



# The Case for Enterprise Single Sign-On:

What Every Security Executive Needs to Know

By Kenneth Tyminski



WHITE PAPER

# The Missing Link in Password Management

Every information security executive is familiar with the problems of password fatigue, password inflation, and the associated burdens on end users as well as network administrators. The irony is that so many companies fail to implement the most effective antidote: enterprise single sign-on (ESSO).

Most organizations have adopted other best practices for password management, from password composition rules and password update policies to authentication of users who request a password reset. Procedures like these can go a long way toward thwarting hackers by strengthening and protecting the passwords themselves.

But many IT managers have not taken steps to combat the broader problem of password overload — that is, the user frustration, productivity losses, security risks and administrative overhead stemming from the need for users to remember different passwords for applications they require to do their jobs.

To adequately address these issues, organizations need a solution that can (1) reduce the number of application passwords that users must remember, (2) automate the process of password entry, and (3) store every user ID and password for every application in a very secure central repository for easier management and recoverability.

Enterprise single sign-on meets these needs better than any other technology on the market. It has been proven for over a decade in many of the world's most respected organizations, from major banks, hospitals and businesses to the U.S. Postal Service.

What follows is a brief overview of the business justification for ESSO deployments, the misconceptions that have discouraged security managers from adopting the technology, and how to determine whether your organization is an ESSO candidate.

## Top 5 Reasons to Adopt ESSO

Imagine if you needed a different key for every door in your house. Either you would have to memorize the exact grooving pattern of every key and mentally match it to the proper door, or you would have to fumble to find the right key every time you needed to open a lock.

End users face the same kind of aggravation when they need different passwords for their various business applications, databases and Web accounts. At the most basic level, then, enterprise single sign-on technology offers a cure for that distress by absolving users of all password responsibilities except for the initial logon.

That enhanced user satisfaction is a valuable and even critical benefit of ESSO, but it is frequently difficult for security executives to justify the investment on that basis alone.

If you analyze the effects of simplifying the user logon experience on areas such as productivity, IT support, password-related security and corporate governance, however, the business case for single sign-on is clear. From this perspective, the five most compelling business drivers are that ESSO:

## 1 – Saves hours of user time wasted on password-related activities .

One study by the Burton Group estimated that the average user in certain environments spends 15 minutes a day in application logons. That would add up to 65 weekday hours wasted in entering user IDs and passwords every year.

Another study by the Network Applications Consortium reported that the typical user spends up to 44 hours annually logging on to just four applications. With other surveys showing that 36% of users have six to 15 passwords and another 18% have more than 15, you're talking about weeks of work going down the drain.

The Case for Enterprise Single Sign-On

ESSO can reclaim those hours as well as time squandered in password changes, password resets, searches for lost passwords, and application lockouts caused by expired, forgotten or out-of-synch passwords.

## 2 – Reduces help desk costs associated with password support.

Various Gartner studies have estimated that 25% to 35% of calls made to help desks are related to password resets. For some organizations, the number is much higher. At analysts' estimates of \$25 to \$40 per call and four password reset calls per user per year, this can add up to hundreds of thousands or even millions of dollars on an annual basis.

Even if your cost per call is much lower or you have implemented automated reset functions, the cost of supporting passwords at the help desk can still be substantial.

By reducing the number of passwords that users have to manage to a single network logon, ESSO can slash the number of password-related calls received every year along with associated costs.

Recently, for example, a company with 78 offices around the world reported an expected savings of \$600,000 in access-related help desk calls after implementing ESSO as part of a global identity management system.

## 3 – Increases security by enforcing strong password standards.

As every security administrator knows, it is easier to develop a strong password policy than to enforce it. Users who must manage large numbers of passwords either ignore the rules by adopting easy-to-remember formulas or keep a written record of their complex passwords as a memory aid. The simple passwords are easy to hack, and the password lists are easy to steal. Either way, security is compromised.

In an enterprise single sign-on environment, these issues and security risks disappear — and password quality rules can be easily enforced — because users no longer have responsibility for carrying out password protection schemes. Consider:

- No user involvement. Unique, complex alpha/numeric passwords of any length, case or format can be created and used for every application, database or account logon because there is no need for users to remember and input them. The ESSO system responds to each logon prompt without user intervention.
- Automatic updates. The ESSO program automatically generates new passwords when the old ones expire, ensuring

that passwords change at prescribed intervals as well as adhere to whatever policies the administrator specifies during system setup.

- Harder to hack. The random passwords generated by the ESSO system are far more secure than user-created versions that rely on familiar words or patterns. These computer-generated passwords cannot be easily cracked by any technology available today.
- No written lists. Each password is securely stored and encrypted in the ESSO database as well as unknown to the employee once the initial set of user-selected passwords has expired, so there is no user-maintained record that can be pilfered.
- Safer network logon. Since users are required to remember only a single network password to log onto the network, they are more likely to create a strong password for that one purpose. Memorizing one complex pass phrase is doable; memorizing many is not. In this way, ESSO becomes a core part of the information security framework and a vital adjunct to the overall security infrastructure.

#### **4 – Centralizes password storage for easier management & recovery.**

ESSO also yields substantial IT time savings in password management and recovery by consolidating all user IDs and passwords into a central repository.

If a user's system crashes, an application password needs to be reset, an application is locked, or a departed employee's accounts need to be accessed, IT personnel have a central record as well as a central backup of all user credentials to expedite problem resolution. Each application still maintains its own database of user IDs and passwords, but the laborious process of retrieving each set of credentials individually is no longer necessary.

This also relieves line managers of password crisis duties for department-specific applications or accounts for which they may be responsible.

Without ESSO technology, there is no practical way to create a single view of user names, IDs and passwords across all information assets in an enterprise. Active Directory, for example, cannot accommodate credentials for mainframe, legacy, Web or certain specialized applications without significant effort to ADenable them.

Yet that single view is as essential to efficient password management as seeing every PC on your network is to hardware maintenance and other IT duties. ESSO is simply the shortest distance to building that central repository.

#### **5 – Aids compliance with federal data protection mandates.**

Another fringe benefit of an ESSO deployment is that it helps establish the data protections and related audit trails mandated by regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley (SOX).

In the case of HIPAA, for example, an ESSO system delivers the unique user identification method, password management capabilities and automatic termination of inactive sessions required under the legislation's security rules.

In the case of Sarbanes-Oxley, ESSO's ability to ensure enforcement of strong password policies and provide comprehensive user logon and application access reporting helps companies show that they have imposed the controls required to preserve the integrity of their financial applications.

For some organizations, this is the magic bullet that secures the funding required for an ESSO implementation. While support for regulatory compliance initiatives is not the primary function of ESSO technology, it is therefore playing an increasingly important role in driving ESSO adoptions and enabling enterprises to achieve all of ESSO's other benefits.

## Debunking ESSO Myths

Despite these solid business drivers and successful implementations by world-class organizations, many security executives still hesitate to undertake ESSO initiatives because of lingering misconceptions about the technology.

A detailed examination of these fallacies goes beyond the purview of this discussion, but there are three points that will be briefly addressed here to lay the major concerns to rest. Specifically:

### 1 – ESSO does NOT offer hackers the 'keys to the kingdom.'

While it is true that a single network logon password unlocks the ESSO system to enable automated entry of individual application passwords, the barriers to hacking the logon password and then gaining access to the user's applications are formidable.

First, as discussed earlier, users who need to remember only one Windows password are far more likely to adhere to strong password policies that block dictionary attacks and increase the difficulty of cracking the code exponentially. Increasing password length by just one character can add years to the decoding effort.

Second, after cracking the network logon password, the hacker would need access to a workstation with the ESSO software (or the software itself plus the ability to configure it with the organization's directory) to open the door to each application.

Organizations concerned about these highly unlikely scenarios can add an additional layer of protection by asking for an additional pass phrase (such as the mother's maiden name) or adding strong authentication such as smartcards, tokens, proximity badges or biometrics to the mix.

But think about this: in years of ESSO deployments, there have been no reports of "keys to the kingdom" attacks. The risk is more theoretical than real.

## 2 – ESSO is NOT difficult to deploy.

The idea that an ESSO implementation is a never-ending project came from first-generation solutions that required custom-written connectors to replace the native authentication of each application. Modern ESSO systems have eliminated that requirement. As a result, deployments can begin quickly if you narrow the focus to the applications that are the major contributors to password headaches.

Start with a small group of users and a subset of the applications they use, for example, and then extend that small list of programs to a broader user population before bringing additional applications into the ESSO fold.

One way to decide which applications to target in the first phase is to ask the help desk which programs are causing the preponderance of calls for password resets. You will probably find that a few applications are causing 80% of the problems.

In addition to swiftly reaping the benefits of ESSO, one virtue of this approach is that it's easier to do a mid-course direction with 100 users using single sign-on with five applications than with thousands of users navigating scores of accounts. You don't have to manage every user ID and password out of the gate.

## 3 – ESSO's benefits are NOT difficult to justify.

The savings in help desk costs have been well-documented and are the easiest aspect of ESSO deployments to quantify, but the return on investment goes well beyond a reduction in support expenses.

Gains in user convenience and productivity, network security and tools for regulatory compliance capabilities may be difficult to measure, but so are the benefits of upgrading from Windows XP to Windows Vista or deploying a new Customer Relationship Management system.

The bottom line is simple: the number of application passwords that must be managed in many enterprises today is untenable, undesirable and unsafe. ESSO provides a proven solution that removes the burden from end users and administrators alike, and simultaneously hardens the network against attack through strengthened password policies.

In addition, ESSO can both complement and facilitate strong authentication and identity provisioning initiatives by extending single sign-on to smart cards or other authenticators as well as helping to guide provisioning efforts.

It is difficult to imagine a stronger set of arguments in favor of ESSO technology.

## Are You an ESSO Candidate?

To determine whether your organization should investigate an enterprise single sign-on implementation, answer these questions:

- 1 – Does your average user have six or more passwords to remember?
- 2 – Are you having difficulty enforcing strong password policies?
- 3 – Are at least 15% of your help desk calls for password reset?
- 4 – Are you facing HIPAA, GLBA, Sarbanes-Oxley or similar audits?
- 5 – Are you spending too much time issuing, updating and deleting passwords?
- 6 – Are you deploying strong authentication or identity provisioning?
- 7 – Do you have shared workstations that require individual logons?

If you answered yes to these questions, you should consider adding ESSO technology to your security framework. Passwords should be managed as proactively as any other component of the IT environment. ESSO provides the tools to get you there.

For more information on Enterprise Single Sign-On, contact Passlogix today.

### About the Author

Kenneth Tyminski is a long-time technology executive and retired chief information security officer (CISO) for one of the country's largest financial services companies.

# passlogix®

V-go®

WHITE PAPER

75 Broad Street, Suite 815, New York, NY 10004

Tel: 212.825.9100 x 2

Or : 866.727.7564 x 2

Fax:212.825.0326

Web: [www.passlogix.com](http://www.passlogix.com)

E-mail: [sales@passlogix.com](mailto:sales@passlogix.com)