



The Realities of Single Sign-On

PistolStar, Inc.
PO Box 1226
Amherst, NH 03031
USA

Phone: 603.546.2300
Fax: 603.546.2309
E-mail: salesteam@pistolstar.com
Website: www.pistolstar.com

The Realities of Single Sign-On

Table of Contents

Introduction	1.0	
What is True Single Sign-On (And is it Even Possible?)	1.1	
Purpose and Overview	1.2	
All About Single Sign-On	2.0	
Single Sign-On's Upside (& Dispelling the Reputed Downside)	2.1	
The Power Of SSO	2.1.1	
Not to be Confused With Password Synchronization	2.2	
Existing Definitions of Single Sign-On	3.0	
The Many Login Methods Considered Single Sign-On	3.1	
The Five Major Types of Single Sign-On	3.1.1	
Noteworthy Types of SSO Solutions	3.1.2	
Single Sign-On Variants	3.1.3	
Lotus Domino and Notes Single Sign-On	3.1.4	
How We Define Single Sign-On	3.1.5	
<i>What is True Single Sign-On (And is it Even Possible?)</i>	PistolStar's Password Power 8	4.0
	Robust and True Single Sign-On	4.1
	Access to the Notes ID	4.2
	Benefits to Lotus Users	4.3
Summary	5.0	
Appendix A – System Requirements	6.0	
Appendix B – Resources	7.0	

1.0 Introduction

1.1 What is true Single Sign-On (and Is It Even Possible?)

Single Sign-On (SSO) capabilities have been in existence for several years, yet the technology is still gaining steam. As *CRN* reported in April 2005, "If (recent acquisitions) are any indication, single sign-on (SSO) is hot." The article was referring to Oracle's buyout of Oblix and BMC's purchase of OpenNetwork, and it suggested that small SSO companies such as Version3 might also be targets for buy-out. The fact these acquisitions come on the heels of Computer Associates' 2004 purchase of Netegrity bolsters this contention.

SSO technology was developed in response to a new security issue (and opportunity) that arose as organizations installed more enterprise-wide applications — integrating new and legacy systems — and enabled greater intranet/extranet access to employees, customers and vendors.

To protect the valuable corporate data contained in their broadening computer and network environments, organizations incorporated strict security measures centered on the use of passwords. However, the complex procedures involved proved to be difficult for end-users to navigate, as they have to remember multiple passwords (as many as 8-10) and follow repetitive logon authentication prompts to access applications — all in an attempt to get their work done. To add to end-users' distress, IT security teams generally require that passwords are changed every 30 – 60 days, and place restrictions on setting new passwords that resemble previous ones.

As a result, most end-users sidestep password security best practices in favor of other methods, such as writing passwords on notes left in conspicuous places, using passwords that can be easily guessed by hackers, and constantly calling the Help Desk to obtain their passwords or reset them. The more difficult the login process, the more likely end-users resort to these practices, creating new security problems for organizations.

Password authentication measures have also posed a challenge for IT departments as they have been increasingly inundated with Help Desk calls about password resets, which drain their resources, time and productivity. IT administrators also face dealing with the network intruders who attempt and gain access by using openly-posted or easily-guessed passwords.

What SSO technology has done is alleviate the multi-password experience of end-users and the password management burden felt by IT staff by permitting end-users to make only one login attempt to access several platforms and applications.

In the simplest terms, single sign-on has been defined as follows:

- A specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems (From Wikipedia, http://en.wikipedia.org/wiki/Single_sign-on)
- A simplification of the security and logon process by consolidating multiple security schemes under a single authentication process. In other

Single Sign-On capabilities have been in existence for several years, yet the technology is still gaining steam.

words, a user can sign on once to a computer and have secure, protected access to multiple applications. (From CRN, "CryptoCard Speeds Sign Ons," 7/9/04)

- A consolidation of identities and passwords into a single repository that can be accessed by operating systems and applications. The key benefit to SSO is that users only need one set of credentials to access a particular line of business systems, which brings convenience to the user while reducing Help Desk calls regarding user-access issues. (From CRN, "Finding Opportunities in Identity Management," 11/21/03)
- Users only have to remember one password in order to gain access to all their password-protected applications. They log on once, and the SSO software provides the necessary credentials, however complicated the requirement may be, to the various applications. (From SC Magazine, "Single Sign-On 2005," 2/05, <http://www.scmagazine.com/products/index.cfm?fuseaction=GroupTestDetails&GroupId=16892>)
- Single sign-on allows users to enter security credentials once (typically by logging into a workstation or a Web application) and have those credentials propagated to each local and network application the user accesses during his or her session. Local applications exchange authentication information directly, while remote network applications exchange authentication information across the network via encrypted security tokens." (From devx.com, "Cross-Domain Single Sign-On Authentication with JAAS," 8/5/05)
- While the above definitions are articulated differently, the interpretation is the same — single sign-on is the ability to logon once and access all platforms and applications in an enterprise that the user is authorized to use. However, when you look among the vendors who offer SSO, you find vastly different definitions (or interpretations) of the technology based on how each vendor enables it. The question is: Does anyone provide true "single sign-on?" Not only do some forms of the technology have their limitations and/or present security concerns, but many authors and analysts question whether SSO is even possible in a heterogeneous environment.

Single Sign-On has emerged as a significant technology that resolves a major issue for organizations with multiple platforms, servers and applications requiring unique usernames and passwords for access.

At present, there is no "universal" definition of SSO, no agreement on whether it is really possible and no understanding of what is considered *true* SSO.

1.2 Purpose and Overview

Single Sign-On has emerged as a significant technology that resolves a major issue for organizations with multiple platforms, servers and applications requiring unique usernames and passwords for access. As it has evolved and more vendors introduce (or acquire) their SSO capabilities, we are seeing numerous different types, implementations and subsequent definitions of SSO. Further, single sign-on "variants" have surfaced as a result of frustrated end-users pursuing the simplest means to getting authenticated and gaining access (for example, saving a password on the system by checking "Save to this Computer" when available in the application's authentication dialog box.)

In this paper, we will discuss SSO's upside as well as the arguments against it. We will also review all the many different types of SSO that exist. By conducting this review, the goal is to facilitate understanding of all the different login methods that are considered SSO, but also get to the heart of what truly

constitutes SSO in the current technological landscape.

We'll also present our definition of true SSO, which we arrived at by talking to customers about their most critical authentication needs and challenges, as well as what would most benefit their entire organization. We've developed a password authentication and management solution which embodies this definition of true SSO, especially for companies utilizing IBM Lotus technology.

The final section of this paper provides a brief overview of our solution. Password Power offers robust single sign-on but also other critical password management capabilities such as self-service password reset and automatic recovery of the Notes ID. It also delivers striking benefits, addressing and eliminating the password-related pains and burdens previously wrought on end-users and IT staff.

2.0 All About Single Sign-On

2.1 Single Sign-On's Upside (& Dispelling the Reputed Downside)

Single sign-on has clear and obvious benefits for an entire organization because of the simplicity and convenience it provides to end-users, allowing them to avoid the wasted time involved with forgotten passwords and frequent password prompts. However, SSO is not without its detractors.

A major argument against SSO (and it is a valid one) is that by allowing an end-user to have only one password to access all their applications, a hacker's intentions are made that much easier because all they need to do is obtain that one password and they gain unfettered access to all the user's resources in the enterprise. Clearly, the security ramifications are of major concern and the potential for catastrophe is high.

However, one password with high-quality password values is preferable to half-dozen or so passwords with low-quality or differing values that are posted somewhere in the end-user's cubicle or can be easily guessed. Of course, higher-quality passwords can exist on some or all applications without SSO. But, this is not very feasible, as the password policies would have to be handled on an application-by-application basis. Also, without SSO, individual applications can still be compromised.

That said, the concern that all applications are compromised when the single sign-on password becomes known to a hacker is easy to remedy by changing the central directory password. This is not possible for applications without SSO, because if one application is compromised because of a low-quality password, it may not be readily apparent which password. Also, it's more difficult for the administrator to reset that application's password.

The theoretical notion that SSO sacrifices security for convenience doesn't hold water when you realize the power of SSO, which greatly eases password management and the authentication process to the point that password security is tremendously enhanced. Hackers' guessing attempts are thwarted and end-users change their habits, since with only one password to remember, posted reminders are no longer necessary.

2.1.1 The Power of SSO

The power and value of SSO is generally associated with the convenience it

Single Sign-On has clear and obvious benefits for an entire organization because of the simplicity and convenience it provides to end-users, allowing them to avoid the wasted time involved with forgotten passwords and frequent password prompts.

offers users by releasing them from the constraint of managing numerous passwords. However, effective SSO also offers tremendous gains across the organization. To be most effective, a single sign-on solution should deliver benefits in the following areas:

End-Users

By enabling them to use just one password and make only one login attempt to access their applications, end-users are freed from having to remember multiple passwords and dealing with repeated login prompts. They also no longer experience downtime from waiting for password resets or recovery from the Help Desk. The time-savings involved leads to improved productivity and the authentication ease creates happier employees.

IT Administrators/Help Desk

It's debatable whether the end-users are the real beneficiaries of single sign-on. Password and account management for IT administrators is dramatically simplified, and with end-users no longer making constant password reset calls, the Help Desk can decrease the total number of calls it receives by as much as 30%. This significant reduction frees up a large chunk of time, allowing the IT department to increase productivity and devote resources to more serious matters.

Training

Among its end-users, single sign-on provides the most noticeable time savings to new employees, who generally experience a time-intensive learning curve when getting on new systems and applications. With SSO in place, new employees encounter less confusion with accessing their new applications and navigating their new organization's networks. SSO facilitates training as the authentication process occurs transparently without the need for additional logins and learning which password is for each application.

Security

Single sign-on plays a major role in boosting an organization's security and protecting corporate data. Its security contributions are significant: First, and most obviously, there's added security when end-users no longer have Post-it notes with their passwords placed on or near their computers. Second, SSO helps enforce password security policies such as password quality and expiration. Because of these two points, potential hackers will find considerably fewer opportunities for gaining access to your networks.

Compliance

In addition to strengthening security across the enterprise, single sign-on ensures that organizations fulfill the requirements of Sarbanes-Oxley and other recently implemented governmental regulations such as HIPAA and the GLB Act. Sarbanes-Oxley, in particular, necessitates periodic assessments of internal controls relating to the security of critical data, particularly financial information.

By guaranteeing enterprise-wide adherence to a strong password policy, SSO minimizes unauthorized access to critical financial applications and databases. SSO's strong and reliable authentication also contributes to controlling which end-users can access which applications. To make certain that regulatory compliance is achieved, a SSO solution should have capabilities for reporting on login attempts and end-user requested access to specific data.

To make certain that regulatory compliance is achieved, a SSO solution should have capabilities for reporting on login attempts and end-user requested access to specific data.

2.2 Not To Be Confused with Password Synchronization

Because single sign-on removes the need for several passwords, allowing the use of only one to enter various applications, it has sometimes been misconstrued as password synchronization. However, clear distinctions exist between the two capabilities.

With password synchronization, one password (such as Windows) is synched with the passwords of other applications (such as Notes and Domino HTTP) so that one and the same password can be used for each login prompt the end-user encounters. Even though only one password is needed, having multiple password prompts still creates a cumbersome login experience, as the average user might need to login 6-8 times in a single day. Administratively, password synchronization has more overhead, as it requires IT to still manage all the primary user accounts.

The beauty of SSO is that it allows end-users to have only one password *and* to login only once (hence, the reason it is called “single sign-on”). There’s a huge leap forward in usability.

3.0 Existing Definitions of Single Sign-On

3.1 The Many Login Methods Considered Single Sign-On

Most IT managers and security personnel are aware of two types of SSO — Web-based and non-Web-based (or legacy) SSO — and variations that could only loosely be considered single sign-on (see “Single Sign-On Variants” below). What actually exists are several types of SSO, single sign-on in hardware as well as software form, and client-side products offered along with server-side solutions.

A surprising fact is that SSO solutions aren’t always the end-all/be-all remedy they’re touted to be. Oftentimes, SSO solutions can pose issues for IT departments with respect to integration and management. Challenges range from maintaining user accounts and scripting custom sign-on processes for various network applications to dealing with the heterogeneous nature of most enterprise systems.

Some SSO products require a great deal of setup — they don’t work right out of the box. There is often the need for cross-department collaboration and teams as the administrators for Microsoft Active Directory, LDAP and any other systems included need to be involved. For the more complex offerings, a fair amount of scripting may also be necessary to set up the access rules.

3.1.1 The Five Major Types of Single Sign-On

These are the five major types of single sign-on in common use at this time:

Enterprise Single Sign-On – Also known as legacy single sign-on, which is not Web-based, E-SSO occurs after the primary user authentication by intercepting login prompts presented by secondary applications and automatically entering the login ID or password. E-SSO systems interoperate with applications that are unable to externalize user authentication by “screen scraping” (see below).

Web Single Sign-On – Also known as Web access management, Web-SSO allows end-users to get to applications and resources that are accessed via a

Most IT managers and security personnel are aware of two types of SSO — Web-based and non-Web-based (or legacy) SSO — and variations that could only loosely be considered single sign-on.

Web browser. Authentication is achieved when user identification information is presented and stored in a cookie on the Web proxy server or a targeted Web server. The information in the cookie is retrieved each time the end-user attempts to enter a Web portal or new Web resource.

Kerberos (or Ticket/Token Authentication) – Named after the three-headed guard dog of Hades in Greek mythology, Kerberos was designed as a client-server model providing mutual authentication – both the end-user and the service verify each other's identity. End-users sign into the Kerberos server with their password and receive a ticket in exchange, which the client software presents to servers they attempt to access, authenticating them to different network services. A variant of Kerberos is used as the default authentication method for Windows 2000, Windows XP and Windows Server 2003.

Federation or Federated Identity – A new approach that is also for Web applications, Federated Identity uses standards-based protocols (SAML and WE-Security) to enable one application to affirm the identity of a user to another, thereby avoiding the need for redundant authentication. It allows organizations to provide multi-site SSO, account linking and other network and application services for the benefit of employees, customers and partners.

OpenID – A distributed and decentralized process, OpenID is a simple mechanism that ties the user's identity to an easily-processed URL, which can be verified by any server running the protocol. On OpenID-enabled sites, users don't need to create and manage a new account for every site before obtaining access. After authenticating with a trusted site that supports OpenID, the user's identity is confirmed to other OpenID-enabled sites. Because its philosophy is different from SSO, where authentication plays a big role, and since it does not rely on a trust mechanism, OpenID is not meant to be used in sensitive areas such as banking and online purchasing.

3.1.2 Noteworthy Types of SSO Solutions

The SSO Appliance

Surprisingly, single sign-on comes in many forms; it is generally available as a software product, however at least one hardware solution exists. We discovered an SSO appliance that addresses the management burdens of many SSO solutions by leveraging XML to auto-script the logon process. It uses intelligent automation via its Application Profile Generator, creating XML-based profiles for applications and storing these until they're ready to be downloaded by client-side software when users authenticate themselves at a workstation. Multiple passwords and application logon events are replaced with a single, centrally-managed user logon.

This SSO appliance also integrates with existing user security directories such as LDAP and Microsoft Active Directory, eliminating the duplication of security accounts that normally occurs with SSO-based solutions.

IBM ThinkPad Notebook Fingerprint Reader

Definitely the next generation in single sign-on is represented by the IBM ThinkPad Notebook R51/R52 series, which contain a built-in fingerprint reader to provide SSO to Windows, other applications and Websites. The setup is easy, then end-users can logon by just sliding their finger over a swipe sensor molded into the palm rest.

SSO with JAAS

To address the issue of dealing with the heterogeneous nature of most enter-

We discovered an SSO appliance that addresses the management burdens of many SSO solutions by leveraging XML to auto-script the logon process. It uses intelligent automation via its Application Profile Generator, creating XML-based profiles for applications and storing these until they're ready to be downloaded by client-side software when users authenticate themselves at a workstation.

prise systems (different technologies, operating on different platforms, accessing disparate data sources), the Java Authentication and Authorization Service (JAAS) combined with LDAP provides a solid framework for designing and implementing a robust SSO enterprise security framework.

JAAS uses login modules to facilitate the smooth integration of J2EE's security framework with various systems and their respective heterogeneous authentication mechanisms (OS, LDAP, database, etc.). These modules can be configured to share authentication data and designed to correctly identify users and roles by mapping principals and roles — even across domains with different security schemas.

Simply put, single sign-on is achieved across multiple security domains by mapping primary credentials gathered from the user to secondary credentials stored on the server and used to authenticate transparently against other enterprise systems.

3.1.3 Single Sign-On Variants

The following are methods for achieving single sign-on which are widely used but clearly are not secure. Use of some of these authentication methods can disastrously impact the security of an entire enterprise.

- Saving a password on the system by checking “Save to this Computer” when available in the application's authentication dialog box.
- Using session cookies. For example, when visiting Google mail, where a session is good for two weeks with the password you presently use.
- Using a “screen scraper” — a type of software that captures the window information for an application's authentication dialog box and stores the password in a database for when the dialog box opens in the future.
- Using third-party directories and data stores that offer SSO but are proprietary and have a proprietary hash. Third-party directories use a master password that allows access to other passwords, but they make it hard to leverage SSO for applications other than theirs. This is because they are a closed system — they own and manage the passwords for other systems and don't make them available for use somewhere else. There is no programmatic way to access these passwords.

3.1.4 Lotus Domino and Notes Single Sign-On

Single sign-on is offered as an optional component with the installation of Lotus Notes, but organizations wishing to install or uninstall it must run the Notes client setup to do so. Lotus' SSO for the Notes client starts when the end-user logs into Windows by storing the network password for later use. However, the Notes client only authenticates against the Notes ID — redirecting authentication to another password, such as a network or directory password, is not possible. The end-user isn't prompted to enter credentials when opening the Notes client.

Domino does not allow SSO from a Web browser, forcing end-users to remember what password to enter. Forgotten passwords then lead not only to increased Help Desk calls, but also to end-user frustration and loss of produc-

Single Sign-On is offered as an optional component with the installation of Lotus Notes, but organizations wishing to install or uninstall it must run the Notes client setup to do so.

tivity due to slowed Web server access.

What Domino does offer is its multi-server session authentication, which allows administrators to set up a listing of Domino servers in the same DNS domain to which end-users should have single sign-on. When an end-user logs on the first time to server A, they then have SSO to all the other servers in that listing. This involves browser session cookies, which terminate the session when the end-user closes the browser or the pre-configured timeout is reached.

Since Domino only allows authentication against the Notes ID, a forgotten Notes ID can create a nightmare for both IT and the end-user. The steps for recovering a Notes ID password are complicated, time-consuming and can only be executed by the Help Desk. The result is excess work for IT and a drain on IT resources, as well as a considerable amount of downtime for the end-user.

It is possible with Domino to authenticate against LDAP directories (e.g. Microsoft Active Directory and Sun ONE LDAP) from a browser client by using Directory Assistance (DA). Otherwise, end-users with accounts in both Domino and LDAP find that DA locates their Person document in names.nsf first and never goes to LDAP, eliminating the benefit of LDAP authentication.

PistolStar's Password Power provides single sign-on to companies with IBM Lotus technology enabling authentication with Windows, Microsoft Active Directory, Novell eDirectory and LDAP for accessing Lotus Notes clients and Domino servers.

3.1.5 How We Define Single Sign-On

To give you our definition of single sign-on, we start at the desktop with the Windows session. We leverage Microsoft Active Directory and Novell eDirectory — both significant technologies in Windows-centric computer environments — by enabling use of either of their passwords at the initial computer login to access the Notes client and all Domino server applications in multiple domains. With this capability, the number of times an end-user must supply log-on information during a Windows session is reduced to a single instance.

End-users can alternatively use their password for Windows, Novell eDirectory or Sun ONE LDAP to access Windows and Lotus applications. They may also leverage these passwords for performing password resets and recovery of the Notes ID. Using a central directory password to access servers and applications, including Notes clients, Domino HTTP, and Lotus Sametime and QuickPlace, enables single sign-on that is simple, robust and secure.

4.0 PistolStar's Password Power 8

4.1 Robust and True Single Sign-on

Password Power provides single sign-on to companies with IBM Lotus technology by enabling authentication with Windows, Microsoft Active Directory, Novell eDirectory and LDAP for accessing Lotus Notes clients and Domino servers. System access is simplified, as Lotus end-users typically have separate passwords for Windows NT, 2000 or XP, Lotus Notes (including the Notes ID file), Lotus Domino Web applications, Lotus Sametime and Lotus QuickPlace.

By allowing end-users to authenticate against Windows or a central directory, Password Power makes it possible to have only one password to remember or change, eliminating the downtime and lost productivity associated with maintaining multiple passwords. End-users enter their password only once — at the Windows login screen — and experience the convenience of smoother, faster logons.

With Password Power, end-users can also login or achieve single sign-on to Notes clients using their network password (Active Directory or Novell) or other LDAP passwords such as Sun ONE or Domino. If an end-user forgets their network password, answering the previously-created challenge question will give them immediate access to the Notes client. Because Password Power facilitates authentication with network logon credentials, password synchronization of the Notes ID is no longer required.

End-users who forget their Windows login password can also set a new one by correctly answering the challenge question. The Windows password reset capability is available from the Windows logon screen and supports domain accounts (Windows NT or Active Directory) and local accounts (Novell support is slated for end of 2005).

To provide secure single sign-on, Password Power utilizes cookies, creating them for each end-user at login or a network password change from Ctrl-Alt-Del. When the computer is shutdown or an end-user logs out of Windows, the SSO cookies are destroyed. By default, each cookie remains valid for 12 hours, however administrators can change this value to suit their organizational requirements. To secure workstations, Password Power relies on the operating system's functionality by setting the screen saver to automatic time-out or by locking the workstation.

Password Power reduces the number of times an end-user must logon during a Windows session to a single instance. As a result, end-users only need to remember and make changes to one password in one place.

4.2 Access to the Notes ID

Notes ID files are inaccessible and essentially useless if the end-user doesn't know or recall the password. Performing Lotus Notes ID password reset/recovery has always been a daunting and dreaded task for end-users and administrators, mainly because there is no concept of an "administrator" with Notes IDs who can simply reset the password on it.

With Password Power, end-users are relieved of having to deal with this limitation and the process of recovering the Notes ID password. Because Password Power allows end-users to self-service their Windows and Notes client passwords, they can use their Windows password to unlock the Notes ID password automatically.

4.3 Benefits to Lotus Organizations

Password Power reduces the number of times an end-user must logon during a Windows session to a single instance. As a result, end-users only need to remember and make changes to one password in one place. When a new password is implemented in Windows or Novell, the Internet passwords and, optionally, the Notes ID file password, are automatically updated.

Password Power also helps to maintain and enhance the security of corporate data. During the single sign-on authentication process, the password security policies (e.g., password expiration and password quality) implemented by the administrator through Windows are automatically transferred to the other passwords, ensuring the coordination of disparate password policies.

Both end-users and IT administrators benefit in several ways from Password Power. Since end-users will only need to remember one password instead of several, Password Power eliminates the frustration that results from the difficulty of remembering multiple passwords and greatly decreases the likelihood end-users will write down their password and become a target for internal network intruders.

Password Power also creates convenience for end-users by allowing them to perform their own password resets and requiring them to make changes to only one password in one place. By removing the need to engage IT to create a new password, Password Power also reduces end-users' downtime, allowing them to be more productive.

For IT administrators, Password Power dramatically reduces the number of Help Desk calls regarding password resets, enabling them to allocate fewer resources for managing passwords. Since Notes, Domino and network password security become one, it is also easier to respond to questions regarding Domino.

Most importantly, by enabling end-users and IT to diminish downtime and increase productivity, and by incorporating security "best practices," Password Power helps meet the corporate objectives of senior management. Ultimately, Password Power can positively impact an organization's bottom line.

5.0 Summary

The emergence of single sign-on technology has achieved a giant leap forward in usability, permitting end-users to ease the frustration of juggling several passwords and facing numerous password prompts. However, as the technology has evolved, several types of SSO and methods for achieving it have been introduced. In a sense, SSO has become a general term to describe any products that enable end-users to reduce logons and the number of passwords used. No universal definition exists and no criteria for what is true SSO have been established.

At the top of its performance, single sign-on drives efficiency and productivity for end-users and administrators, while it enhances security and ensures regulatory compliance — making the solution a clear winner. However, ideal single sign-on can be difficult to achieve because of the complexity of most enterprise systems, which include Web as well as legacy applications and are naturally heterogeneous. For some, single sign-on is really just "reduced sign-on."

Also, even though single sign-on achieves gains in security, it presents its own security concerns — with only one password in use for accessing several applications, a hacker can inflict a good deal of damage if they're able to seize upon that single password. Nonetheless, this factor is outweighed by SSO's increase in password quality, which can be most effective at thwarting the cleverest hacker.

Looking at the many types of single sign-on and ways it is enabled, there are clearly various possibilities for organizations to achieve it, however careful consideration should be made by organizations to acquire a solution that's right for their environment.

Companies with Lotus technology can achieve single sign-on through a solution that best addresses their particular password management issues. With PistolStar's Password Power, it is possible for end-users to authenticate against a central directory such as Microsoft Active Directory or Novell eDirectory to access all their applications on Domino servers across multiple domains. By also enabling self-service network password resets, Password Power allows use of the Windows password to recover forgotten Notes ID passwords.

At the top of its performance, single sign-on drives efficiency and productivity for end-users and administrators, while it enhances security and ensures regulatory compliance — making the solution a clear winner.

It is our conviction that with the flexibility to authenticate against standards-based directories, organizations can really reduce the number of passwords and achieve true single sign-on. Without it, resets will always need to be conducted on all the different accounts, and keeping password policies balanced and synchronization processes intact will remain major concerns.

By integrating third-party systems, Password Power has made strides in improving the password management experience for end-users and administrators in numerous organizations across diverse industries. For Lotus users, Password Power has allowed the promise of true single sign-on to become a reality.

6.0 Appendix A

System Requirements – Password Power 8

Password Power is a client-side solution with an optional server component that integrates seamlessly and doesn't require end-user setup. Password Power's server-side capabilities support Windows, Linux, Solaris, and IBM AIX 5.1. On the client side, Password Power supports Microsoft Windows NT, 2000, and XP.

7.0 Appendix B

Resources

"The Myths & Realities of Domino 6 Password Management," PistolStar White Paper, July 2004.

http://www.pistolstar.com/forms/responseforms/MRD_IP_LP.html

"The Evolution of Password Authentication and Management: Simplifying It Without Having a Complicated Solution," PistolStar White Paper, January 2005. http://www.pistolstar.com/forms/responseforms/EPAM_IP_LP.html

"The Role of Password Management in Achieving Compliance," PistolStar White Paper, May 2005.

http://www.pistolstar.com/forms/responseforms/RPMC_IP_LP.html

###

Password Power is a client-side solution with an optional server component that integrates seamlessly and doesn't require end-user setup.