ORACLE

FUSION MIDDLEWARE
ACCESS MANAGEMENT

An Oracle White Paper
January 2014

Buyer's Guide for Enterprise Single Sign-On

ORACLE

Disclaimer

The following is intended for information purposes only and may not be incorporated into any contract. It is not a commitment to deliver any material, code or functionality and should not be relied upon in making purchasing decisions. The development, release and timing of any feature or functionality described in this document remains at the sole discretion of Oracle.

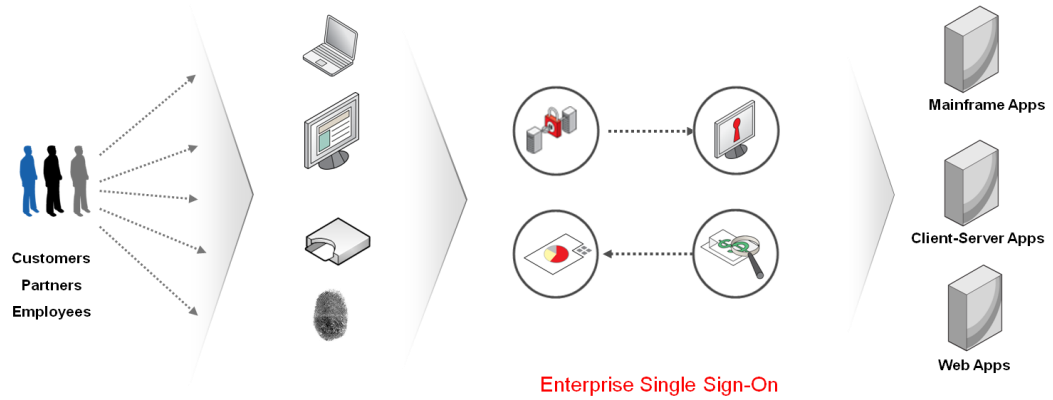
Introduction

Various studies estimate that more than 25% of help desk calls are related to password resets. For some organizations, that number may be much higher. A typical enterprise has hundreds or thousands of users. Corporate users need access to many enterprise applications on a regular basis. Many of these applications could have different requirements for what constitutes a valid password, such as a combination of alphanumeric and/or special characters. In addition, departments and workgroups might each have their own subset of applications, increasing the difficulty of administering identity management and security policies throughout the enterprise. Cloud computing further complicates the situation as enterprises have no control of those applications and their identity management systems at all. 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, they don't enforce strong password policies and moreover this is not secure as passwords can be stolen by malware or lost when users upgrade their desktops. Or if users experience desktop issues, such as a hard disk crash or a malware infection, then the stored password could be deleted or stolen.
- 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 may represent as much as 40 percent of the help desk workload, with the cost of the average call estimated at US$25.

Enterprise Single Sign-On (ESSO) meets these needs better than any other technology on the market. At a basic level, ESSO technology absolves users of all password responsibilities except for the Network logon. 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 helpdesk costs. When evaluating ESSO solutions organizations should think about how to enable a comprehensive solution for managing identity profiles and

permissions throughout the entire identity lifecycle, thereby ensuring regulatory compliance – with mandates like Sarbanes-Oxley and HIPAA, and simplified administration – how you can manage password policies from a single console. A comprehensive ESSO solution significantly strengthens an organization's overall security.



User Sign-On to Enterprise Applications

Business Drivers for ESSO

Here are the main business drivers for ESSO in any enterprise:

- **Password Management** - There is a need within enterprise organizations to simplify the end user experience, to reduce password related help desk costs and enhance security by eliminating poor end user password management.
- **Identity Management** - There is a greater need for integrated enterprise sign-on which is a key requirement for, and often a first step, of a complete enterprise identity management solution and can speed up an Identity Management deployment project.
- **Strong Authentication** - Integrating strong authentication for applications can be complex and costly to implement. Many organizations have existing investments in strong authentication devices such as biometrics, tokens, smart cards, etc which they want to leverage to strengthen authentication for all applications.
- **Compliance** - Eliminate the hidden end user costs associated with compliance driven initiatives. Extend audit and reporting capabilities to include user sign-on data.

Benefits of ESSO

ESSO offers a number of important benefits to an enterprise:

- **Maximizes productivity** - Allows users to gain quick and easy access from any location.
- **Eliminates lost or forgotten passwords –** users have just one password to remember.
- **Lowers user support costs –** virtually eliminates password-related support calls.
- **Securely stores and manages all passwords –** eliminates the need to manually manage passwords.
- **Strengthens authentication security –** leverages existing strong authentication devices to simplify user authentication without the requirement of a separate infrastructure to manage.
- **Improves network security** – prevents unauthorized users from accessing enterprise applications.
- **Aids in regulatory compliance –** including Sarbanes-Oxley and HIPAA compliance.
- **Simplifies administration –** enables control of password policies from a single console.
- **Rapid deployment and Integration –**Can be rapidly deployed with high visibility for quick ROI to start off and IDM project or Integrates with an existing Identity Management lifecycle management solution.

Overview of Oracle ESSO

Enterprise users constantly have the need to access various enterprise applications, whether they are connected to the corporate network, traveling away from the office, roaming between computers or working at a shared workstation. Oracle Enterprise Single Sign-on Suite Plus (Oracle ESSO) lets users login to enterprise applications using a single password to access any password-protected application on the desktop, network or Internet.

Oracle Enterprise Single Sign-On Suite Plus offers a highly scalable enterprise single sign-on infrastructure, providing features such as single sign-on, client-side Windows password reset, centralized user provisioning, support for kiosk environments, strong authentication, and comprehensive auditing, as well as seamless session integration with Oracle Access Management Access Manager, an industry leading web access management solution. It also includes a new cross-platform Logon Manager that provides web-based single sign-on across computer and mobile devices.

The basic steps of operation using Oracle ESSO are as follows:

- User Authenticates to ESSO. This is generally a shared authentication event with the windows workstation, but can be configured to require incremental strong authentication
- User requests access to an enterprise application that can be windows, mainframe, web or Java applications
- Oracle ESSO Logon Manager Agent intercepts user request on his desktop
- The ESSO Logon Manager retrieves the user record, and then fills in the appropriate users credentials for the ESSO enabled application. The application specific username and password are sent to the application.
- User is granted access to the application

Solution Overview

The Oracle ESSO Suite consists of the following components:

- **ESSO Logon Manager (ESSO-LM)** – provides single sign-on functionality.
- **Access Portal** – Provides cross-platform single sign-on functionality to web-based applications.
- **ESSO Password Reset (ESSO-PR)** – provides self-service password reset ability.
- **ESSO Provisioning Gateway (ESSO-PG)** – provides session and application management for kiosk environments.
- **ESSO Kiosk Manager (ESSO-KM)** – provides session and application management for kiosk environments.
- **ESSO Universal Authentication Manager (ESSO-UAM)** – provides strong authentication inside and outside the Windows session.
- **ESSO Anywhere** – provides the ability to deploy custom-configured ESSO-LM installation packages to end-user workstations not connected to the enterprise network.
- **ESSO Reporting Service** – captures event data and stores them in event log or database.

Oracle ESSO supports an extensive list of directories and databases as a central repository for user credentials, application logon templates, password policies, and client settings. Oracle ESSO helps enterprises advance their identity management, compliance and authentication initiatives by simplifying, extending and securing enterprise end user sign-on.

Here is a list of exclusive features offered by the Oracle ESSO solution:

- **Web-based application SSO:** This includes an SSO capability for Web-based applications. With Web-based SSO, the user supplies a credential. The Web server validates the password with a central credential server. If a match is found, the user is granted access to the Web-based application or system. A cross-platform Access Portal provides SSO to various web-based applications, including Oracle Access Management protected resources, federated resources and SaaS applications.
- **Desktop/Mainframe/Host Applications SSO:** The Oracle ESSO solution provides access to all desktop applications (ex: windows/Solaris) Mainframe applications (such as 3270, 5250), and Host applications (example Telnet). Provides users the ability to use multiple emulators and multiple emulator sessions simultaneously. Supports user needs to both logons and password-change for desktop applications and allows administrators to add mainframe/desktop applications and configure them and easily deploy them to users.
- **Java Applications & Applets SSO:** Provides user access to AWT and Swing and standalone Java Applications and Applets
- **Reporting**: Provides rich reports on application usage. Also provides network administrators comprehensive reports on password-related activity, showing who used passwords, what applications they accessed, where, and when.
- **Oracle Access Management - Access Manager Integration**: Access Manager is Oracle's web access management solution. The ESSO and Access manager integration provides organizations the ability to implement a single SSO session no matter what type of application is being accessed. This increases the compliance stance and allows OAM to leverage the strong authentication support of ESSO for the web SSO session.
- **Enterprise-class Scalability:** The Oracle ESSO solution is unique in its ability to scale to service the needs of enterprises of all sizes.
- **On-demand ESSO:** The Oracle ESSO suite Plus solution provides the advantage of allowing system administrators to simply host the ESSO product online for users to download. Users will download and run ESSO with a simple click of a button from a host website or a network file share. This offers true ESSO portability and also reaching a wider set of audience in an Organization like remote, mobile and temporary users, including partners, outsourcers, contractors and other non-employees.

Enterprise Single Sign-On Checklist

This section presents a baseline list of requirements for an ESSO solution. In each of the tables presented, the left column describes a requirement, and the right column describes how the Oracle ESSO Solution meets that requirement.

☑ **Enterprise Single Sign-On**	Allows user to log on to networks, applications, and Web sites using a single password. Once a user authenticates to Windows for the first time, the solution manages the passwords for all subsequent application logons with the ability to add layered security if required.
☑ **Windows Application SSO**	Pre-configured for Microsoft Office, Adobe Acrobat Reader, FrontRange Goldmine, Interact Act!, PKZip, and virtually all other Windows applications.
☑ **Web based application SSO**	Pre-configured for accessing web applications on Microsoft Internet Explorer Mozilla Firefox and Google Chrome. Also provides Support for Web pages including form based and pop-up sign-ons.
☑ **Mobile Device Support**	A cross-platform Access Portal provides Single Sign-On to web-based resources from various platforms, including mobile platforms from Apple and Google.

☑ **Java Application and Applets Desktop SSO**	Supports Java Runtime Environment (JRE) version 1.3 or later
☑ **Host/Mainframe application Single sign-on**	Supports AS/400 (5250), OS/390 (3270), and Unix (Telnet) Pre-configured for most emulators including: Attachmate Extra!, G&R Glink, Hummingbird HostExplorer, IBM Pcom and Host On-Demand, NetManage Rumba, ScanPak Aviva, WRQ Reflection, Zephyr Passport, and many more Supports multi-screen logon/password change scenarios Supports multiple emulators simultaneously.
☑ **Credential Sharing**	For applications that authenticate using the same repository, the password is always in sync no matter where it is changed from.
☑ **Password Reset**	Provides self service (GINA or Browser) or assisted password resets for users
☑ **Provisioning to Desktop and Enterprise Resources**	Facilitates a way to provision users to ESSO applications with the out-of-the box connectors for Oracle Identity Manager , Tivoli Identity Manager and Sun Identity Manager (SIM) This enables user provisioning to enterprise resources and enable ESSO for applications in the enterprise. Supports bulk import of user accounts.

☑ **Strong Multi-factor User Authentication**	Provides multiple authentication modes for the user, including Windows login, LDAP, PKI, smart card, biometric or token-based authentication without modifying applications for rapid deployment and low cost adoption
☑ **User Access Modes**	Provides multiple ways for the users to access enterprise applications, including desktop, offline, kiosk, or shared workstation
☑ **Support for Offline or Disconnected Users**	Oracle ESSO was designed to support all user work modes; Connected, Disconnected, Stand-Alone, Roaming, Mobile and Kiosk. As a result, Oracle ESSO is not directly dependent on a server in order to provide enterprise SSO. Supports Offline/Disconnected usage by keeping a locally cached encrypted copy of the user credentials on the local workstation. This local copy automatically synchronized at a record level when the user regains connectivity to the designated repository. The ability to enable the off-line cache is fully controllable by the administrator centrally. You can control these settings globally, by group/role or user and by specific machine in order to achieve the use cases desired by your organization.

☑	**Enterprise Directory Integration**	Fully supports roaming users, defined as users who move from workstation to workstation. Oracle ESSO can provide each user with access to their unique credential repository from virtually any workstation with connectivity to the Server. Supports the following directories for synchronization; SunOne Directory, Novell NDS eDirectory, Microsoft Active Directory, Microsoft ADAM, Oracle Virtual Directory, or virtually any other LDAP v2 or v3 directory.
☑	**Encryption Support**	Protects each user's credential store using one of several selectable encryption algorithms. By default, Oracle ESSO uses the Microsoft CAPI AES encryption algorithm to secure all user credentials locally on the desktop and to remote directories or network drives. MS CAPI 3DES is certified to meet FIPS 140-2 requirements. Oracle ESSO also includes MS-CAPI AES 256 bit (FIPS 140-1), RC4, Blowfish 448, and Cobra 128 as administratively selectable algorithms. Each credential is only decrypted on an as-needed basis and is never stored or cached in the clear. Oracle ESSO uses cryptography to confirm user authentication and to secure storage of user credential data.

☑ **Administrative Console**

The Oracle ESSO Administrative Console is a GUI based, wizard driven configuration. It allows administrators to configure all of the Oracle ESSO agent settings.

- Configuring all application specific settings for single sign on
- Extending the schema for the directory
- Managing, adding and updating ESSO specific configuration settings across
- Updating Oracle ESSO application configuration templates
- Generating and publishing application templates to the LDAP/directory.

☑ **Authentication**

Allows for a variety of Primary/Front End Authentication methods as it ships with authenticators for Windows Logon, Windows Active Directory/Domain Logon, LDAP, PKI Systems, Smartcards and Biometrics.

The authenticator allows users to prove their identity, whether through a Windows Domain Password, biometric or smart card. The authenticator takes the user's proof and passes it to the authentication service. The authentication service validates the credentials provided by the authenticator against either its own store, or a system authentication Service such as a Windows domain or a PKI.

☑	**Directory Synchronization**	Synchronizes with the directory based on intelligent activity, adding a logon, password change, starting up, logging off, a configurable timer, etc. Some companies synchronize data based on a fixed time interval, which can allow for data to get out of sync if it is changed, and for synchronization to occur from numerous machines when none is necessary.
☑	**Directory Schema Extension**	Oracle uses an effective class schema extension, which leaves your base schema intact as delivered by your directory vendor and creates a self-contained configuration object using our own object classes. Conversely, some companies make a base schema extension, which modifies your base schema, specifically the user object and appends SSO data to it. This causes you problems during directory upgrades, and directory replication (user object is always replicated).

Password Policy Management

Password Policy Management allows administrators to define a default global password policy, application specific password policies, as well as subscribing several applications to one password policy.

☑ **Password Management**

Oracle ESSO can recognize a password expiration/password change request, and either prompt the user to compose a new password (forcing the user to comply with the password policy) or automatically (and transparently) generate a random password that complies with password policies set by an administrator on behalf of the end user. Additionally, Oracle ESSO has the ability to monitor the age of a stored password and at a pre-configured time interval (30 or 60 days for example) initiate the password change process at the local application level.

Additionally, with Oracle ESSO, the administrator can specify:

- Maximum/minimum password lengths
- Maximum repetition of a character
- Number of times a character can be adjacent to itself
- Allow numeric characters
- Maximum/minimum occurrence of numeric characters
- Allow numeric to start password
- Allow numeric to end password
- Allow special characters (specify the characters to allow and exclude)
- Maximum/minimum occurrence of special characters
- Alpha usage (none, upper, lower, upper and lower)

Reporting

The Reporting component of the Oracle ESSO Suite provides organizations with the ability to create reports to leverage all data and events that routinely take place in the day-to-day usage of applications protected by the ESSO Suite.

☑ **Centralized Reporting Database**	Stores all event data from which reports can be generated in a central Oracle ESSO database.
☑ **Web-based Admin Console**	Reports can be generated remotely via a Web interface. Accesses the SQL database and generates reports from the stored event data. Reports may also be manually generated by querying the Oracle database
☑ **Reporting Service**	Collects audit/reporting events into the database.
☑ **Application Integration**	Capture events information such as application logon, credential capture, password change, and so on, from applications protected by ESSO Suite and sends the data to the reporting service.

Oracle ESSO simplifies the creation of audit reports from the event logging data provided by Oracle ESSO Logon Manager. Additionally, from the Oracle ESSO Administrative Console, the administrator can initiate a ESSO Usage report against the data stored in the central repository to export a report containing the credential usage information by user so that you can easily and quickly see which users have credentials for which applications and identify their usage and last change. Once logged, all ESSO events are permanently stored and become part of the overall audit record of computer use and policy control.

Strong Authentication

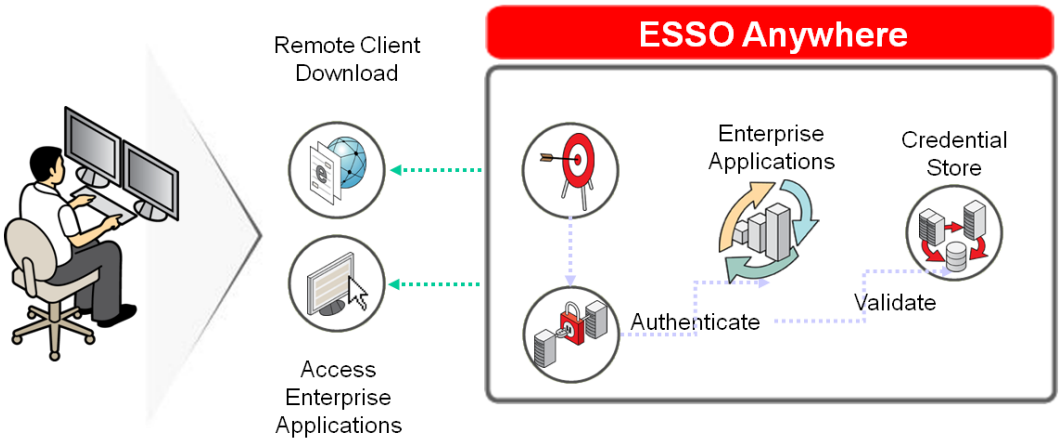
Oracle ESSO Universal Authentication Manager (UAM) strengthens security for virtually any application by enabling customers to layer applications with existing strong authentication solutions. Integrating strong authentication with applications can be a costly and complex process. UAM overcomes this challenge by enabling organizations to leverage existing investments in strong authentication schemes to bolster security for virtually any application transparently without the need to modify backend application infrastructure.

☑	**Biometric Logon**	Enables the enrollment and use of third-party fingerprint scanners, such as external USB scanners and scanners built into laptop computers.
☑	**External Biometric Service Provider (BSP) Support**	Enables the enrollment and use of a 3rd party BioAPI-compliant BSP modules, including fingerprint, palm, retina/iris scanners and facial feature analyzers.
☑	**Smart Card Support**	Allows the enrollment and use of smart cards. Additionally, the PIN present on the card can be enforced if two-factor authentication is desired.
☑	**Proximity Card Support**	Allows the enrollment and use of RFID. Additionally, a PIN can be defined and enforced if two-factor authentication is desired.
☑	**Support for Offline and Online Modes**	• In the offline mode, configuration is configured and stored in the user's secure local cache on the user's workstation, • In the online or enterprise mode, configuration is synchronized with the central repository and configured remotely by an administrator

☑	**Auditing Support**	Captures detailed authentication events such as logons, enrollment, etc and logs events to the reporting service.

On-Demand ESSO Install

Oracle ESSO Suite Plus simplifies ESSO deployments for system administrators while also extending the benefits of Enterprise Single Sign-On to users who are remote and mobile. For organizations that have users who need access to ESSO from anywhere at any time, ESSO Suite Plus provides the ability to click and run ESSO on-demand from anywhere. Unlike any other product on the market, ESSO Suite Plus does not require a traditional installation or does not depend on the browser to achieve ubiquitous ESSO access.

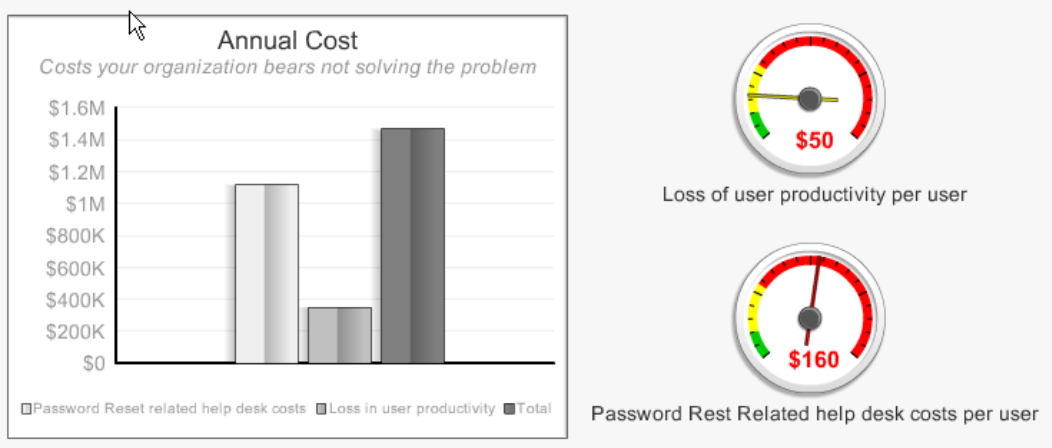


ESSO Anywhere

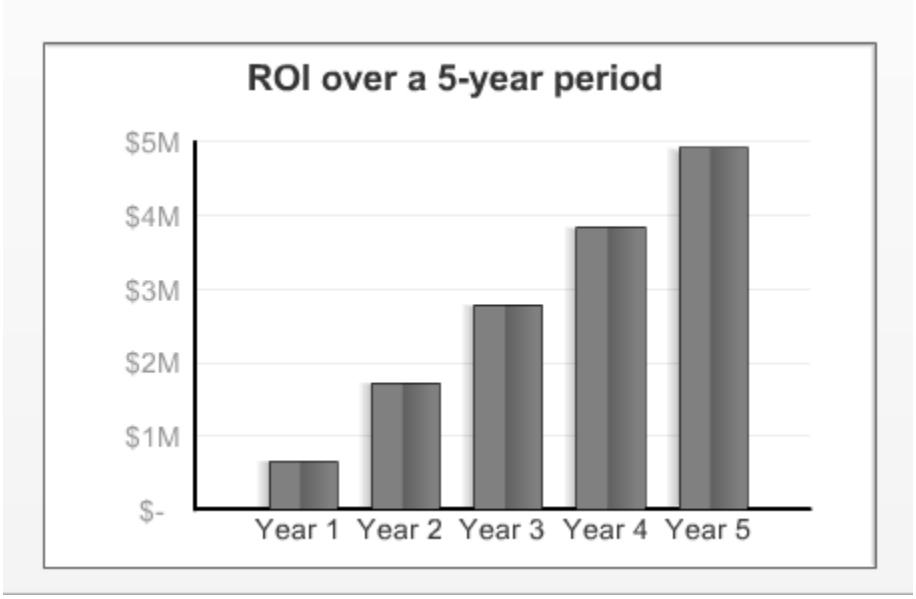
☑ **Centralized Deployment Option**	Provides one deployment package for all the ESSO software.
☑ **"Click and Run" (On-Demand) ESSO**	Users will download and run ESSO with a simple click of a button from a hosted website or a network file share.
☑ **Auto Updates and Rollback**	The deployment packages can be version controlled hence offers easy updates and rollback. Updates can be set as required or optional. Force update can be set by set with against a minimum version of deployment package. Can specify how often to check for updates like very time the ESSO client is started, weekly or monthly

Return on Investment (ROI)

Organizations implementing Oracle Enterprise Single Sign-On Plus realize a healthy ROI by saving on password reset related helpdesk costs and by significantly reducing lost user productivity related to forgotten passwords. For instance, an organization with 7,000 users, an average password reset cost of $40 where users on average forget 4 passwords a year, loses about $1.12 million annually to password related helpdesk costs. Adding productivity losses from password reset related calls, the organization could lose nearly $1.5 million annually. Implementation of Oracle ESSO Suite Plus results in an ROI of more than 100% within the first year for such an organization. Oracle ESSO Suite Plus not only eliminates helpdesk costs it also improves user productivity and yields an ROI of nearly $5 million for the organization over a 5 year period.



Hard dollar costs of not solving the problem of forgotten passwords



Projected Return on Investment over a 5 year period from Oracle ESSO Suite Plus Implementation

Conclusion

Oracle Enterprise Single Sign-On (ESSO) enables users in an enterprise to access virtually all applications through a single authentication event and do self-service password management as well.

Since Enterprise Single Sign-On (ESSO) systems are designed to minimize a user typing in their credentials to sign onto multiple applications, the ESSO solution automatically logs the users in,

acts as password filler and avoids the user the need to know his password. This works well even when enterprises have to deal with different types of users for their enterprise applications like Suppliers, Contractors, Resellers, Distributors, Agents and Joint Development partners. eSSO also provides a quick and effective way to enable single sign on to cloud applications with improved user experience and productivity. In addition to providing a single, secure sign-on to all enterprise applications, an ESSO solution enables strong authentication, improves compliance and accelerates cost savings resulting in high ROI for enterprises.

Oracle ESSO Suite Plus can accelerate deployments by eliminating the need to perform system integration tests before deploying the software and then relying on desktop refresh or scheduled push procedures for installation. It helps avoid traditional installation problems, such as the need for administrative rights on the destination computer. In addition, it allows software updates and rollbacks to be applied automatically and managed from a central location.

Oracle ESSO Suite Plus is a proven solution that works with most enterprise applications without a lengthy and complex implementation effort. Seamless session integration between Oracle ESSO and OAM further enables enterprises to harvest the synergy of a web access management solution and an eSSO solution by providing superior user experience with all type of applications. Oracle ESSO Suite Plus delivers huge usability improvements for end users, indirect cost savings from decreased employee downtime, and high ROI through direct savings in helpdesk costs, while providing vastly improved security for all applications in the enterprise.

Buyer's Guide for Enterprise Single Sign-On
Jan 2014

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

Oracle is committed to developing practices and products that help protect the environment

0109