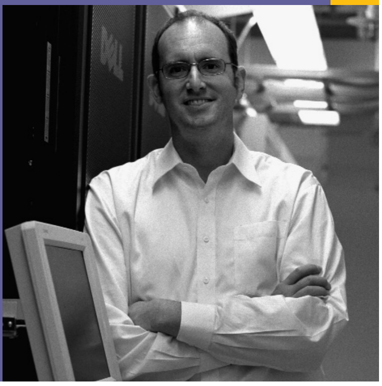
SAP Technical Brief



INTEROPERABLE: SAP NetWeaver™ PLATFORM AND Microsoft ACTIVE DIRECTORY

In today's complex, heterogeneous IT landscapes, users often log on separately and with different passwords to numerous systems, thus complicating user management, increasing the possibility of error, and using valuable IT staff time. SAP® software, built on the SAP NetWeaver™ platform, provides a solution to these problems, as it interoperates with Microsoft Active Directory. This enables the use of single sign-on, which reduces the number of user identities that need to be managed.

Introduction

A centralized user management and single sign-on process can reduce the operational costs of user management in an IT landscape significantly, while also increasing productivity of the individual end user. With standard interfaces from SAP, it is possible to implement a centralized user management and single sign-on process, based on existing SAP and Microsoft infrastructure, allowing for a fast return on investment.

That is because the SAP NetWeaver™ platform is fully interoperable with Microsoft Active Directory, which is used by many SAP customers since it is part of the Microsoft Windows Server platform. SAP NetWeaver unifies integration technologies into a single platform and is preintegrated with business applications, which reduces the need for custom integration and lowers your total cost of ownership (TCO). Its component, SAP® Enterprise Portal, can serve as an end-to-end single sign-on solution that fits the needs of most companies leveraging existing directories, such as Active Directory, via Lightweight Directory Access Protocol (LDAP).

The Challenge

In today's complex system landscapes, employees often have to authenticate themselves separately in different SAP software–based systems. The problem is compounded by the existence of additional passwords, such those used to log on to individual workstations through Active Directory or other non-SAP software.

User management for all these processes is usually distributed. Whenever an employee enters a company's IT systems or moves to another company location, that person's logon information must be created and maintained manually across various systems, and by different user administrators.

Deactivation of a user from various systems – for example, when an employee leaves the company – is crucial to security in big enterprises, since every account of a terminated employee is a potential security hole. Therefore, control of the user-administration process is very important.

Security guidelines usually dictate that passwords have to be changed regularly in all systems. If password life cycles differ in SAP software-based systems and other systems, such as Active Directory services, then a user's password might be valid in one place and be invalid in another. Not surprisingly, users are annoyed by the continuous need to change their passwords for multiple systems. This results in a huge number of calls to a company's IT help desk from users who have forgotten their passwords.

The problems described also present security risks, because users tend to choose either passwords that are easy to remember – and also easy to guess – or so complicated that users must write them down, leaving reminders on their keyboards or other places where they are easy to find. In a typical situation, a company can get at least one help desk call per user, per month, about passwords. In a IT landscape with 2,000 users, that's 24,000 calls a year.

Finding a Solution

Reducing the time spent on managing user accounts by automating the user-administration process can free up vital resources in IT departments. And simplifying and decreasing the number of different logon procedures with single sign-on can increase end-user productivity.

To do this, you need a **central user repository** that can be accessed by various applications using open standards such as LDAP. Using a central user repository enables the central maintenance of user data, thus avoiding redundant, error prone maintenance of user information in several systems. And it allows user administration to assign user rights in various applications with one keystroke. **Automated user provisioning** reduces the administrative overhead for creating user identities manually in various systems. A good solution for logon problems is **single sign-on**, which provides users with a single password that enables access to every system. With single sign-on, administration costs and efforts are drastically reduced.

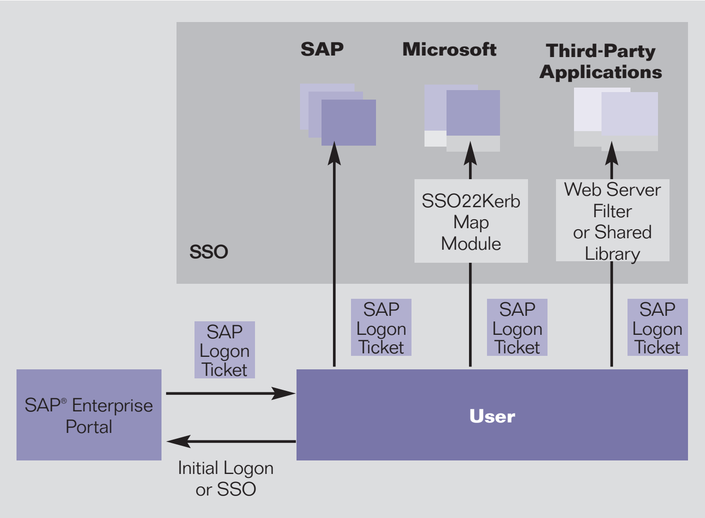
Single Sign-On

Single sign-on is a key functionality of SAP Enterprise Portal that eases a user's interaction with the many component systems available to him or her in a portal environment.

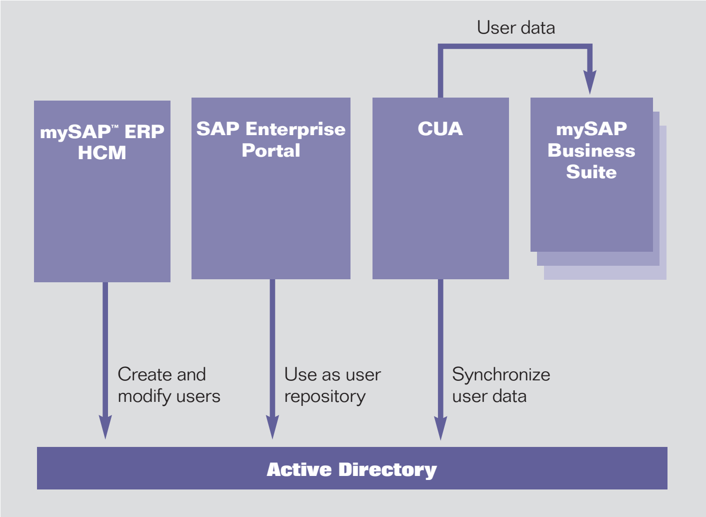
Authentication of portal users can be delegated to Active Directory. Users can log on to SAP Enterprise Portal using their Microsoft Windows password, since Active Directory can be utilized as the user repository for SAP Enterprise Portal. In an intranet scenario, SAP Enterprise Portal supports Windows Integrated authentication as an external authentication method. In this case, the credentials a user provides during the initial logon to his or her workstation can be reused.

After logging on to SAP Enterprise Portal, the user is issued an SAP logon ticket. SAP logon tickets are the flexible central authentication tokens used with SAP software that can also be used for single sign-on to all SAP software systems as well as multiple non-SAP back-end systems.

Third-party applications can also leverage SAP logon tickets for single sign-on. To enable this, SAP provides a Web server filter that can be used for authentication by means of an HTTP header variable, a dynamic-link library, and Java classes for verifying SAP logon tickets in third-party software. The dynamic link library and Java classes can be used to provide native support for SAP logon tickets in custom-developed applications written in C, Visual Basic, or Java.



How Single Sign-On Works



User Management

SAP has developed a new Kerberos-compatible ticket-bridging mechanism that allows single sign-on to Microsoft Web-based back-end applications by means of SAP logon tickets, based on new delegation features that are available with Microsoft's Kerberos implementation in Windows Server 2003 and Active Directory 2003.

With single sign-on, a portal user can access applications in back-end systems without the need to provide a user name and password. Since users only have to remember one password (their Active Directory password) instead of several user names and passwords for each back-end system, help desk calls about forgotten passwords or reset of passwords can be kept to a minimum.

Central User Management

SAP NetWeaver and Active Directory can be integrated in terms of user management. With Active Directory as a central user repository, you can centrally maintain user data, thus avoiding the redundant, error-prone maintenance of user information in several systems. You get access to this data through standard LDAP.

HR data in SAP software can be used to control user life cycles in Active Directory. When a new employee enters an organization, its HR department can store information about that employee in the mySAP™ ERP Human Capital Management (mySAP ERP HCM) solution. At the same time, existing employees can update their personal information in mySAP ERP HCM using employee self-services: the solution provides an interface that allows the creating and modifying of user identities in Active Directory from employee data stored in mySAP ERP HCM.

Whether created automatically or manually, user information stored in Active Directory can be leveraged for user management by companies utilizing SAP Web Application Server or SAP Enterprise Portal, which are both components of SAP NetWeaver. The automated provision of users in SAP user-management software offers a simple, cost-effective solution. The user management engine (UME) of SAP Enterprise Portal can utilize Active Directory as a user-persistent store. Roles in SAP Enterprise Portal can be assigned to users and groups, leveraging existing information about users and groups in Active Directory.

www.sap.com/contactsap

User-management processes for SAP back-end software can also leverage data stored in Active Directory. User identities can automatically be created and maintained in mySAP Business Suite solutions, including mySAP ERP, using SAP Central User Administration and the standard BC-LDAP-USR interface of SAP Web Application Server. User identities can automatically be created and maintained in mySAP Business Suite solutions using, SAP Central User Administration and the standard BC-LDAP-USR interface of SAP Web Application Server.

Since user data is not entered manually, the accuracy of user data is enhanced and the process of changing user data is sped up. Immediately after a user identity has been created in Active Directory, that user can log on to SAP Enterprise Portal and all SAP back-end software using a single sign-on. The integration of user management and single sign-on also helps boost security. Users need to remember only one password: they no longer need to leave notes with their passwords lying around.

Cutting Costs and Freeing Up Resources

SAP software user management can be easily integrated with Active Directory, resulting in substantial cost savings for SAP customers. That is true not only because IT staff time and effort is reduced, but also because the integration enables you to leverage existing SAP and Microsoft licenses without further software investment.

IT departments can substantially reduce the number of help desk calls from users with password problems when these errors no longer occur in multiple systems. With your IT department workload significantly reduced, user satisfaction high, and cost benefits realized, you can utilize IT staff in a more productive way – to add value to the business.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group 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.

THE BEST-RUN BUSINESSES RUN SAP™