Implementing Enterprise Single Sign-On in an Identity Management System
Introduction

Most users need a unique password for every enterprise application, causing an exponential growth rate in passwords. Unfortunately, most applications provide no easy way—or no way at all—to centrally control user passwords. As a result, users create passwords that are often easy-to-guess derivatives of names, Social Security numbers, and birthdays. These "obvious" passwords make it easy for unauthorized users to gain access to enterprise applications and data. Moreover, authorized users frequently lose or forget their passwords, creating a significant password management burden on IT support.

Concerns about ineffective password systems and lax password security have led to many regulations calling for improved password security, for example, in the U.S., the Sarbanes-Oxley Act (SOX) and the Health Insurance Portability and Accountability Act (HIPAA), and in the U.K., the Data Protection Act.

By implementing enterprise single sign-on (ESSO), network administrators can set, assign, securely store, and change passwords from a single point of control. Benefits to the enterprise include

- Simplified administration
- Reduced support costs
- Improved enterprise security
- Greater user productivity
- Ability to achieve compliance with HIPAA, SOX, and other regulations
Understanding the Problem

A typical enterprise has hundreds or thousands of users. To do their job, each user runs half a dozen or more applications on a desktop. Virtually all these applications should, if they are securely administered, have different requirements for what constitutes a valid password, such as number and combination of alphanumeric characters.

Private individuals as well as corporate employees use most, if not all, of these applications. In addition, departments and workgroups might each have their own subset of applications, increasing the difficulty of administering identity management (IdM) and security policies throughout the enterprise. Yet, the password protection schemes of popular applications were clearly not designed with the overall infrastructure management needs of the enterprise in mind:

- There is no central repository for password storage. End users store their passwords casually, with little regard for security.
- Although some Web applications store and “remember” the password for the user, passwords can be lost when users upgrade their desktops. Or if users have a PC problem, such as a hard disk crash, then the stored password could be deleted.
- Each application requires its own password. Therefore, an employee who uses six different applications might have six unique passwords. If the enterprise has a thousand employees, then the result is 6,000 unique passwords to manage. To eliminate the need to look up passwords each time they want to use one of their applications, users deliberately select easy-to-remember passwords. Unfortunately, these obvious passwords are easier for unauthorized users to figure out, enabling them to gain access to the user’s desktop application and hack into the network. Network security is no stronger than the weakest password in the system.
- If users forget their passwords, then they call IT support. Password-related help desk calls cost money and take IT personnel away from core tasks. Password reset calls now represent as much as 40 percent of the help desk workload, with the cost of the average call estimated at US$25.

Single Sign-On Options

Implementing single sign-on (SSO)—either on a standalone basis or integrated into an IdM system—solves these password-related problems and reduces IT support costs, improves enterprise security, and simplifies password management.

An SSO system enables users to access all their applications through a single authentication event. Depending on the solution selected, the SSO could also enable the network administrator to assign and control passwords from a single console, eliminating the need to personally set passwords at each user’s workstation.

There are several variations on SSO available.
Web Single Sign-On

A Web-based access management solution can include an SSO capability for Web-based applications. With Web-based SSO, the user supplies a credential. The Web server then validates the password with a central credential server. If a match is found, then the user is granted access to the Web-based application or system.

With users accessing more and more applications over the internet from application service providers and other sources, Web-based SSO is critical. However, Web-based SSO does not cover password sign-on for non-Web-based applications such as mainframe and client/server applications. A separate ESSO is often needed for such applications.

Password Synchronization

Some IdM solutions offer password synchronization, where all applications that the IdM supports share the same password. In password synchronization, a change to a password on a connected system is automatically replicated to all other integrated or supported systems.

For end users, synchronization does provide some simplification for their password issues. Even though they still have to type in their user credentials for each application, they can—for some applications—use the same password. However, relatively few enterprise applications have the interfaces needed to support synchronization.

Another weakness of synchronization is that the password to which the applications are synchronized must be set at the weakest capability among all the supported applications. Therefore, all supported applications are susceptible to a security breach based on exploiting this weak password. Hackers can choose to attack the system with the weakest security controls, knowing that the password they obtain can be used on all other synchronized systems, regardless of their security controls. Thus, the security controls of all synchronized applications are reduced to that of the weakest system.

In addition, applications that lack the necessary interfaces or are hosted on other networks cannot be supported. Users are still required to log on to all unsupported applications.

Difference Between Synchronization and Enterprise Single Sign-On

Password synchronization actually changes the passwords for all the applications to a single common password. So all applications have the same password, but users must enter it into each application that requires the password. By comparison, ESSO keeps an encrypted database of credentials for every application. It enters the unique password automatically and transparently to the corresponding application whenever users open that program. With ESSO, users do not have to remember or enter a user ID or password to use their associated applications, the ESSO system does it automatically—users log on once through a single authentication event.
The Evolution of Enterprise Single Sign-On

When first introduced, ESSO was highly touted for its ability to create a strong, simplified security infrastructure. However, implementing the solutions was difficult. Many projects were abandoned or failed to achieve desired results. Fortunately, technology has improved, and current ESSO solutions are more sophisticated and easier to deploy.

First-Generation Enterprise Single Sign-On

First-generation ESSO solutions were server-based. The user had to access an SSO server to be authenticated, and then the server would 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 infeasible. 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, ranging from US$15,000 to US$40,000 in added programming costs per connector. Multiply that by hundreds of thousands of enterprise applications, and these first-generation 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.

Second-Generation Enterprise Single Sign-On

With the new generation of ESSO solutions, network administrators do not need to replace applications’ native authentication. These ESSO solutions incorporate a client-side agent to recognize and respond to a wide variety of applications’ logon and password change requests. Although each application presents its requests differently, a client-based agent can consistently and reliably identify and respond to these disparate requests.

ESSO frees you from the “authentication silos” built into your various enterprise applications. Best of all, you can give users a single authentication event to unlock the client-based agent and grant access to every application they use—and you can make that password as simple or complex as you desire.

Oracle Enterprise Single Sign-On Suite Plus

Oracle Enterprise Single Sign-On Suite Plus is an ESSO solution with a patented architecture that enables seamless implementation with your existing infrastructure without change—no integration or large deployment effort required. The software can also be used to provide standalone ESSO.

Typically, end users will have separate accounts for several applications. Each application requires users to enter a user ID and password. Access is granted only if the correct ID and password are entered. With Oracle Enterprise Single Sign-On Suite Plus, users only have to log on to Windows with a single password. After they are logged in to Windows, whatever application they go to gets the correct ID
Implementing Enterprise Single Sign-On in an Identity Management System

and password transparently and automatically from Oracle Enterprise Single Sign-On Suite Plus—eliminating the need for users to remember all the IDs and passwords for their applications.

When an application presents a dialog box asking for an ID and password, Oracle Enterprise Single Sign-On Suite Plus recognizes the request and searches an encrypted datafile for a corresponding set of credentials. If these credentials are present, then Oracle Enterprise Single Sign-On Suite Plus decrypts them on the fly and submits them to the application. The user can log on to any application—Windows, mainframe, telnet, Java, or Web-enabled—without touching the application, through the integration of server-side connectors or agents.

Oracle Enterprise Single Sign-On Suite Plus can use virtually any LDAP directory, Microsoft Active Directory, or SQL database server as its user profile and credential repository. Initial authentication can be provided from the Windows logon using a password as well as industry-leading smartcards, biometrics, or tokens.

Benefits of Oracle Enterprise Single Sign-On Suite Plus

Oracle Enterprise Single Sign-On Suite Plus offers several important advantages to the enterprise:

- Gain access from any location to maximize productivity.
- Eliminate lost or forgotten passwords; users have one password to remember.
- Lower user support costs by eliminating password-related support calls.
- Securely store and manage all passwords—no more searching for lost passwords.
- Improve network security by preventing unauthorized users from accessing enterprise applications.
- Facilitate regulatory compliance including SOX and HIPAA.
- Simplify password administration from a single console.
- Integrate and scale ESSO with your IdM solution.

Maximize User Productivity

Have you ever wasted time frantically searching for a password to access an application? Then you know how password problems can adversely affect user productivity. Imagine a company with 10,000 users who spend one hour a month looking for passwords, asking for new passwords, or spending time on other authentication problems that prevent them from logging on. If the value of their time is US$60 an hour, then the cost in lost productivity to the organization is more than US$7 million.

With ESSO, users can log on to all their applications with a single password, eliminating the need to remember or keep a record of multiple passwords for the different software packages. Users can access their applications from the desktop or when traveling, roaming between computers, or working at a shared workstation.
Lower Support Costs

The return on investment from ESSO is generated by reducing password-related calls from users to IT support. For an enterprise with 10,000 users, assume that the average user makes two password-related calls to IT support per month. Each call costs US$25. The total cost of all password support calls for the 10,000 users is US$500,000 a year. A reasonable expectation is that integration of ESSO with IdM can eliminate 95 percent or more of password-related support costs, which represents a savings in the 10,000-user enterprise of US$475,000.

Securely Store and Manages Passwords

In many enterprises, passwords are assigned in a haphazard fashion—and stored randomly in file drawers and on written lists. Without a centralized and organized means of storing and controlling passwords, users have a difficult time when passwords are lost or forgotten. ESSO provides end users with a central point of control for password administration, so when needed, users can retrieve passwords in seconds.

Improve Network Security

Conventional password protection systems entail several security risks for the enterprise.

- Passwords created by users are usually short, simple, obvious, and easy to hack.
- Users are often cavalier about protecting passwords, leaving them scribbled on notes affixed to their monitor or posted on a wall or bulletin board—in plain view for anyone to see and copy.

With ESSO, network administrators can assign users application passwords of any length or complexity, because each user needs to remember a single password to log on.

Facilitate Regulatory Compliance

By controlling password access to enterprise applications, ESSO can help your organization achieve compliance with key regulations.

Sarbanes-Oxley Act

Enacted in the wake of corporate and accounting scandals, SOX dictates more-restrictive requirements for corporate governance and the reporting of business, accounting, and financial data. Under SOX, companies must certify that no one has tampered with quarterly and annual financial reports.

Health Insurance Portability and Accountability Act

Signed into law in 1996, HIPAA protects the rights of American workers who have pre-existing medical conditions or might suffer discrimination in health coverage based on their individual health. Specifically, the HIPAA Security Rule requires organizations to implement a unique user identification method, password management, and automatic termination of inactive sessions—all of which an ESSO solution provides.
Password synchronization does not comply with these laws: the regulations require each application to have its own user ID and password, and synchronization resets all applications to a common password. Auditors are now telling certain companies to remove or replace password synchronization products with a solution that uses a specific, unique user ID and password for each application. ESSO meets that requirement.

Implementing ESSO does not automatically achieve full legal compliance. But it can mitigate regulatory and security compliance costs. ESSO and other identity-based access controls are important components of accountability and restrictive access to data, but other security and audit controls are also required. Data confidentiality might require cryptographic methods to be used, both while the data is rested (stored) or in motion (such as over Secure Sockets Layer or virtual private network secure channels).

**Simplify Password Administration**

Network administration is greatly simplified when any authorized administrator can perform administrative functions from a single console. Oracle Enterprise Single Sign-On Suite Plus can provide this single point of control for the creation, distribution, and maintenance of enterprise application passwords. With this solution, new hires and moved users can get access privileges faster. In addition, network administrators can reliably ensure compliance with secure standards and globally audit user access rights.

**Report on Password Activity**

IdM is not only about knowing who has been granted access rights to what resources, but it is also about knowing who actually accessed those resources, where, and at what times. With ESSO, network administrators get comprehensive reports on password-related activity, showing who used passwords, what applications they accessed, where, and when.

Application use can also be tracked and reported. Oracle Enterprise Single Sign-On Suite Plus allows the administrator to correlate historical access data to the access rights originally granted, ensuring that security policy is maintained over time. Oracle Enterprise Single Sign-On Suite Plus knows in real time which users accessed various applications and when. The solution captures this data because it actually executes the access for the user. By publishing that audit trail to the appropriate management consoles, Oracle Enterprise Single Sign-On Suite Plus compiles a total view of user activity.

**Integrate with Identity Management and Scale to Enterprise Levels**

The fundamental notion of IdM is that users have identities and access rights and can access the network resources they need based on those identities. IdM systems should effectively and consistently manage users over large numbers of systems and directories.

However, if users must use multiple IDs and passwords, then as far as they are concerned, IdM does not serve them well: they need multiple credential sets—one for each system—as a proxy for their true identity. By integrating Oracle Enterprise Single Sign-On Suite Plus with your IdM system, you make identities portable and functional across all systems.
A key objective of IdM is to simplify user management by relying on one centrally managed identity for each user that, in theory, all applications and access processes can leverage. ESSO further simplifies IdM and access while improving security.

Without ESSO, only account identities for the small subset of applications with provisioning connectors are correlated to the user's identity. But Oracle Enterprise Single Sign-On Suite Plus can correlate all user identity information and publish it to the provisioning system. Oracle Enterprise Single Sign-On can be integrated with leading IdM provisioning solutions, including Oracle Identity Manager and IBM Tivoli Identity Manager. Through integration of ESSO with IdM, administrators can transparently add credentials to each end user. Eliminating the need for users to touch or know their applications' credentials results in stronger authentication standards.

Conclusion

Enterprises make significant investments in firewalls, antivirus software, data encryption, and other computer security technologies. But passwords are an often-overlooked aspect of enterprise security.

A password that can be found or figured out by an unauthorized user provides easy entry into the network and bypasses all other security measures. As for authorized users, forgetting or losing passwords is a too-common problem that adversely affects productivity and adds a costly and time-consuming administrative burden to IT support.

By implementing Oracle Enterprise Single Sign-On—either standalone or integrated into your overall IdM system—network administrators can consolidate all user authentications under a single authentication to access all applications with one logon. Through this comprehensive ESSO architecture, companies can

- Increase user productivity
- Lower IT support costs
- Enhance network security
- Facilitate compliance with HIPAA, SOX, and other regulatory requirements