passlogix®

white paper

v-go®

# The Death of Passwords

3 Easy steps to increasing user productivity, enhancing authentication, and lowering password reset costs with Enterprise Single-Sign On.

# The Death of Passwords


## Executive Summary

For decades, IT security has depended on users having to remember a unique password for every enterprise application. And the result has been a nightmare.

On one end of the spectrum, users ease their burden of password management by choosing easily remembered “obvious” passwords like a variation on their name, birth date, or social security number.

Because of their obvious nature, these passwords are the easiest to hack, leading to security breaches.

On the other end of the spectrum are complex passwords. While hackers have a tougher time figuring these out, users often forget them. Strict password change and selection policies add to the user’s burden.

The result: frequent calls to the help desk for password resets, which industry analysts estimate cost $25 to $40 per call for IT support alone. That doesn’t include the lost productivity of the user waiting for the password to get back into the application he needs.

Computer industry gurus as influential as Bill Gates are now calling for the elimination of passwords. But what can replace them?

In this white paper, we examine a 3-step process for phasing out the need for users to remember the individual passwords for each of their applications while enhancing security.

## The Trouble with Passwords

"A major problem for identity systems is the weakness of passwords," says Bill Gates. "Unfortunately, with the type of critical information (protected by) these systems, we aren't going to be able to rely on passwords."

Concludes Gates: "There is no doubt that over time, people are going to rely less and less on passwords. In time, we will completely replace passwords." He says that Microsoft will issue smart cards to its employees for accessing both buildings and computers.

"I am officially calling for the death of passwords because they do not work," writes Brent Huston in Security.ITWorld.com. "Passwords simply do not adequately secure information. There are better solutions available and we need to start applying them to our security models."

Phil Young, head of IT at Amtrak, says, "Passwords are hard to manage, and due to the number of passwords people need to remember together with PIN numbers, it is becoming harder for the user."

So, what are the drawbacks to passwords?

- Too many passwords. Assume each user has a unique password for each application he uses. In an enterprise with 10,000 employees using two dozen applications each, that's 240,000 different passwords for IT to manage, creating enormous administrative complexity and burden.

- Weak passwords. Users choose easy-to-remember passwords, the simplicity and obvious nature of which provide a lower level of security. If users do not need to remember the passwords to all the different applications they use, complex application credentials can be used instead. A "complex application credential" is a password that is not obvious and is as long and varied as the logic of the application permits.

- Lazy users. Do you use your birthday, social security number, name, or some combination for any of your passwords? Most people do. Why? Because it's the first thing that comes to mind – and far easier than taking the time to think up a complex password. In addition, lazy users tend to pick the same password, or a close variation of it, for every application on their desktop. Unfortunately, computer hackers know this, and routinely breach security systems through passwords derived from easy-to-discover personal data.

- Reliance on human memory. There are two types of users: those who write down their passwords, and those who don't. The latter rely on memory for password recall, the performance of which declines in direct proportion to both the complexity and number of passwords. If each user in a company of 10,000 employees makes one password reset call to the IT help desk per month, and the cost is $25 per call, the annual password reset bill comes to $3 million a year.

- Easily obtained. As for those users who write down passwords, they naturally do it in easily remembered places: an index card in the top desk drawer, a sheet of paper taped to the cubicle wall, or a sticky note on the side of the PC monitor. Of course, it's a simple matter for unauthorized users to pirate these passwords for illicit network access. Hackers also call unsuspecting users, pretend to be from the computer support staff, and ask for the password. Or, the hacker calls the help desk, pretending to be a user who forgot his password.

- Easy to steal. Many desktops allow Windows to automatically fill in the password data. If the individual application passwords are stored on the desktop in unsecured cookies, then spy ware, worms, and other malicious codes can easily steal the passwords and other account information. A secure solution stores passwords in an encrypted file on the desktop.

- Easy to hack. Cyber-thieves have easy access to a wide range of "password crackers" -- software specifically designed to decipher passwords. Examples include John the Ripper, Brutus, and Russian Password Crackers.

- Phishing. The user is sent an e-mail asking him for his password, which he either e-mails back to the sender or types into what looks like a legitimate site. In reality, the e-mail is a scam, the purpose of which is to steal the password.

- Unique identification not required. The idea of computer security is for each user to have a unique identifier, but no password or PIN really meets that requirement: anyone, not just the user, who possesses that password or PIN can get into the system. By comparison, a biometric system is uniquely keyed to the physiology of each individual user (see Table II on page X).

- Limited protection. Once the password is purloined, the system is breached. There is nothing stopping an unauthorized user who manages to get a hold of – or figures out – any user's password.

- Force of habit. Training users to pick better passwords and store them more privately and wisely simply does not work. Busy users always pick the path of least resistance, which is to either pick an easy password or to post passwords in plain sight.

Every IT professional has heard stories about password frustration, like the bond trader who supposedly threw his PC through a window because he lost his password, couldn't access the system before the closing bell, and lost his company millions.

One real life example: a disgruntled former employee of Omega Engineering used a stolen password to infect the company's network with malicious code. It erased software under contract with NASA and the U.S. military, costing the company nearly $10 million in losses.

More recently, a hacker used an authorized user's ID and password to access personal data – including birth dates and social security numbers -- on more than 33,000 U.S. Air force officers.

Every user has personally experienced password frustration: the inability to remember a password for an important application when you need it, and the difficulty and delay in getting the password reset by the IT help desk.

## The "Holy Grail": Enterprise Single Sign-on

The solution to the password problem is not to eliminate passwords, but rather, to eliminate the need for users to remember passwords.

This technology, known as enterprise single sign-on (ESSO), enables users to sign onto the network once with a single password.

Once signed in, those users can access all their applications -- without remembering or entering the individual passwords for those applications.

ESSO is the "holy grail" of passwords, and some IT professionals believe it to be unattainable. Reason: first generation, server-based ESSO solutions were, in fact, too costly and labor-intensive to implement throughout large enterprises.

The user had to access an SSO server to be authenticated, and the server would then submit the authentication to the application. This meant that IT had to write connectors for each application to replace the native authentication, which was uneconomical if not outright unfeasible.

In practice, this meant that, at best, “single sign-on” became a “somewhat reduced sign-on.” Requiring IT to write connectors for each enterprise application incurred a considerable extra cost element in ESSO implementation. Writing connectors also takes time and delays delivery of the ESSO solution.

This added cost of writing connectors ranges from $15,000 to $40,000 per application. Multiply that by hundreds of thousands of enterprise applications, and these first-generation, server-based ESSO products quickly became cost-prohibitive.

As a result, ESSO hardly ever made it beyond the evaluation or pilot stage. And if it did, it got stuck during deployment.

Not surprisingly, first-generation ESSO solutions did not meet market acceptance. These inadequate systems gave ESSO a bad name, leading many to consider ESSO nothing more than a pipe dream.

## Other Password-Related Security Solutions

In addition to ineffective first-generation ESSO systems, several other solutions have been proposed for enhancing password security and reducing password reset costs – and each has flaws limiting its effectiveness.

Weaknesses of non-ESSO password security solutions include:

- Failure to work with all applications and platforms, especially legacy and “home grown” systems.
- Failure to work with a growing number of externally hosted applications such as ASP, extranet, and Internet.
- Costly system integration schemes requiring extensive scripting, customization, and problematic maintenance requirements.

- Failure to support all works modes including disconnected kiosks and terminal services.
- Failure to leverage existing infrastructure, requiring a new and costly independent infrastructure.

### *Web SSO*

Single sign-on (SSO) systems for Web applications enable a partial solution by limiting the number of passwords.

With more and more applications being accessed as Web services on extranets and company portals, Web-based SSO is an important security measure. Web SSO grants access entitlements to controlled Web resources based on the user's role or group.

However, Web-based SSO does not cover password sign-on for non-Web-based desktop applications. So the user still needs passwords for all those applications.

### *Password Synchronization*

Some enterprises have opted for password synchronization, in which all applications share the same password.

The greatest flaw of synchronization is that the password to which the applications are synchronized must be set at the weakest capability among all of the supported applications. Therefore, all supported applications are susceptible to security breach based on exploiting this weak password.

Synchronization also requires integration for each application. Users need to know and remember the application passwords, and have to handle and enter them.

The bottom line is that both Web SSO and password synchronization deliver limited solutions for a subset of enterprise applications – and not a true single sign-on for all enterprise applications.

### *Self-Service Password Reset*

Many enterprises are deploying self-service password reset (SSPR) as a portal service. But SSPR is only a partial solution: the user still needs to remember his passwords – or reset them each time he uses the application. Also, the passwords

SSPR users choose when they reset their passwords are often easily remembered – compromising IT security.

## ESSO: the Next Generation

The new generation of ESSO solutions eliminates the problems associated with both previous ESSO generations as well as with password synchronization, Web SSO, self-service password reset, and other authentication systems.

Typically, an end user will have separate accounts for a number of applications. Each application requires the user to enter an ID and password. Access is granted only if the correct ID and password are entered.

With the new generation of ESSO, the user only has to log into the network session with a single password. Once he is logged into Windows, whatever application he goes to gets the correct ID and password transparently and automatically from the ESSO solution – eliminating the need for the user to remember and enter all the IDs and passwords for his applications.

When an application presents a dialog box asking for an ID and password, the ESSO solution intelligently recognizes the request and searches an encrypted data file for a corresponding set of credentials.

If these credentials are present, the ESSO solution decrypts them on-the-fly and submits them to the application. The user can sign on to any application – Windows, mainframe, telnet, Java, home-grown, or Web-enabled – without the need for touching the application through the integration of server-side connectors or agents.

## A Standard Platform for ESSO

In the past, authentication and provisioning solutions were stand-alone, with limited interoperability between them.

What was needed was an industry-standard sign-on platform upon which an enterprise can build a full suite of single sign-on solutions addressing all of their password-related authentication requirements.

Why is having a standard sign-on platform so desirable?

* From one central point of control, network administrators can provision and manage passwords across the enterprise. Extended event logging and reporting capabilities enable administrators to uniquely identify all applications configured for an end user as well as the usage details for each user on each application.
* A sign-on platform provides out-of-the-box functionality and open interfaces. It leverages the common look and feel of application logon requests on the client, regardless of the back-end operating systems, databases, or hardware platforms.

* The enterprise is freed from the limitations of the "authentication silos" built into various enterprise applications. The platform can accept any form of user authentication, deliver single sign-on to any application, and leverage any application infrastructure, in any user work mode, with a full audit trail.

* The platform intelligently recognizes and responds to application logon requests as they present themselves to users. By eliminating scripts, connectors, and wrappers, the platform can work regardless of the various application versions that may be deployed or the network or application latency, delivering quick time to value.

## 3 Easy Steps to Eliminating Passwords in Your Enterprise

Another reason for the delay in widespread implementation of ESSO is IT's lack of knowledge and experience in ESSO implementation. But enterprise ESSO can be implemented in a matter of months using a phased 3-step approach outlined below:

1. Implement ESSO and move to a single strong network password and complex application credentials.

2. Implement a provisioning system to provide an automated means of distributing complex application credentials.

3. Add strong authentication to the single password the user must remember to log into the network.

In this process, you start with ESSO to get down to one manageable password per user to access the network. Then you implement provisioning to eliminate all user

knowledge of individual passwords for each application. Finally, you add strong authentication to eliminate user knowledge of the Windows or other corporate directory password.

This process has been tested and refined installing the v-GO Sign-On Platform at millions of seats worldwide. Let's look at each step in a little more detail.

***Step 1: Implement ESSO and move to a single strong password and complex application credentials.***

When you implement v-GO SSO, your users no longer need to remember the individual passwords that protect the applications they use.

Freed from reliance on human memory, passwords can be made complex – as complex as the logic of the individual application permits.

When creating complex application credentials, you should choose passwords with at least 8 characters, at least one number, and at least one special character. Mix upper and lower case letters whenever the application's logic allows it.

Application credentials can be as complex and changed as frequently as the application permits. V-GO SSO generates complex credentials for all applications randomly and automatically.

These randomly generated user IDs and passwords provide a much higher level of security, because they are nearly impossible for unauthorized users to discover. Routinely changing passwords and implementing two-factor authentication can further strengthen security.

Passwords with difficult combinations make it more difficult for password crackers to decipher your password.

With a different complex credential for each user -- and each application he or she uses -- you gain a huge improvement in the overall level of IT security. Applications are more difficult to breach, and data is more securely locked down.

Table I outlines Microsoft's character count recommendations for complex application credentials. With ESSO, all applications can be moved to complex application credentials.

Table I. Complex application credentials.

| Password length (characters) | | Average time to crack | Usage |
|---|---|---|---|
| 1 - 7 | Low | Short | Not recommended |
| 8 - 9 | | Long | Network logons in organizations with low risk profiles |
| 10 - 11 | High | | Network logons, external application logons, virtual private networking |
| 12 - 23 | Very High | | Network logons for high-security environments, VPNs, service accounts. |
| 24 or more | | | One-time cryptographic key exchanges, highly valuable accounts |

***Step 2. Implement a provisioning system to provide an automated means of distributing complex application credentials.***

An enterprise identity provisioning system enables IT, not users, to set passwords for individual applications.

ESSO eliminates open handling, distribution, and knowledge of application passwords – giving you a means to move to complex application credentials that are too difficult for a user to remember, let alone enter accurately.

The v-GO Platform's integrated support for leading provisioning systems provides an automated means to distribute complex application credentials from the provisioning system to the ESSO system. With single sign-on and provisioning, users need never know or touch an application password again.

This eliminates end-user enrollment and delivers "day one" sign-on. When an employee leaves or is terminated, his access to all applications can be terminated that same day.

Passlogix's v-GO Provisioning Manager (PM) allows system administrators to directly distribute user credentials, usernames, and passwords to a users's individual v-GO Single Sign-On (SSO) credential store.

The user automatically gains access to the account without having to manually track down the ID or password from e-mail or voice mail and type it into v-GO SSO. The administrator

can add credentials for new applications and new users, as well as modify or delete old credentials.

When provisioning a new user on a network, the administrator can place the user's credentials directly into the v-GO SSO system, so the user never knows or touches them.

***Step 3. Add a second factor for advanced authentication.***

Many companies today want to move from simple authentication, which uses only a password, to advanced or "strong" authentication.

There are three forms of authentication: something you know, something you have, and something you are (see Table II). Advanced authentication typically requires two forms of authentication.

One is usually a password – something you know. The second form of authentication is an "authenticator."

An authenticator is a mechanism used to authenticate someone. Examples include passwords, tokens, smart cards, biometrics, dongles, and other devices (see Table I). Many biometric systems operate with the fingerprint or retinal scan alone, without the password as a second authentication factor.

Table II. Advanced authentication factors.

| Authentication factor | Description | Examples |
|---|---|---|
| Something you know | Secret information known only to the user | Passwords, PINs |
| Something you have | A physical device possessed only by the user | Token, smart card |
| Something you are | A unique, measurable characteristic of the user | Voice print verification, fingerprint, retinal scan, or other biometrics |

Result: you can implement advanced authentication without locking yourself into specific authenticator vendors or technologies. The software integrates seamlessly, providing granular control over the level of authentication required to access specific applications.

## Result: the Death of Passwords

After completing the 3-step process outlined in this white paper, your enterprise will have the following password and authentication measures in place:

- Single sign-on – enabling users to sign onto the network once per session with their Windows password, and then access all their applications without the need to remember or use any other passwords, because the passwords are served to the applications automatically by the v-GO SSO system.

- Provisioning – IT administrators can quickly and easily provision passwords to users throughout the enterprise remotely, without e-mail, voice mail, or pieces of paper.

- Advanced authentication – two forms of authentication – the PIN and a token, smart card, or other authentication device carried by the user -- are required to access the network, greatly enhancing computer security.

The easiest way to measure the ROI of freeing the user to touch application passwords is through reduction in password reset calls to the help desk.

Based on a decade of experience in passwords, we estimate that as many as 40% of help desk calls may be password related.

At the world's largest enterprise, the United States Postal Service, implementing v-GO SSO reduced password reset costs and saved the organizations millions of dollars a year.

## Benefits of ESSO Implementation

Implementing ESSO with the 3-step process outlined in this white paper offers a number of benefits to the enterprise:

- Users gain quick and easy access – from any location – to maximize productivity.
- Eliminates lost or forgotten passwords – users have just one password to remember.
- Lowers user support costs – by virtually eliminating password-related support calls.
- Securely stores and manages all passwords – no more searching for lost passwords.
- Improves network security – prevents unauthorized users from accessing enterprise applications.
- Aids in regulatory compliance – including Sarbanes-Oxley, HIPAA, homeland security, and other regulations requiring data to be kept private, confidential, and secure.
- Simplifies administration – you can control password policies from a single console.
- Reduces programming costs – works with your applications right out of the box – eliminates the need to write custom scripts for connectors.
- Scales to any enterprise – accommodates up to 100,000 seats or more – and integrates with your other identity management solutions.
- Quick time to value – most organizations experience payback in less than 6 months, and triple-digit ROI after 3 years.

## Blended Authentication Strategies

Not all situations require complex application credentials that are unique and frequently changed. In low-risk situations, a simple, user-selected password can provide the appropriate level of safeguard; in others, not.

IT professionals can choose today from a variety of safeguarding strategies including ESSO, Web SSO, federated identity, leveraging the Windows log-in or the Kerberos network authentication protocol, and LDAP log-ins.

What about legacy applications whose embedded authentication processes and password systems are extremely difficult to change? Kerberos is not on all commercial applications, and it would be impossible to Kerberos-enable all applications within your organization. Therefore it is part of a limited solution.

One factor to consider is how you can protect both desktop and online applications. Typically, two separate solutions must be installed. An ESSO safeguards applications running on the desktop. A Web SSO gives users seamless access to their online services, applications, and accounts.

Do you have business partners, agents, suppliers, and vendors who need to access your application and databases from their companies? In that case, a Web SSO must be part of your blended authentication strategy.

Another factor to consider in a blended authentication strategy is whether you need to maintain passwords for non-enterprise applications (e.g., eBay or Hot Mail). If so, you can leverage the flexibility of ESSO. If not, make it the user's responsibility to remember these passwords.

Also, does your authentication system need to leverage the federation solution? Some industries, especially those concerned with homeland security issues – such as oil and gas, which is considered a vital part of the U.S. infrastructure – are proactively pursuing federation solution standards. Can you share resources and knowledge with other companies in your industry whose federated solution implementation is further along than yours?

Passlogix's v-GO Authentication Manager (AM) allows organizations to use any combination of tokens, smart cards, biometrics, and passwords to control access to their applications.

## Conclusions

Eliminating passwords is no longer a "pipe dream." It is an attainable reality – one that you can implement in your enterprise this year.

ESSO is no longer the unattainable "holy grail." The Passlogix v-GO Sign-On Platform has emerged as the first industry standard sign-on platform with a full suite of integrated solutions for single sign-on, authentication management, and provisioning.

With v-GO's automated password generation and provisioning capabilities, passwords can be longer and more complex, with a unique password for each application. Passwords can be changed more frequently, further bolstering IT security.

###

For more information on how you can eliminate the need for users to remember passwords to their enterprise applications, contact Passlogix today:

Passlogix, Inc.
160 Pearl Street, #400
New York, NY 10005
Phone 212-825-9100
1 (866) PASSLOGIX Toll free
1 (866) 727-7564
Fax 212-825-0326
www.passlogix.com

v-go®

passlogix®

white paper

160 Pearl Street, 4th floor, New York, NY 10005
Tel: 212.825.9100 x 2
or 866.727.7564 x 2
Fax: 212.825.0326
Web: www.passlogix.com
Email: sales@passlogix.com

Copyright. © 2005 Passlogix, Inc. All rights reserved. All trademarks and names referenced herein are the property of their respective owners. FSSSO-070805