



The Evolution of Password Authentication and Management: A Simple Solution

White Paper

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 Evolution of Password Authentication and Management: A Simple Solution

Table of Contents

Introduction	1.0
Authentication Past and Present	1.1
Purpose and Overview	1.2
Passwords – Entryways to Critical Applications	2.0
Passwords Serve A Vital Purpose	2.1
Yet, Passwords Have Their Issues	2.2
Password Management – A Critical Necessity	2.3
The Difference Between Mammoth Multiple Server-Based Systems and Client-Side Solutions	3.0
The Large Scale Identity Management System	3.1
The Client-Side Solution: A Different Yet Trouble-Free	3.2
PistolStar’s Web Set Password – A Client-Based Solution With the Performance of a Robust Identity/Password Management System	4.0
Simplifying the First Step to Password Management	4.1
Unique Capabilities of Web Set Password	4.2
Summary	5.0
Appendix A – System Requirements	6.0
Appendix B – 32 Ways to Better Secure Your Environment	7.0
Appendix C - Resources	8.0

The Evolution of Password Authentication and Management: A Simple Solution

1.0 Introduction

1.1 Authentication Past and Present

In 14th century England, entering a private or protected place might be possible through a pre-determined code of knocks on the door or a code word used by all attempting access. This code or “password” might be changed on occasion, but usually only after getting into the wrong hands. Authentication was also achieved by requiring entrants to produce a letter with the wax seal of their kingdom.

In the course of history, symbols, words, phrases, keys and secret codes have been assigned to individuals and groups to authenticate and gain access to castles, fortresses, hideaways, and private organizations. Fast-forward to the present, with the proliferation of computers and networks, and access is still primarily granted through the use of passwords. Although they’ve become unique to each individual using them for authentication, passwords can still be stolen or lost, making them less than secure.

Now that organizations possess multiple systems, servers and applications, requiring that end-users juggle numerous credentials for accessing crucial information, files and networks, password management has become the issue of the day. It’s easy to forget how essential passwords are for ensuring only authorized individuals gain access and protecting an organization’s digital assets. Nonetheless, password management is a critical necessity for simplifying and speeding admission across the enterprise, and diminishing end-user downtime and IT workloads as result of lost, stolen or forgotten passwords.

To the boon of organizations everywhere, numerous password management solutions abound. However, many are part of mammoth systems that require multiple servers and can create more issues than they resolve. An alternative now exists that is desktop-based, making it quick and easy to deploy. This client-side solution is a next-generation product that possesses the robust capabilities found in the large server-based systems, but also has the flexibility to be used in one of three different ways depending on an organization’s size and environment.

Future development of password management will reach technological depths and introduce organizations to more innovative authentication methods, including face recognition and other biometrics, and token-based solutions such as smart cards. However, many of these new solutions will still require hardware. The client-side system will maintain the technological edge because it doesn’t require additional hardware, an attribute that makes it inherently flexible, adaptable and user-friendly.

1.2 Purpose and Overview

This paper delves into the world of password authentication and management.

While passwords serve a very significant purpose, they have not been without their own set of issues and obstacles for organizations. Both end-users and administrators bear the brunt of managing numerous passwords; for end-users it’s the task of remembering them, and for administrators it’s dealing with password resets and the responsibility of ensuring passwords are secure. As a result, both parties experience a sizable loss in their productivity — end-users because of downtime waiting for administrators to reset or recover forgotten or lost passwords, administrators because of the time-intensive nature of addressing password issues.

Password management is a critical necessity for simplifying and speeding admission across the enterprise, and diminishing end-user downtime and IT workloads as a result of lost, stolen or forgotten passwords.

Another major headache for administrators with respect to the abundance of passwords being used in their organizations is the disparate policies of those passwords. Password quality and password expiration settings differ for various passwords, which can complicate password synchronization.

All of the above makes the rationale for password management more compelling. Because organizations maintain an unwavering vigilance of their bottom line, they need to reduce the time and resources IT administrators devote to password-related issues, protect important applications, files and data from hackers and intruders, and improve end-user and administrator productivity.

Obtaining the right password management system is another matter, however, as more than one type of system is available. There are the various large multi-server-based systems and there are client-side solutions. Organizations want to consider what's best for their environment, what will immediately meet their needs, and what will not present further issues for them.

The large-scale access and identity management systems provide several capabilities, from authentication to user self-service to password management. However, these systems require pre-planning, a 12 to 24 month time-frame to deploy, and purchase of extensive services.

With client-based systems, organizations acquire similar functionality, but without the time-intensive installation requirements or deployment issues. Client-based systems can be deployed in groups or by department, whereas server-side systems can only be deployed to everyone at one time, since the entire enterprise would be connected to that server. A client-based system also offers an organization greater flexibility, as it can be utilized as the main solution (particularly by small-to-medium businesses) or as a bridge or point solution for a larger system (particularly with large enterprises). A client-based solution can provide the significant functionality an organization needs as it performs a larger system deployment. A client-based solution can also offer an additional layer of functionality that may not be available in the larger system or is more robust.

There are also several options available with client-side systems that present advantages over server-side systems, such as selecting only the functionality that the organization's environment needs from the full menu of capabilities and controlling which passwords are used. Usability is several times that of large server-side systems, as end-users don't encounter anything they're not already accustomed to. There is no logging in or out and no need for retraining. End-users also don't need to access a new portal or Web page for logins or password changes, as is typically the case with server-based systems. Client-side solutions have the performance of a highly robust password management system. They rival the larger systems by offering several important capabilities, such as single directory authentication, self-service password resets and management, unified password policies, and synchronization of multiple passwords across the enterprise, among others. Client-side systems are also a fraction of the cost for a server-based system.

These are capabilities that greatly benefit both IT and end-users in numerous ways — from consuming significantly less Help Desk time to enabling end-users to manage their own passwords — and can have a major impact on productivity across the organization. By combining the benefits of these capabilities with the simplicity and ease of deploying and using a client-side password

Client-side solutions have the performance of a highly robust password management system.

authentication and management system, organizations can find themselves big winners in the race for secure yet simplified password authentication and management.

2.0 Passwords – Entryways to Critical Applications

2.1 Passwords Serve a Vital Purpose

From an historical standpoint, passwords have always served a valuable purpose. In the current age, where the progress of business is achieved via highly complex computer systems and high-speed networks, organizations need a way to provide its employees with access, yet they also need to ensure protection of their digital assets.

Therefore, passwords serve two functions:

1. Passwords provide access to servers, applications, the Web, intranets, extranets and across and beyond the enterprise. Every legacy system and every new application an organization installs requires a password to enter and use it.
2. Passwords enable organizations to secure specific data, files, etc. from unauthorized persons, internally as well as externally. In addition to helping organizations ensure that only authorized individuals gain access, passwords also allow organizations to limit access to specific areas to designated groups or individuals.

2.2 Yet, Passwords Have Their Issues

While passwords serve a crucial purpose, they are not without their issues. Because of the wealth of servers, systems, networks, and applications at their disposal, end-users are juggling multiple passwords. “What’s my password?” becomes a daily issue as there are so many passwords, but end-users can only remember a few of them at one time.

Taking the end-user’s perspective, imagine you’re working at your computer using and opening a number of different applications when you encounter another login screen. You can’t quite remember the password for that particular application, but you make an attempt to login anyway. Access is denied, so you wonder what to do. Should you call the Help Desk? Where is the Help Desk phone number? Is it after hours? As a consequence to the plethora of available software tools, applications, etc., for which they have passwords, end-users are straining IT personnel resources as they repeatedly call the Help Desk to reset passwords they’ve forgotten.

End-users are also choosing passwords that are easy to remember, while also easy to guess and therefore not secure. The key question regarding passwords then becomes: What characteristic in passwords can be affected to make them secure yet easy to remember?

Another dilemma occurring with respect to passwords is disparate password policies. It stands to reason that if there are numerous passwords, each assigned to different systems, the password quality and password expiration settings for each are likely to differ. This creates a problem when end-users are logging on and attempting to synchronize all their passwords to gain immediate access to the enterprise. Obviously, by complicating password synchronization, disparate password policies can slow and even prevent authentication and access from taking place.

2.3 Password Management – A Critical Necessity

Multiple systems. Multiple passwords. An increasing number of Help Desk

It stands to reason that if there are numerous passwords, each assigned to different systems, the password quality and password expiration settings for each are likely to differ.

calls for password resets. Clearly, the case for password management is undeniable. By implementing a robust password management system — particularly one that offers the capabilities that are truly needed, such as self-service password resets — organizations can provide end-users with a quick and easy way to authenticate and reduce the IT department's workload related to password issues.

Accordingly, both end-users and IT personnel will experience a dramatic increase in productivity, as end-user downtime is eliminated, IT time and resources are freed, and facilitation of the authentication process permits instantaneous access. Organizations will also increase and maintain corporate-wide security, as important applications and data will be protected from hackers and intruders.

Password management's ensuing rise in productivity and boost in security can have a direct bearing on overall business performance. Without a password management system, an organization can suffer from overwhelming IT costs due to wasted time and resources, and security lapses that result in stolen or compromised data. With the right password management system, all levels of an enterprise reap the benefits — from end-users to IT to senior management — and the entire organization comes out a winner.

With the right password management system, all levels of an enterprise reap the benefits — from end-user to IT to senior management — and the entire organization comes out a winner.

3.0 The Difference Between Mammoth Multiple Server-Based Systems and Client-Side Solutions

3.1 The Access/Identity Management System

Large-scale access and identity management systems provide a comprehensive set of capabilities, such as authentication and authorization, user administration, user self-service, single sign-on, and access control, as well as password management. Additionally, these systems may enhance security, enforce regulatory compliance, conduct security policy management, perform workflow, and enable provisioning.

Identity management systems are generally positioned and perceived as business solutions, as they can achieve enterprise-wide benefits such as improved information security, increased end-user productivity, reduced operational costs largely due to the near-elimination of Help Desk calls for password resets (the most frequent call for Help Desk support), and demonstrated compliance with industry and governmental regulations. Identity management systems also bear certain similarities to enterprise systems, most prominently with respect to deployment.

Large, server-based systems of any type generally require a hefty timeframe for pre-planning, installation and deployment, typically 12 to 24 months. Identity management systems, whether or not they can be installed in phases, are no exception, as numerous servers are involved, depending on the number of systems and applications in the organization for which there are passwords. The installation and deployment of an identity management system is a far-reaching event, making it inherently fraught with obstacles and challenges, and necessitating the purchase of extensive support services to ensure a smooth process before, during and beyond deployment.

While some providers of identity management solutions offer a suite of products that can be installed modularly, others provide all-encompassing sys-

tems. Depending on a particular organization's environment and end-user requirements, not all of the tools included may be necessary. Also, a smaller organization may find a large system cumbersome.

While a larger, server-based access/identity management system provides numerous business benefits, an organization needs to consider whether it's the right fit and serves their needs appropriately. It's imperative to note that server-side systems offering single sign-on are really only capable of Web single sign-on and not single sign-on to third-party systems. Most importantly, the necessary server changes and end-user retraining can add substantially to the overall cost of implementation, delaying a return on investment. Organizations both large and small have alternatives for attaining the password authentication and management capabilities they need in a less costly, cumbersome and time-consuming fashion.

3.2 The Client-Side Solution: A Different Yet Trouble-Free Experience

With a client-based solution, organizations obtain a high level of flexibility that's not possible with the server-based systems. Depending on size, end-user requirements, number of passwords used, and overall environment, organizations can use a client-based password authentication and management solution in one of several different ways:

1. As the main solution;
2. To add significant functionality during a large server-based system deployment that will integrate well with the larger system;
3. To add specific functionality that is more robust than what is offered in a larger system.

With a client-side solution, organizations obtain a high level of flexibility that is not possible with the server-based systems.

As the Main Solution

Any organization, but small-to-medium businesses (SMBs) in particular, can use a client-side system as the main solution. It is easier and faster to install and less unwieldy for IT administrators and end-users. Installation of a desktop solution is "silent" as the entire process occurs in the background. Microsoft SMS and similar solutions can streamline the process of deployment by enabling IT administrators to create a script of answers to the start-up questions that pop up on the desktops and email the script to all the end-users.

SMBs cannot afford the time, as larger companies and enterprises often can, to perform lengthy installation procedures, deployment, and retraining of staff. Therefore, a client-side solution is the most suitable option for them.

To Add Significant Functionality During a Large System Deployment

Since large-scale, server-based systems require a substantial time-frame for deployment, organizations planning to install one of these systems will often acquire a client-side solution because it offers significant password functionality in a package that is quick and easy to deploy and can integrate with the larger system. By purchasing a client-side solution - which can be rolled out in small phases and has a "silent" install - organizations experience a low investment threshold, obtaining immediate return on investment.

To Add Specific Functionality That is More Robust

Organizations already using one of the large global password man-

agement systems will often purchase a client-side solution because it offers another layer of functionality that is either not available or too cumbersome in the large system or it fulfills a critical need for precise and very robust functionality the large system doesn't offer. For example, as mentioned previously, server-side systems cannot enable "true" single sign-on, which includes third-party systems as well as the Web. The client-side solution provides single sign-on comprehensively while integrating easily with the large system.

There are several options available with client-side systems that present advantages over server-side systems. For starters, an organization can select specific functionality, depending on what it wants or needs, and control which passwords are used, creating a customized system. A full range of capabilities is available with a client-side system, including authentication, single sign-on, leveraging a single directory, user self-service/administration, and comprehensive password management — the same functionality offered by the large, server-based systems, delivering the same benefits.

A client-side system can also be tested or deployed to specific groups in phased rollouts. No retraining of end-users is necessary, as the system smoothly integrates with and compliments what they're already working with. Usability is high since the system's processes are very familiar and steps for various procedures remain the same. For example, end-users already know that pressing Ctrl – Alt – Del on their keyboard is the step to take for password changes.

A client-side solution also provides the benefit of password quality, password expiration, and challenge question-and-answer to remote users and others without a dedicated connection to a server.

Organizations installing a client-side system will also realize business benefits, such as enhanced security of data and applications, reduced Help Desk calls leading to a drop in operational costs, increased productivity, and regulatory compliance.

Clearly, a client-side solution offers a level of functionality that's in step with — and in some cases surpasses — what is offered by a system that is reliant on a proprietary server. Considering the greater ease, flexibility and lower cost with which an organization can install and deploy a client-side solution, it appears that client-side systems have a definite edge in terms of:

- technology,
- performance,
- speed,
- expediency, and
- usability.

4.0 PistolStar's Web Set Password™ – A Client-Based Solution With the Performance of a Robust Identity/Password Management System

4.1 Simplifying the First Step to Password Management

Simplifying authentication and facilitating access have become greater issues

A full range of capabilities is available with a client-side system, including authentication, single sign-on, leveraging a single directory, user self-service/administration, and comprehensive password management — the same functionality offered by the large server-based systems delivering the same benefits.

for companies as a result of all the passwords end-users are required to have for the multiple directories, software applications, servers, and platforms in their IT systems. Companies have witnessed significant losses in productivity, resources and time due to the increased need to perform password resets and recovery, and general password management. They've also seen their corporate security compromised by end-users employing non-secure tactics such as posting notes on their computer to remember their passwords or using passwords that are easy to guess. With the rise in outsourcing and off-site workers, companies have also realized a need for remote access and password management.

To respond to these issues, PistolStar introduces a revolutionary and dynamic product framework — **Web Set Password™** — that integrates the capabilities of its individual Password Plug-ins in one powerful solution. Developed for client-based operation, Web Set Password deploys easily and doesn't require a dedicated server or hardware.

4.2 Unique Capabilities of Web Set Password

Web Set Password offers this suite of capabilities:

- Single sign-on;
- Synchronization of multiple passwords across the enterprise using the Windows password;
- Authentication redirection to a single directory (Microsoft Active Directory, Sun ONE LDAP, and Novell eDirectory);
- Self-service password management;
- Self-service Windows password reset/recovery; and
- Unified password security policies.

Among the capabilities above are three that are very powerful for both the end-user and the IT administrator, and in terms of their far-reaching impact. They are:

- **Synchronization of Passwords from Multiple and Diverse Systems**
End-users can synchronize passwords — even from a browser — using their Windows or Novell password. Web Set Password synchronizes passwords for IBM System i, Microsoft Windows and Active Directory, SAP, Oracle, PeopleSoft, LDAP, Novell, and more.
- **Self-Service Windows Password Reset**
End-users forgetting their Windows login password can set a new one by correctly answering a challenge question set previously on their computer. Available from the Windows logon screen, this feature supports domain accounts (Windows or Active Directory and Novell) and local accounts.
- **Unified Password Security Policies**
Web Set Password maneuvers around the disparate password policies of individual systems by updating the individual policy attributes (e.g., password expiration and password quality) of all the passwords each time a password reset occurs. Web Set Password does this by querying the various systems each time it initiates the syncing process, in order to arrive at a global policy that encompasses all the passwords. This feature allows organizations to enhance the security of their corporate data.

Simplifying authentication and facilitating access have become greater issues for companies as a result of all the passwords end-users are required to have for the multiple directories, software applications, servers and platforms in their IT systems.

With Web Set Password, PistolStar has broadened its product focus to include passwords for numerous platforms, servers, directories and applications, as well as the Lotus Notes ID and Domino HTTP. Web Set Password allows end-users to unlock the Notes ID password automatically by using their Windows password.

To provide single sign-on, Web Set Password has a server-side authentication hook (plug-in) to interpret cookies. For Web single sign-on, cookies are created through the Web browser. The Web Set Password framework has been developed with two security pieces for storing end-user credentials: the cookie for Web applications and authentication, and Windows services. Therefore, with Web Set Password, end-users can access both local applications and Web-based applications.

Web Set Password further enables:

- Transitioning from multiple directory authentication (password synchronization) to single directory (authentication redirection), utilizing PistolStar's hybrid authentication capability;
- Communication and seamless operation between the Password Plug-ins; and
- Tight integration between the Plug-ins and operating systems and applications.

With Web Set Password, PistolStar has broadened its product focus to include passwords for numerous platforms, servers, directories and applications, as well as Lotus Notes ID and Domino HTTP.

To provide you with an idea of the types of configurations that can occur with Web Set Password, here are two typical scenarios as examples:

Scenario A: Microsoft Active Directory as network logon – Could include Notes ID password redirection to Active Directory and SAP single sign-on

Scenario B: Novell eDirectory as network logon – Could include System i password synchronization, Domino HTTP synchronization, and Domino HTTP single sign-on

Addressing the issue of non-secure passwords, Web Set Password applies specific attributes to passwords to make them more difficult for hackers and intruders to guess, but still easy enough for the end-user to remember. These attributes, such as making various letters either upper or lower case, or using numeric or special characters, make the password more unique.

Web Set Password demonstrates flexibility by allowing customers to only install the Password Plug-ins that are relevant to their environment, so purchasing the full suite of functionality is not necessary to achieving any of its benefits. Customers just select and purchase licenses for specific Plug-ins based on the directories they use and their password authentication needs. If a customer wants to include another password in their current configuration, another plug-in can be added easily, and without the need to install a new product version. When new plug-ins are introduced, they can also be installed with ease, as Web Set Password has a dynamic framework with automatic “self-discovery” of new plug-ins when they're installed.

Web Set Password delivers tremendous benefits to both IT administrators and end-users, such as a significant reduction in Help Desk calls and the use of IT time and resources to handle password-related issues. End-user downtime from waiting for password resets is also eliminated. In general, there is a siz-

able increase in productivity among both IT personnel and end-users, resulting in a positive impact on the organization's bottom line.

Overall, the benefits of Web Set Password include:

- Minimized IT security and administrative costs
- A rapid return due to the product's value
- Superior flexibility
- Sharply increased productivity
- Dramatically reduced Help Desk calls
- Nearly eliminated need for password management from administrators
- Ability to add functionality with ease
- Smooth integration with Microsoft Windows XP and 2000

5.0 Summary

Until more innovative authentication methods are widely employed, passwords — and more of them than any end-user can remember or handle — will remain a part of our reality in the information technology world. A system of password management that minimizes the downside of password authentication without compromising security is imperative, but selecting the *right* password management system for your organization is also critical. Different-sized systems exist, offering various types of functionality. Some systems are mammoth, multi-phase deployment systems that are dependent on hardware, while others are client-based systems that integrate with a Windows desktop. The evidence presented here clearly indicates that client-side systems have a distinct advantage, as they offer greater flexibility and unique capabilities at a much lower cost and require less time to install.

A system of password management that minimizes the downside of password authentication without compromising security is imperative, but selecting the right password management system for your organization is also critical.

But it bears repeating that selecting the right password management system is critical. Your organization's specific needs with respect to its size, environment, end-users and passwords used should be seriously considered. The right system should address all these needs and respond to the distinctiveness of your business. For example, many companies find they have separate IT departments handling the different systems/accounts within their organization, such as a Microsoft group, a Domino group, etc., each of which requires specialists in that system. By enabling your end-users to authenticate against a single directory and to synchronize passwords across the enterprise with the Windows password, PistolStar's Web Set Password promotes a more unified community among your IT staff and encourages the broadening of individual IT expertise.

Web Set Password was developed to serve as a business solution for senior management, but with the organization's IT staff and end-users firmly in mind. The root of all password-related issues —which impacts IT and end-users most directly — is the number and diversity of the passwords an organization requires to access its systems. By allowing end-users to have only one password to remember or change themselves in only one place, and enabling that without sacrificing security or placing a drain on the IT staff, is just one characteristic of being the right system. Availability as a client-side solution is another, as it permits rapid deployment, no reliance on servers, and tremendous flexibility.

PistolStar is pioneering password management by challenging traditional approaches. The company focuses on developing new capabilities that enhance IT's and end-users' experience, and revolutionizing how organizations install

and utilize password solutions. For the present and for the future of password authentication and management, PistolStar delivers the next generation.

6.0 Appendix A

Systems Requirements

Web Set Password is a client-side solution with an optional server component that integrates seamlessly and doesn't require end-user setup. On the client side, Web Set Password supports Microsoft Windows NT, 2000, and XP. Web Set Password's optional server-side capabilities support IBM System i, AIX 5.1 and higher, Linux, Sun Solaris, UltraSPARC, and Microsoft Windows Server 2003.

7.0 Appendix B

32 Ways to Secure Your Passwords

While some items on the list may seem obvious, we've tried to put together a comprehensive list of password security measures you can use to secure your network. If you know of a password security measure we've left out, please let us know: webmaster@pistolstar.com.

PistolStar is pioneering password management by challenging traditional approaches. The company focuses on developing new capabilities that enhance IT's and end-users' experience, and revolutionizing how organizations install and utilize password solutions.

Keep passwords secure by implementing password quality:

1. Use password length of at least 7 characters.
2. Use upper and lower case passwords.
3. Use mixed alpha and numeric passwords.
4. Use symbols in passwords.
5. Enforce password expiration - change password at regular intervals (every 30 days).
6. Do not reset a password with a previously used password or a previously used password with a number appended to it.
7. Set password history – set it high enough so that it makes it inconvenient for users to reuse their password by going through the password history rotation in one sitting.
8. Do not use company name or company name variations.
9. Do not use dictionary words or reverse dictionary words.
10. Do not use username or username variations.
11. Do not use personal data (e.g., birthdays, spouse's name, or license plate numbers).
12. Don't use passwords easily guessed by the personal items in your office (e.g., sports team posters or vacation spots).

Keep passwords secure by enforcing password encryption and transmission standards:

13. Encrypt all communication channels (e.g., SSL).
14. Store passwords in their encrypted form in the directory.
15. Use SHA-1 password encryption (developed by the National Institute of Standards and Technology (NIST) and by the National Security Agency (NSA), SHA-1 is the encryption standard the USA has adopted as the Federal Information Processing Standard).
16. Use 3-strikes functionality to lock-out additional attempts and prevent dictionary or "brute-force" attacks. Keep passwords secure by enabling end-user managed passwords:

17. Use encrypted challenge question/answer functionality –
 - a. Challenge question/answer functionality adds security because forgotten passwords are no longer communicated to the user from the help desk by phone or email.
 - b. Challenge questions and answers (stored in the user profile) should be encrypted or hashed in your database.
18. Prevent users from using Internet Explorer Auto Complete – a list of previously used entries lets anyone see the username.
19. Expire all passwords on first login – force users to change their password after it has been initially set for them by the administrator.
20. Send an automated email notification to the end user when a password has been reset successfully. This can alert the user that an intruder has gained unauthorized access. Include the message: Your password has changed. If this is not you, please notify security immediately.

Keep passwords secure by using Notes specific functionality:

21. Enable the isProtected property on the HTTP password field, upgrading the required access level from Author to Editor. Once this property is set on a field, a user must have Editor level access or higher to modify the field(s) in the Person Document.
22. Use salted or “more secure” passwords to create unique hashes for the same password.

Keep passwords secure by tracking user activity to detect intrusions in real-time:

23. Log password strikeouts to know when a logon or other failed authentication was attempted (e.g., setting a password, using or setting a challenge question/answer).
24. Log password strike events to know when a logon or password reset was successful.
25. Store last login date and time to know when an account was last used.
26. Store set password date and time to ensure that passwords are continually changed.
27. Log the use of invalid usernames and passwords on failed authentication attempts.

Keep passwords secure by communicating with your users:

28. Never write down a password (network intruders can be internal as well as external).
29. Never share your password with anyone, including coworkers and Help Desk personnel.
30. Don't be fooled by someone impersonating an administrator who asks for your password.
31. Select a password that is easy to remember, but hard to guess (make up an acronym to help remember your password).
32. Don't use passwords, use “passphrases”. These are not susceptible to dictionary attacks and are easier for users to remember (e.g., “I need a raise!”).

###

*PistolStar serves
Global 2000 companies
and organizations
across multiple vertical
industries including
automotive, chemicals,
consumer products,
finance/banking, gov-
ernment, healthcare,
manufacturing, adver-
tising and media, com-
munications, pharma-
ceuticals and retail.*