the SAP Access Control application – an application that gives you a dependable means of identifying and addressing role and authorization conflicts – you can achieve transparency and security in your rights management while fulfilling comprehensive compliance.



Allow users to log in once to [gain secure access](#) to all the software they require throughout the day with no need to log in again.

---

### More Users = More Benefits

With the SAP® Single Sign-On application, you can take the pressure off your help desk – and your IT budget. Combined with identity management, the application can be key in cutting IT costs through the optimization of your IT infrastructure. But how about the dark side of cutting costs – increased risk? Identity management and single-sign-on solutions can deliver real value when it comes to fulfilling compliance requirements. More than this, these solutions mitigate risk by providing change management control features to maintain authorized access to vital corporate assets even when target applications are updated or new releases installed.



# Log In Once to Handle Job After Job Securely with No Interruptions

## WHY SINGLE SIGN-ON?

By implementing single-sign-on (SSO) technology, you can provide your employees with the convenience of logging in only once to access all of their individual user accounts. Doing so makes your company more secure and leads to fewer calls to the help desk, which means significantly lower costs.

In essence, SSO architectures all function in the same way. A user logs in to the central SSO software. If the software can authenticate the user, the user receives a confirmation for a predetermined period of time, usually in the form of a “ticket.” The time limit is configurable but is usually set to last the entire calendar day, so a user logs in once at the start of the work day, with the token remaining valid for the rest of the day. The applications connected to the SSO software verify this digital “pass” in the background and then grant the user access. Both the process and the concept are straightforward for users. To start work, they need only log on to the central software – the single application upon which the security of your company’s access authorization relies. Depending on your organization’s or a specific application’s security requirements, they can log

in with user name and password or use more advanced procedures, such as smart cards or two-factor authentication.

No matter what procedure your company chooses, you can help ensure that the risk of abuse will be kept to an absolute minimum in all of the systems linked to your SSO software.

## THE SSO SOLUTION FOR EVERY SITUATION

If you’re looking to achieve centralized authentication throughout your IT landscape, look no further than SAP Single Sign-On. The solution’s functional scope gives you true SSO architecture and supports identity verification through a variety of authentication scenarios that are perfectly adapted to your organizational and security requirements.

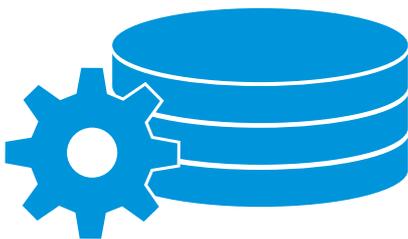
After logging on to their operating systems just once, your employees can access all services connected to your SSO configuration – from e-mail clients and portals to customer relationship management (CRM) software and database applications. There will be no further requirement for them to identify themselves for the rest of the day.



In addition, you can set rules that allow users to log on to systems with higher security requirements. Even if users need to remember just one password, you can require them to explicitly enter it every time they access a specific system. Taking it one step further, a stronger form of verification can come into play: two-factor authentication. While one factor of the authentication process may continue to be the knowledge of a password, the other factor could be the possession of a specific mobile device, a concept that helps defeat remote attacks. This is particularly useful in situations involving business-critical applications or functions – such as access to credit card information.

Combined with risk-based authentication, a method of increasing authentication requirements for access requests that match a higher risk profile, you can ensure that the extra level of security is enforced in those situations where you want it, based on rules that you define.

You have the option of encrypting communications between the SAP GUI interface for Microsoft Windows and the SAP ERP application. When you do, you block all unauthorized tools from recording or manipulating transmissions between your users and their target systems. SAP Single Sign-On enables you to fulfill all of these requirements.



You have the option of encrypting communications between the client and the server. When you do, you **block all unauthorized tools** from recording or manipulating transmissions between your users and their target systems.

# Profit from Three SSO Scenarios for High Security

SAP Single Sign-On enables three key scenarios: SSO for SAP Business Suite applications, SSO for heterogeneous environments, and SSO for cloud-based and cross-company scenarios (see the figure on the next page).

## SINGLE SIGN-ON FOR SAP BUSINESS SUITE

You can use Kerberos authentication tokens to set up SSO for SAP Business Suite software, leveraging the considerable simplification a single-sign-on solution can mean for authentication processes. You also gain benefits as far as security and operational costs are concerned with very little implementation effort. Using Secure Network Communications (SNC) and the Simple and Protected GSSAPI<sup>1</sup> Negotiation Mechanism (SPNEGO), a Kerberos technology, you establish a trust relationship between the user's front end and the back-end SAP Business Suite applications. The user's front end could be, for example, SAP GUI for Windows or a Web browser.

Employees log in once when they start their computers by signing on to their Windows domain. Any subsequent authentication processes are left to a Kerberos token mechanism provided by SAP Single Sign-On and based on Microsoft Active Directory. The scenario requires no additional server. Working in the front-end software, the user experiences streamlined, easy accessibility.

## SINGLE SIGN-ON IN A HETEROGENEOUS ENVIRONMENT

While many newer software applications support Kerberos authentication and can easily be inte-

grated into the scenario described above, legacy systems often lack these features. If you want to take SSO a step further and integrate legacy systems into your SSO landscape, SAP Single Sign-On offers support for X.509 certificates, for example, based on smart cards. This digital certificate standard is a tried-and-true Internet standard that the majority of business software products available today support. You can set up your own dedicated public-key infrastructure (PKI) to issue X.509 certificates, or have the secure login server software, a component of SAP Single Sign-On, issue short-lived certificates. With the secure login server software, you do not need to set up a full-blown PKI with its inherent administrative processes, such as certificate revocation lists, but you can still benefit from the same level of security. Enabling this kind of scenario means that users can sign on once to gain access not only to their SAP software but also to many of their non-SAP applications.

## SSO IN CLOUD-BASED AND CROSS-COMPANY SCENARIOS

Kerberos and X.509 certificates cover many use cases for SSO in the corporate world. However, an increasing number of companies are now seeking to establish trust relationships across company domains or in the cloud. In those cases, you can use the identity provider component to establish SSO using Security Assertion Markup Language (SAML) 2.0 tokens, an Internet-standard technology that enables Web-based SSO and guarantees secure authentication even when identity data is transferred beyond your company boundaries.

<sup>1</sup>. Generic Security Services Application Programming Interface (GSSAPI) is an application programming interface for programs to access security services.

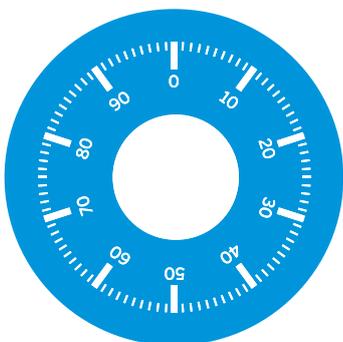


### MORE THAN ONE WAY

The three options mentioned above are not mutually exclusive. It makes perfect sense to start with a simple scenario that allows you to ensure fast return on investment. If there is a business need for it, you may then decide to enable additional systems

for single sign-on based on a different technology. The technologies can be integrated smoothly, so your users won't notice any difference. SAP Single Sign-On gives you the flexibility to start small and grow at your own speed, based on your requirements.

Figure: Scenarios Supported by the SAP Single Sign-On Application



SAP Single Sign-On gives you plenty of possibilities to [simplify your users' everyday work](#) in the long term. While implementing powerful security measures for your business-critical applications, you can boost employee productivity.

# Make an Effective Long-Term Strategic Investment

SAP Single Sign-On gives you plenty of possibilities to simplify your users' everyday work in the long term. While implementing powerful security measures for your business-critical applications, you can increase your employees' productivity:

- Thanks to SAP Single Sign-On, your employees have only one password to remember. This helps them to focus on their work, increases their satisfaction with the IT environment, and reduces the risk of their passwords being compromised and their identities being stolen. It is a prerequisite for any strong password policy.
- Giving your users fewer passwords to remember leads to fewer help-desk tickets, which in turn saves you the considerable cumulative costs involved in resetting passwords.
- The combination of a single sign-on and encrypted client-server communication protects your data from unauthorized access and manipulation at the network level.
- SSO technology for cloud-based business scenarios makes it possible to distribute identity-related data and enable authentication across companies.

The potential annual savings of password-related help-desk costs can be substantial. You can perform an easy calculation to establish impressive proof of how you can achieve a rapid return on investment with SAP Single Sign-On:

- **If** each employee creates an average of one help-desk ticket a month

- **And if** the direct cost of a help-desk ticket to unlock the user and reset passwords is about US\$20
- **Then** you can avoid at least \$240 in password reset costs for each user every year – and this doesn't factor in the productivity lost when users can't log in

The key to these tremendous potential savings goes by one name: SAP Single Sign-On. By requiring just one password and one login process, you can pave the way for a sustainable increase in productivity. With just 500 employees involved, your company's rollout of SAP Single Sign-On could pay for itself in less than a year.

Meanwhile, the gains your company will make with regard to greater security will be invaluable. With SAP Single Sign-On, you can effectively prevent cybercrime attacks – whether they involve massive authorization abuse, compromised passwords, or targeted data espionage. In addition, identity federation functionality based on the SAML 2.0 standard supports a future-proof approach to authentication and single sign-on. These are just a few more reasons why you can be sure that your investment will pay off in the long term.



# Gain Greater Productivity and Security with SSO

## FIND OUT MORE

With SAP Single Sign-On, user satisfaction and security go hand in hand. The software eliminates multiple authentication procedures and leads to marked reductions in password recovery tickets and downtime. You save in help-desk costs, general administrative effort is reduced, and your users get a boost in productivity. Meanwhile, encrypted

connections between your client systems and servers plus strong authentication will help your company achieve a valuable increase in security by protecting your network transmissions and business processes from abuse and cybercrime. For more information, please visit <http://scn.sap.com/community/ssso>.



The potential **annual savings** of password-related help-desk costs can be substantial.

---

© 2015 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. Please see <http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark> for additional trademark information and notices. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors.

National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP SE or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP SE or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.



The Best-Run Businesses Run SAP®

