

Single Sign-On Products

Stop frustration over multiple sign-on requests

In many organizations, users struggle with having to sign on multiple times to access different applications, Web portals, and servers. As the number of mandatory unique sign-ons grows, the burden on users to remember numerous usernames and passwords increases. The result is often unhappy users who innocently create serious security breaches by writing down usernames and passwords because they can't remember them all. Frustration might also extend outside an organization. Business partners, field representatives, and customers might need to access multiple Web portals or applications from outside the organization (typically over the Internet), and they might also be subject to multiple sign-on requests.

Unfortunately, reducing the need for multiple sign-ons isn't a simple task. The products that address this problem use one of two approaches:

- Enterprise single sign-on (SSO) products—These products target an end user's desktop sign-on. Because the user sign-on process is often the weakest link in the security chain, enterprise SSO products can provide alternatives to username/password credentials that include smart cards and biometric identification.
- Web SSO products—These products use a Webcentric approach to solve the problem. With this approach, a user signs on to an internal or external Web portal, and all subsequent applications run in that browser context. In most cases, this approach requires username and password authentication at the portal but can occasionally use public certificates.

The primary purpose of enterprise SSO and Web SSO products is to arbitrate between the user and target applications. If the user accesses an application that requires a separate authentication, the SSO product must do one of two things: pass the initial user credentials to the application for behind-the-scenes authentication or map the user credentials into a different set of credentials that it passes to the application for behind-the-scenes authentication.

JOHN ENCK
(john@enck.com) is a vice president and research director for Gartner. He has written more than a dozen commercial computer books and hundreds of articles.

In a heterogeneous server environment, credential arbitration depends on many moving components. Terminal emulators need to pick up credentials and emulate the sign-on process for the host. Scripts handle applications that demand a separate sign-on. And you need to have username/password synchronization software in place to keep different user repositories current and synchronized. All

these components bring to the table technical nuances that make SSO difficult to achieve.

Reduced Sign-On

Although SSO products provide clear benefits to end users, they might present security risks to the IT organization. For example, standardizing on one username and one password across all servers and applications increases the risk of a security breach. A successful AD attack could enable an intruder to penetrate into multiple servers quite easily if the servers all share the same authentication credentials.

Because of such security concerns, many IT organizations have taken the alternative approach of reduced sign-on. With a reduced sign-on approach, IT organizations determine which servers and applications can share a common sign-on, which servers and applications require a separate sign-on that uses the same user credentials, and which servers and applications require different user credentials.

A reduced sign-on approach is a less than perfect solution from the user's perspective. With reduced sign-on, a user signs on to a desktop or Web portal and can access one set of applications and server resources without having to sign on again. However, some applications or server resources might require additional sign-ons with the same username and password, and another set of applications might require additional sign-ons with a completely different username and password.

Reducing users' sign-on complexity problems requires a balance between user satisfaction and security. If the scale swings too far toward security when trying to prevent a breach, user satisfaction decreases. Similarly, if the scale swings toward user satisfaction, you can compromise IT security.

Selecting an SSO Product

If you decide that an enterprise SSO or Web SSO product is right for your organization, you must determine which one is a good fit for your infrastructure. For example, you need to verify that the enterprise SSO product supports the desktop environments you use. You want to make sure that any Web SSO product you're interested in will integrate well with your portal infrastructure (e.g., Microsoft IIS, Sun Microsystems' Sun Open Net Environment—ONE, Apache). In each case, you need to evaluate whether the sign-on product supports your target platforms and applications. Finally, you must make sure the SSO product you choose can support mainframe applications.

EDITOR'S NOTE

The Buyer's Guide summarizes vendor-submitted information. To find out about future Buyer's Guide topics or to learn how to include your product in an upcoming Buyer's Guide, go to <http://www.winnetmag.com/buyersguide>.

Windowscentric enterprises should also evaluate how an SSO product integrates with Active Directory (AD). SSO products that can leverage AD as their authoritative user directory will provide the best integration. Conversely, products that force you to implement an alternative directory will complicate your infrastructure and might require you to

implement additional solutions, such as metadirectory or user-provisioning products, to synchronize accounts between AD and the SSO directory.

Make sure to closely examine the product licensing structure. Most vendors prefer to offer per-user licenses (often with additional per-connector licenses), but most enterprises prefer to

purchase under a per-processor or a tiered pricing structure (i.e., you pay a fee for a certain number of users). Be prepared for heavy negotiation to achieve a fair pricing structure, and keep in mind that obtaining competitive bids from several vendors is essential to the negotiation process.

InstantDoc ID 40453

Contact Information	Product Name	Price	Description
ActivCard 510-574-0100 800-529-9499 http://www.activcard.com	Trinity Secure Enterprise Sign-On	\$30 to \$79 per user, depending on configuration and quantity	Designed for large-scale distributed enterprises; can reduce Help desk support costs for password resets; improves security through multifactor authentication, including biometrics, without requiring additional third-party products; authorizes access to workstations, networks, applications, and Web sites
ASG 239-435-2212 800-726-5555 http://www.asg.com	ASG-Focal Point for Enterprise Single Sign-On	Approximately \$30 per user	A scalable, comprehensive Web-based SSO solution; supports crucial applications; provides high availability by taking advantage of fault-tolerant servers and replication facilities from corporate databases and enterprise directories
Cafesoft 858-455-1800 http://www.cafesoft.com	Cams	\$2995	Web SSO and access control software that centralizes Web security management for Microsoft IIS, Apache, and Java 2 Enterprise Edition (J2EE) servers; supports AD and Microsoft SQL Server either as a primary or secondary user directory; runs on Windows Server 2003, Windows 2000, Windows NT, Red Hat Linux, and Sun Solaris systems
Citrix Systems 954-267-3000 800-437-7503 http://www.citrix.com	Citrix MetaFrame Password Manager	Contact vendor for pricing	An SSO and password security solution that can access password-protected applications running in the Citrix MetaFrame Access Suite environment or on a variety of local clients; provides secure access to Windows, Web, proprietary, and host-based applications
Communicator 914-872-2800 http://www.communicator.com	Hub ID	Contact vendor for pricing	Solution for Web-based and enterprise applications; can provide user authentication or integrate with existing authentication infrastructure; supports multiple data stores and protocols, including AD, Lightweight Directory Access Protocol (LDAP), and Simple Object Access Protocol (SOAP)
Computer Associates 631-342-6000 800-225-5224 http://www.ca.com	eTrust Single Sign On	Starts at \$7500 for a 100-user pack	Automates access to all authorized Web services and enterprisewide applications through one logon; provides users and customers with instant access to personalized resources; can use network authentication for AD as primary user authentication; runs on XP, Win2K, NT, Windows Me, Win 9x, HP-UX, Sun Solaris, and IBM AIX systems
Datakey 952-890-6850 888-328-2539 http://www.datakey.com	Datakey Axis	\$100 per user	A smart card-based solution for the enterprise; consolidates all credentials and user identities onto one smart card and automates access through SSO; automates policy, credential, and desktop management through Management Center; supports all Windows OSs

Contact Information	Product Name	Price	Description
Entrust 888-690-2424 http://www.entrust.com	Entrust GetAccess 7.0	Contact vendor for pricing	A scalable Web access control solution; enables Web SSO and enterprise SSO; centrally manages access to multiple applications through one portal; features AD support as either the primary or secondary authentication source; supports many platforms and applications, including Microsoft Internet Explorer (IE), Netscape Communicator, IIS, and Sun ONE
IBM Tivoli 512-286-0000 877-848-6541 http://www.ibm.com/software/tivoli/products/access-mgr-e-bus	IBM Tivoli Access Manager for e-business	Priced per user or site license	Policy-based centralized access control system; features integrated security for customer relationship management (CRM) and enterprise resource planning (ERP) e-business solutions, Windows desktop SSO, and delegated administration; supports access from wired and wireless devices; supports a range of directories; OS support includes Windows, Solaris, AIX, HP-UX, and Linux; Web platform support includes IIS and IBM WebSphere Application Server
Imprivata 781-674-2700 http://www.imprivata.com	Imprivata OneSign	\$7995 for 100-user appliance	Appliance that provides automated SSO of enrolled subscribers to multiple applications; securely unifies user credentials for applications into a single identity; supports Web, client, server, and legacy applications; supports all the back-end environments you have listed for SSO; the SSO agent runs on XP, Win2K, NT, and Win98
Microsoft 425-882-8080 800-426-9400 http://www.microsoft.com	.NET Passport	Contact vendor for pricing	Suite of services for authenticating users across a number of applications; suite includes the Passport SSO service and Kids Passport service; lets users create one set of credentials that will let them sign in to any site that supports a Passport service; requires a Windows server but you can refer to a third-party solution to implement Passport on other platforms
Netegrity 781-890-1700 800-325-9870 http://www.netegrity.com	Netegrity SiteMinder	Priced per user	Web SSO solution lets you centrally administer and enforce user authentication and authorization management; scalable; supports users; AD and Kerberos; library of interface modules can serve as front end to most legacy applications; OS support includes Win2K, NT, Solaris, Red Hat Linux, HP-UX, AIX, and IBM OS/390
Novell 801-861-7000 888-321-4272 http://www.novell.com	Novell SecureLogin 3.5	\$79 per user	Provides SSO to a range of systems, including Win32, Web applications, Citrix, Telnet environments, mainframe applications, and terminal emulators
Oblix 408-861-6100 800-438-0626 http://www.oblix.com	Oblix NetPoint	Starts at \$10 per user with enterprise licensing available	An integrated enterprise identity management and Web access solution; scalable; connects users to crucial business systems and maintains consistency with core business processes; supports Windows Server 2003, Win2K, NT, Solaris, and AIX; Web server components support Windows 2003, Win2K, NT, HP-UX, AIX, Linux, and Solaris
OpenNetwork Technologies 727-561-9500 877-561-9500 http://www.opennetwork.com	Universal Identity Platform (IdP)	Priced on a per user basis	Provides .NET and Java-based management; features Web-based access control, authentication, authorization, SSO, delegated administration, and auditing capabilities

Contact Information	Product Name	Price	Description
PassGo Technologies 888-652-3983 home@passgo.com http://www.passgo.com	SSO Plus	Contact vendor for pricing	A password-management product that lets users access all applications on their desktop with one user ID and password
Passlogix 212-825-9100 866-727-7564 http://www.passlogix.com	v-GO SSO 4.0	\$60 per user, with volume discounts available	An enterprise SSO solution that supports AD as primary or secondary authentication source, depending on configuration; supports Windows OSs and mainframe, homegrown, and Web applications
Protocom Development Systems 800-581-3502 support@protocom.com http://www.protocom.com	Protocom SecureLogin Single Sign-On 3.5	\$79 per user	An enterprise SSO solution that supports AD as the primary authentication source; supports most commercial and homegrown 16- and 32-bit applications; provides support for more than 150 mainframe, UNIX, ANSI, and custom terminal emulators; supports Telnet emulators; supports Citrix MetaFrame and NT Server 4.0, Terminal Server Edition (WTS); features directory support for AD, eDirectory, NT domains, iPlanet, and any LDAP-compliant directory
RSA Security 781-515-5000 800-495-1095 http://www.rsasecurity.com	RSA ClearTrust	Pricing starts at \$26 per user for as many as 1000 users	Designed to let enterprises manage and enforce a centralized authentication policy; Web SSO functionality lets users seamlessly navigate across multiple applications and domains; identity management capabilities enforce business policy; supports AD; OS platform support includes Win2K, NT, Solaris, Red Hat Linux, Red Hat Enterprise Linux AS, SuSE Linux Enterprise Server, HP-UX, and AIX
Schlumberger 713-513-3000 http://www.slb.com/dexabadge	DeXa.Badge	Price based on volume	Provides enterprisewide SSO with smart card portable security; supports most Windows, Java, Internet, and intranet applications, Web sites, and more than 150 commercial terminal emulators; leverages existing infrastructure, including eDirectory, AD, NT domains, and LDAP-compliant directories; can randomly generate passwords
Utimaco Safeware 508-799-4333 http://www.utimaco.com	SafeGuard Advanced Security	Contact vendor for pricing	Extends security functions of the Windows OS and server-based computing environments; features a two-factor logon through a smart card; also available as a PIN or fingerprint authentication between workstations and servers; the SSO function provides automatic, wizard-based password administration; offers extended rights administration for integrity protection
Wedgetail Communications 415-929-2288 http://www.wedgetail.com	JCSI SSO	\$7500	SSO solution for J2EE applications that use AD; features a pure Java server-side component suite that provides authentication by using the Windows integrated login and Kerberos technology; supports enterprise SSO; OS platform support includes Windows, Solaris, Linux, HP-UX, AIX, and OS/400; uses AD as the primary authentication source