A modern business’s typical system landscape comprises a variety of solutions hosted on different types of platforms — each element tightly protected against the reality of mounting security challenges. A byproduct of this environment that is familiar to even the most casual non-business user is the need for multiple sets of credentials to access all of these systems, which can lead to passwords that are weak, reused, or written down somewhere so they are easy to remember. In business environments, this can lead to not only security and compliance issues, but also productivity issues caused by repeated manual logins and help desk calls, for instance.

The SAP Single Sign-On solution solves this problem for SAP customers by enabling users to log in just once and gain secure access to both SAP and non-SAP business applications across the entire system landscape while protecting sensitive company and personal data. It supports both cloud and on-premise scenarios, providing simple and secure single sign-on access through the web, via mobile devices, and using native SAP clients. It also uses state-of-the-art standards such as the SPNEGO security mechanism for Kerberos-based HTTP authentication, X.509 digital certificates, and Security Assertion Markup Language (SAML) to meet company and regulatory security requirements.

The latest support packages for SAP Single Sign-On 2.0 — support package 4 (released in November 2014) and support package 5 (released in May 2015) — deliver a number of innovative enhancements to address the security needs of SAP customers, including advanced authentication functionality and simplified configuration features, to help security administrators further improve the user experience while strengthening the security of critical business data. This article provides an overview of these key authentication and administration enhancements, and how they help organizations centralize and simplify the way users log on to systems and applications.

Authentication and Identification Enhancements

Authentication and identification functionality lay the groundwork for SAP Single Sign-On. The latest support packages for the solution build on this foundation with advanced features that augment these capabilities, including support for two-factor authentication, fast user identification via radio-frequency identification (RFID), and risk-based authentication using access policies.

Additional Protection with Two-Factor Authentication

Many organizations rely on user IDs and passwords for authentication. However, for increased security scenarios — such as protecting especially critical systems or securing access from outside the company — a stronger form of authentication for access to corporate resources may be required.
To meet this need, support package 4 for SAP Single Sign-On 2.0 includes support for two-factor authentication via a time-based one-time password (TOTP) — a six-digit or eight-digit code that is based on a shared secret key and the current time, and is valid for one login attempt only — generated by the SAP Authenticator mobile app. This approach requires not only knowledge of a regular password (the first factor), but also possession of a particular mobile device (the second factor) that is registered to generate TOTPs for specific business applications, making it much harder for a remote attacker to succeed, as access to the second authentication factor requires physical proximity.

Enabling two-factor authentication with SAP Single Sign-On is simple (see Figure 1). Users download and install the SAP Authenticator mobile app on their mobile devices, and then activate the app for their specific corporate user ID and one or more backends using self-service functionality. This backend could be an SAP Enterprise Portal with local applications, or an Identity Provider or Secure Login Server that provides security tokens for single sign-on to other systems. On the backend, the administrator uses a login module to configure SAP NetWeaver Application Server (SAP NetWeaver AS) Java to enable two-factor authentication and generate a secret key, which is stored on the mobile device, when the mobile app is activated for a user ID and the respective backend.

Once the app is activated and the configuration is complete, users can securely log into the system associated with their corporate user IDs using two-factor authentication. Figure 2 illustrates this authentication process at runtime. On their desktop client, users first enter their regular password, and then enter a TOTP generated by the mobile app based on the current time and the device's secret key. Once the password and TOTP are validated by SAP NetWeaver AS Java, the user is authenticated and has access to applications on the portal, or the Identity Provider security token is made available to enable single sign-on for the user.

Two-factor authentication is available as an additional protection level for web-based and SAP GUI-based single sign-on scenarios, and in addition to a standalone Java application server, such as SAP Enterprise Portal, it can be integrated with the Secure Login Server (providing X.509 digital certificates) and the Identity Provider (providing SAML assertions) of SAP Single Sign-On on SAP NetWeaver AS Java. For additional security, users can also protect the SAP Authenticator mobile app with a password.

### Fast User Identification via RFID

In traditional single sign-on scenarios, organizations can increase productivity by allowing users to authenticate just once to gain access to a large number of systems for a period of time. In some cases, however, a user needs to very quickly access only one system to perform short tasks — maybe the user works on an assembly line and needs to urgently fix a supply problem before it causes any damage, or perhaps the user works in a warehouse and quickly needs to check or enter data on a shared computer while packing boxes. In these types of scenarios, users don't want to spend extra time taking off their gloves and entering a secure password.

To enable quick logons for users in these scenarios, support package 4 for SAP Single Sign-On 2.0 includes user identification based on an RFID token, such as a company batch card. With the Secure Login Server of SAP Single Sign-On...
in place, an end user can authenticate to an SAP system with a temporary X.509 digital certificate, which the Secure Login Server issues when the user places the RFID card on a reader. This instant authentication is much faster than entering a password and is easy to perform even in a shop floor environment. After the user’s work is finished, the user simply picks up the RFID card and logs out, at which time the X.509 certificate is deleted.

RFID authentication is ideally suited to warehouse and production scenarios with dedicated kiosk PCs for authentication, which protects against compromised RFID readers or cards — the Secure Login Server first validates the identity of the kiosk system before accepting the RFID information to authenticate the user. RFID authentication is available for SAP NetWeaver AS ABAP and SAP NetWeaver AS Java backends via the Secure Login Server of SAP Single Sign-On, and uses X.509 digital certificates. Currently, SAP Single Sign-On supports RFID readers based on the standard PC/SC interface for personal computers and smart cards, and also WaveID readers by RF IDEas.

**Risk-Based Authentication Using Access Policies**

In the past, users usually accessed SAP systems from desktop computers inside the corporate network, meaning all authentication requests came from the same kind of environment. As a result, the security level required for a specific authentication request depended only on the criticality of the accessed system — for example, the value of the data managed inside of the system. As organizations use increasing numbers of cloud and mobile applications, however, authentication requests are coming from a diverse assortment of environments, and the one-size-fits-all authentication approach of the past can have unintended — and unwanted — consequences.

When you assume that all authentication requests are coming from a secure environment, this can result in an authentication process that is fast and lean, but leaves you at risk if a potentially illegitimate request is received and your process cannot adapt to handle it. On the other hand, if you assume that all authentication requests are potentially illegitimate and harden the authentication process against potential attacks, corporate users who were sufficiently screened when entering the office can become frustrated by excessive steps in the login process and productivity can suffer.

Support package 5 for SAP Single Sign-On 2.0 addresses this challenge with an authentication process that can dynamically adapt to the context of an individual authentication attempt.
Figure 3 outlines how this works. The user attempts to authenticate from the client. The authentication request goes to the Access Policies Engine running on SAP NetWeaver AS Java, where a custom-defined access policy will check the context information of the request and determine the next steps. For example, you can specify that the access policy check the IP address of the client and, based on this, dynamically enforce two-factor authentication before granting access via a SAML assertion or an X.509 digital certificate. You can even forward a perceived risk level to the ABAP backend system as part of the SAML assertion, and implement custom code to disable critical functionality. This capability gives you the flexibility to implement security checks in a very precise way.

Authentication based on access policy is available as part of a standalone Java application server, such as SAP Enterprise Portal, as well as the Identity Provider and Secure Login Server of SAP Single Sign-On on SAP NetWeaver AS Java, and uses SAML 2.0 or X.509 digital certificates.

Implementation and Administration Enhancements
In addition to strengthened authentication options, the latest support packages for SAP Single Sign-On include implementation enhancements for security administrators. These features — including out-of-the-box support for modern SAP clients, simplified ABAP administration, and enhanced cryptographic support — enable an even easier setup that allows the solution to be up and running with the highest levels of security in no time.

Support for a Modern User Experience
The user experience is central. From personalization to consistency across devices, users expect a seamless and responsive experience when using their business applications. SAP Single Sign-On 2.0 combines modern user interfaces and enhanced usability with out-of-the-box support for new SAP clients such as SAP Fiori, SAP NetWeaver Business Client, and SAP Screen Personas, allowing you to combine sophisticated user interfaces with enhanced usability while keeping sensitive data secure at all times.

SAP Fiori enables a personalized, responsive, and simple user experience across devices and deployment options for customers using SAP Business Suite powered by SAP HANA. By implementing SAP Single Sign-On, users can access their SAP Fiori apps after just one initial authentication. A detailed explanation on how to enable single sign-on for SAP Fiori-based applications using Kerberos/SPNEGO, X.509 certificates, or

---


SAML assertions is available as part of the SAP Fiori Infrastructure rapid-deployment solution.  

SAP NetWeaver Business Client enables users to access data from ABAP backend systems using multiple user interface technologies, such as traditional SAP GUI transactions and applications based on Web Dynpro ABAP. **Figure 4** shows vendor data displayed in an SAP NetWeaver Business Client user interface. To make data access both simple and secure, you can combine SAP NetWeaver Business Client with SAP Single Sign-On and, by leveraging its Kerberos/SPNEGO technology, simply reuse the user’s Windows domain authentication for single sign-on.

**Simplified ABAP Administration**

SAP Single Sign-On 2.0 includes various features that help streamline administration tasks required for enabling access to the ABAP backend. In particular, it provides enhancements for setting up Secure Network Communication (SNC) and configuring Kerberos/SPNEGO on the ABAP backend. SNC is the interface used to enable single sign-on and network encryption from SAP GUI and numerous Remote Function Call (RFC) clients to the ABAP backend server. While setting up SNC has always been a straightforward task, support package 4 for SAP Single Sign-On 2.0 makes it even easier with support for the SNCWizard transaction, a new transaction included with the ABAP support packages for SAP NetWeaver that enables the easy configuration of SAP NetWeaver AS ABAP for SAP Single Sign-On. This wizard guides administrators through the configuration of SNC for SAP Single Sign-On 2.0 (see **Figure 5** on the next page) and automates tasks, such as creating the required Personal Security Environment (PSE) files and setting the server

---


profile parameters, that previously required access on the operating system level. The wizard enables ABAP administrators to configure SNC on their own, without time-consuming and resource-intensive interaction with the operating system administration team. As manual steps are reduced, administrators no longer need to worry about a typo in the configuration preventing the server from restarting.

In addition, support package 4 for SAP Single Sign-On 2.0 includes an update of the Kerberos transaction to simplify the configuration required on the ABAP system for single sign-on based on Kerberos/SPNEGO — a popular approach among SAP customers for authentication with SAP GUI and web clients because it avoids the need for additional servers by relying on existing Microsoft Active Directory functionality. As part of the Kerberos transaction, SAP provides a number of online checks that detect inconsistencies between the configuration of Microsoft Active Directory and the ABAP system, enabling the ABAP administrator to validate the Kerberos configuration without requiring support from the Microsoft Active Directory team, which streamlines the process significantly. Figure 6 demonstrates part of the validation process.

### Enhanced Cryptographic Support

As consumers and businesses become increasingly concerned about data security, cryptography is no longer a topic reserved for cryptographic experts. To take security to the next level for its customers, SAP delivers the Common Cryptographic Library (CommonCryptoLib) — available via the

---

FIGURE 5 ▲ The SNCWizard transaction guides administrators through the configuration of SNC for SAP Single Sign-On

FIGURE 6 ▲ SAP provides checks for validating the Kerberos configuration against Microsoft Active Directory

---

See SAP Note 2015966 (http://service.sap.com/sap/support/notes/2015966) and SAP Note 2079851 (http://service.sap.com/sap/support/notes/2079851) for details on the required ABAP versions.
ABAP kernel or via download from SAP Service Marketplace — for enabling digital signatures and performing encryption in SAP systems. While in the past SAP Single Sign-On required two separate security libraries, SAP Single Sign-On 2.0 now uses the Common Cryptographic Library as its default library for SNC and Kerberos/SPNEGO for ABAP, and to enable the use of optional hardware security modules to store and protect private keys, making installation much simpler.

Starting with support package 5, the library provides support for elliptic curve cryptography, and initially focuses on the curves most relevant from a market perspective, such as the prime field curves P-192 to P-521, as documented in the Federal Information Processing Standards (FIPS) publication on the Digital Signature Standard (DSS). For a given key size, this form of encryption provides significantly higher data security than previous encryption algorithms, which is why elliptic curve cryptography is being implemented by many of the latest smart card solutions. With support for version 1.2 of the Transport Layer Security (TLS) protocol also included in the latest version of the library, these smart card solutions can now authenticate to an SAP system using SSL client authentication, with the additional security of elliptic curve cryptography as well as perfect forward secrecy to protect customers from future attacks on recorded communication data.

In addition, in January 2015, SAP received the FIPS 140-2, security level 1 certificate for SAP’s cryptographic kernel, ensuring that it works securely and as designed to guarantee protection of your sensitive business data. This certification further demonstrates SAP’s commitment to provide customers with solutions of the highest quality and reliability, along with security they can count on, based on independent, internationally applied standards.

**Summary**

The extensions included in the latest support packages for SAP Single Sign-On 2.0 not only enhance productivity with a simplified user experience, but also lower administrative costs and strengthen the security and confidentiality of login information and sensitive business data.

SAP Single Sign-On is based on a mature set of core components that enable SAP customers to implement secure single sign-on with confidence across enterprise scenarios that range from SAP Business Suite implementations to heterogeneous environments that integrate non-SAP systems, and even cloud-based and cross-company scenarios. While SAP continuously innovates to fulfill customer requests and to meet evolving security demands — such as single sign-on from mobile devices and more efficient management of the certificate life cycle — the overall vision is to keep the product solid and simple to implement and use.


---