



webCONNECT SSO

WebConnect SSO

Secure Single Sign-On White Paper



Executive Summary

Secure Single Sign-On (SSO) is fundamental to a comprehensive identity management program and architecture. Organizations should expect it to create value and to be cost-effective. This white paper will describe how organizations can leverage SSO by finding a worthy partner and adopting the appropriate technology.

Single Sign-On (SSO) Defined

Single sign-on (SSO) means a user can, with a single action, be granted all appropriate accesses to all computers, systems and applications. This eliminates the need to enter multiple passwords. Single sign-on reduces human error, a major component of systems failure. It also has been proven to greatly reduce help desk requests, saving time and money and allowing organizations to reallocate resources. Though single sign-on is highly desirable, it is not always easy to implement. Choosing the right vendor/partner is critical.

SSO and Business Needs

It is quite possible to make investment mistakes because many IT professionals do not have a clear understanding of SSO needs or the solution that can address those needs. The confusion in the marketplace is growing just as fast as the number of vendors. But the need is growing too.

More than 75 percent of all business information still resides on mainframes; the problem is that the mainframe can be very difficult to access. Recent research shows that organizations with annual revenue greater than \$500 million typically have more than 75 applications, databases and systems that require user authentication. Significantly, some 38 percent of external users and 75 percent of internal users are contained in multiple data stores, meaning a single change to a user's ID or access privileges must be input multiple times. The complexity is multiplied many times when there are dozens, if not hundreds, of data stores, applications and databases involved.

The simplicity of single sign-on means reduced help desk calls, reduced costs and enhanced security – for example, no more passwords scrawled on notes stuck to terminals. The ROI of single sign-on comes from greatly reduced user error and the time saved from not having to log in multiple times in multiple applications, or contact the help desk. Enhanced security can be easily addressed, since users often choose passwords that are easy to predict and guess. On the administrative side it's not easy maintaining thousands of separate passwords.

It is important to note that the full benefits of single sign-on are not realized unless an organization endeavors to have full coverage of its IT assets, including the mainframe. The problem is that most major players in this arena don't have an effective mainframe solution. An exception to this issue is OpenConnect. The ability to provide a mainframe SSO solution is becoming increasingly important as partners, vendors, customers and an increasing number of employees need access to mainframe data via Web services.



How OpenConnect Handles SSO

OpenConnect's WebConnect SSO is an example of a cost-effective way to ensure the security of Web-based access to mainframe applications and information. WebConnect SSO delivers secure single sign-on access to multiple mainframe applications with just one mouse click. With WebConnect SSO, user IDs and passwords are stored within the "glass house," thus eliminating serious security issues that result from passwords and login information being stored on the desktop. In addition, WebConnect SSO logs the user off if a session is disconnected before the user can manually log off. This prevents password reset problems that could occur with an improper log off. With its patented persistent secure browser-based access, only WebConnect SSO can support tens of thousands of concurrent Web-based users and at the same time provide organizations with the lowest total cost of ownership.

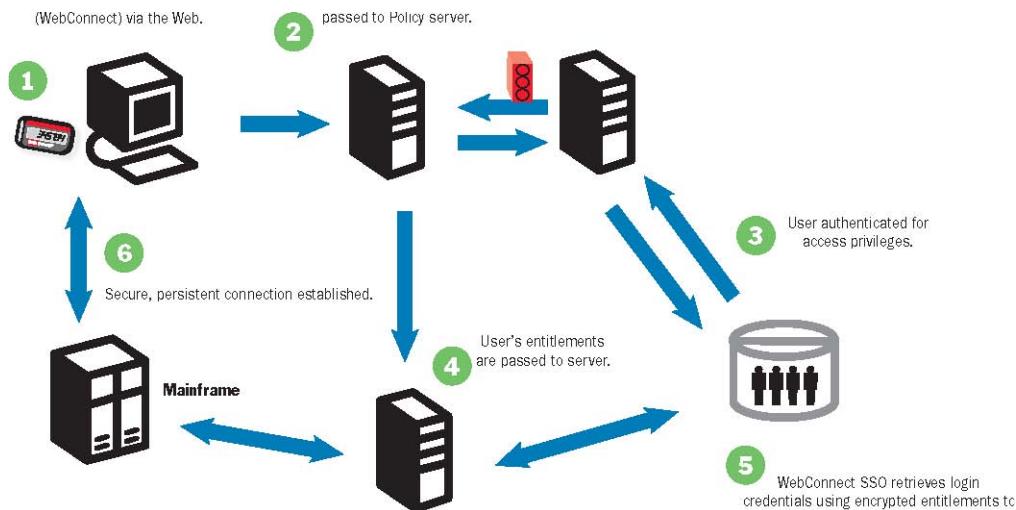
WebConnect SSO Benefits

Organizations can use WebConnect SSO to ...

- > Greatly reduce help desk support costs by eliminating the majority of user access and privileges related questions.
- > Make employees and IT professionals more productive by consolidating mainframe information and application identity management.
- > Efficiently and securely push vital mainframe information and applications out to customers, partners and employees.
- > Gain a more holistic view of the business by integrating mainframe and other line of business applications.

WebConnect SSO Technical Overview

WebConnect SSO works seamlessly and transparently in complex and disparate environments, and is agnostic to an organization's Identity Management solution. The controller applet within WebConnect SSO also manages multiple sessions at one time, enabling users to manage their sessions and terminate them cleanly, allowing employees and IT professionals to be more productive.



User requests access to Mainframe application Encrypted credentials are

webCONNECT SSO complete **Single** Sign-On process.

Integration with Identity Management Applications

OpenConnect works with many identity management programs including IBM Tivoli, SiteMinder, Oblix, etc. Specifically, OpenConnect has integrated RSA Security's encryption technology into its products for years. More recently, OpenConnect has received RSA SecurID and RSA ClearTrust Certifications, which validate WebConnect SSO's interoperability with RSA Security's array of identity and access management solutions. These certifications signify that WebConnect SSO complies with and takes full advantage of RSA Security's market-leading security technologies. The unique combination of RSA ClearTrust and WebConnect SSO fills a serious gap in the secure SSO connectivity space. With WebConnect SSO the mainframe becomes an RSA ClearTrust software protected resource within the enterprise. Once a user has been authenticated and granted access by RSA ClearTrust software, WebConnect SSO takes over to seamlessly and securely complete the sign-on process into multiple host systems and applications - all with a single click on a Web page.



Benefits

Security benefits include the security information being harbored behind the “glass house.” External end-users, such as business partners and vendors, can be shielded from knowing the actual password to the mainframe, as well as the password structure. OpenConnect optionally adds another layer of security by changing passwords in the background, transparently to the end user. It does this by using an administrator-supplied template of alpha and numeric characters, and automatically recognizing when the sign-on process requests a new password. This also makes it easier for users to stay in compliance with periodic mandated password changes.

ROI

Industry Analysts estimate shows that SSO solutions reduce help desk volume by 33 percent, along with a corresponding 32 percent increase in overall security. Overall, an effective SSO solution can result in a 15 percent increase in user and IT productivity and an 18 percent gain in efficiency. SSO also eliminates costly password resets: the average user requires a password reset 5 times per year, at an estimated cost of \$50 per reset. To an organization with 5,000 mainframe users, that could result in a \$1.25 million cost savings in the first year alone.

Companies have made a considerable investment in mainframes and midranges and the business processes/ information that flow through them. By building a Mainframe-to-Web solution, IT departments are able to provide the functionality their users require and meet the stringent ROI requirements needed to launch an IT project. You have an obligation to expect and demand a quick payback. As an example, OpenConnect’s Secure Mainframe2Web Solutions Series provides payback in less than a year. This ROI is based on the ability to immediately enhance security, increase productivity and reduce resource requirements to complete specific tasks.

Getting Started

To get an idea of the scope of an identity management project, a company needs to discuss its priorities. Is single sign-on mainframe access necessary? If so, choose your vendor/partner carefully. SSO solutions should offer flexible storage options, including LDAP, as well as handle password changes and sign-on exceptions dynamically. For Mainframe-to-Web technology selection, the focus will be on the need to maneuver password changes effectively and the ability to integrate with other systems. That’s why OpenConnect partners with companies like RSA and IBM Tivoli. Another need is scalability. If thousands of users must sign on at one time, then the vendor must be skilled in operating that kind of volume. Is your organization likely to be adding more SSO users? If the answer is “yes,” then you must consider the future impact of that decision.

Another feature to look for is true single sign-on protection (versus scripted log on) for multiple data sources at the application layer. OpenConnect offers four layers of protection: application, session, transport and host. OpenConnect also offers secure connection and authentication encryption, along with the flexibility of a concurrent licensing model.



Choosing a Partner

One way to be assured of finding a partner that is solid, reliable and experienced with the proper technology, is to find a vendor with a long history, one that has survived – if not even thrived – through the good times and bad. Another factor is the company's services. Do they offer great professional services and training? OpenConnect has been in operation since 1982 and has an extensive track record of success with blue-chip customers, as well as strategic partnerships with leading mainframe and security players. The company is a proven thought leader – an innovator that listens to customer needs and constantly adds new features and functions, and a company that partners with industry leaders such as IBM Tivoli and RSA Security. Look for a company with products robust enough to meet all your needs. OpenConnect's products include WebConnect, a persistent, secure Mainframe-to-Web access solution; and WebConnect SSO, which provides secure sign-on Mainframe-to-Web access.

OpenConnect's WebConnect SSO facilitates the automation of single sign-on to multiple host applications with a single mouse click. Host user IDs and passwords are stored in the "glass house," eliminating security issues arising from desktop-stored login information. The company's Secure ClientConnect places an SSL security wrapper around desktop clients, using OpenConnect's "persistent connectivity" technology to establish a secure, persistent connection to mainframe applications.

Be sure to look at your vendor's partners. Make sure that they have partnered with organizations that share a successful history and have retained a satisfied client base.

Technical Requirements

WebConnect SSO has the following technical requirements...

Platforms Supported:

- Sun Solaris 2.8+
- IBM AIX 4.3+
- HP-UX 10.20+
- Red Hat Linux 7.0
- Windows NT Server 4.0
- Windows 2000
- Linux for S/390; SuSE 7.0, Red Hat 7.2

Hardware Requirements

- 64 MB Ram required per 1000 concurrent users
- 300 MB hard-disk space



Browser Requirements:

- Netscape 4.5+ Series
- Netscape 7.0+ with JRE 1.4.x
- Microsoft Internet Explorer 5.0.1 with JVM Build 3167 or greater
- JRE Version 1.4.x

Conclusion

Find the right vendor/partner and get SSO done quickly. You cannot afford to be without top-notch security. Every company needs secure access to the host, and every company needs to unlock and unleash the information in its mainframe.

In today's volatile economic climate, the old adage of win-win (in this case increased security and better information distribution) is not enough. You must deploy cost-effective, manageable solutions that increase security and better information distribution. A single sign-on solution, such as OpenConnect's WebConnect SSO arms organizations with secure methods to improve productivity, increase accessibility and reduce costs.

OpenConnect Systems, Inc.

2711 LBJ Freeway Suite 700 Dallas, TX 75234

Phone :: 972.484.5200 Fax :: 972.484.6100

Web :: www.oc.com

Email :: info@oc.com

© 2006 OpenConnect Systems Incorporated. OpenConnect Systems is a registered service mark of OpenConnect Systems Incorporated. OpenConnect and all other OpenConnect product names are trademarks of OpenConnect Systems Incorporated. All other products or services mentioned herein are trademarks of their respective companies. The technology of WebConnect is covered under U.S. Patent number 5,754,830.