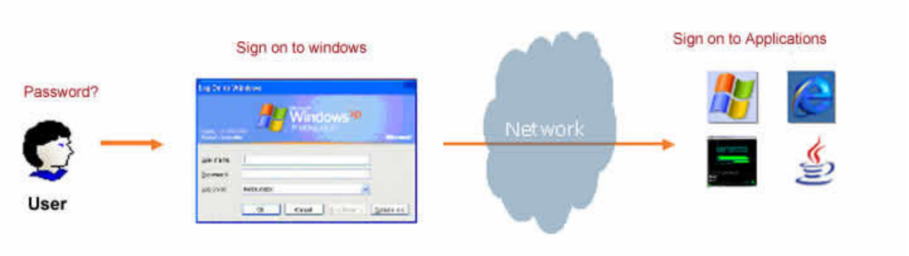
Oracle Enterprise Single Sign-on Technical Guide

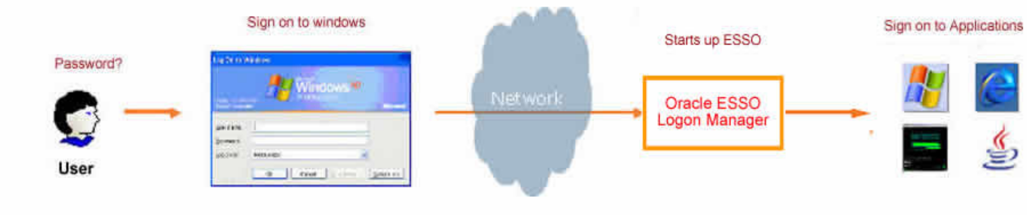
An Oracle White Paper
June 2009

EXECUTIVE OVERVIEW

Enterprises these days generally have Microsoft Windows® desktop users accessing diverse enterprise applications on a daily basis. Each enterprise application often has different security requirements and, as a consequence, users in many organizations are forced to remember multiple different passwords for various applications. In many organizations, users are often forced to remember more than six different passwords for various enterprise resources. As a result, there is a need to enable a simple and secure way for enterprise users to access heterogeneous applications (e.g. Microsoft Windows, Java, Mainframe applications etc) by signing on just once to their windows desktop. This should not only circumvent the need to remember credentials for individual applications but also enhance user productivity by eliminating helpdesk calls associated with forgotten passwords.



The Oracle Enterprise Single Sign-on (Oracle ESSO) Suite facilitates a way for desktop users to access enterprise applications by signing on just once to their desktops using a single set of credentials.



This eliminates the challenge for users to know application credentials for all the enterprise applications that they are entitled to access based on their roles and responsibilities.

ESSO is often the first step in deploying an Identity Management solution in an enterprise since it offers user identity mapping and fast ROI.

INTRODUCTION

Enterprise users have a constant need to access various enterprise applications, irrespective of whether they are connected to the corporate network, traveling away from the office, roaming between computers or working at a shared workstation. Oracle ESSO lets users access enterprise applications using a single password for any password protected application on the desktop, network or Internet.

The basic steps during an Oracle ESSO enabled application logon include:

- User requests access to an enterprise application, which can be a Windows®, mainframe, web or Java-based application. The Oracle ESSO Logon Manager Agent intercepts the user request on his desktop.
- The Oracle ESSO Logon Manager retrieves the user record and then fills in the appropriate credentials for the Oracle ESSO enabled application. The application-specific username and password are then sent to the application.
- User is granted access to the application.

The Oracle ESSO Suite supports an extensive list of directories and databases as a central repository for user credentials, application logon templates, password policies and client settings.

COMPONENTS OF THE ORACLE ESSO SUITE

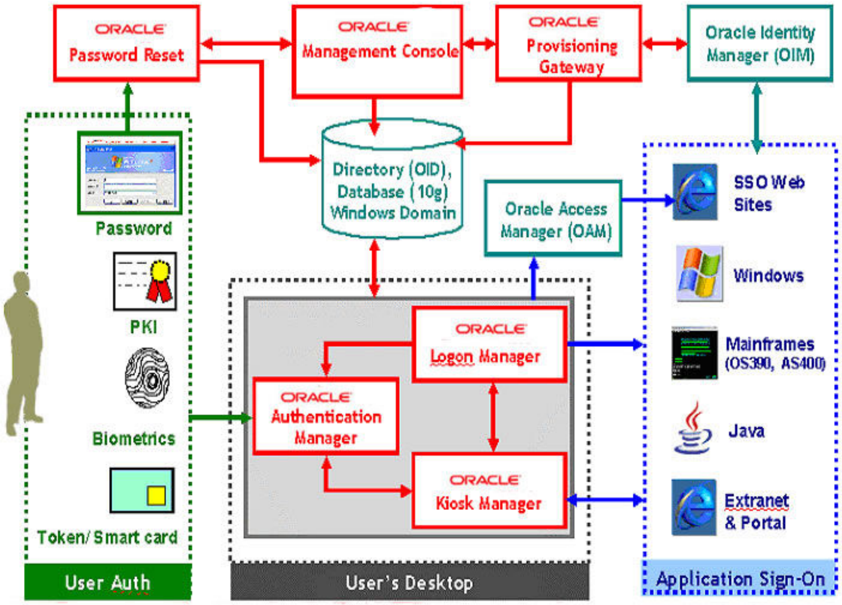
The Oracle ESSO Suite comprises five key components:

- **Oracle ESSO Logon Manager (ESSO-LM)** provides interfaces to network and computer logons as well as sign-on to applications, enabling users to log in one time with a single password. Once users are logged in, whatever application they open is served the correct ID and password transparently and automatically. This eliminates the need for users to remember and manage multiple user names and passwords for their applications, while allowing administrators to centrally manage passwords. The Oracle ESSO Logon Manager Admin Console interacts with the Logon Manager and facilitates management and administration of ESSO attributes.
- **Oracle ESSO Password Reset (ESSO-PR)** provides a recovery mechanism for users who forget their desktop passwords. If users forget their Windows password, then ESSO-PR enables them to regain access to their computer and the corporate network. This allows users to reset their password directly from the Windows logon prompt of their locked-out workstation, so that they can get to their applications within seconds - without having to call the help desk or go to another workstation.
- **Oracle ESSO Kiosk Manager (ESSO-KM)** provides initial user authentication and automatic user sign-off to kiosk environments, enabling secure kiosk computing at any location within the enterprise. The system monitors and protects unattended kiosk sessions from unauthorized access. Inactive sessions are protected by a secure screen saver, which permits the next user to sign on to a new session while safely terminating the prior session.

- **Oracle ESSO Authentication Manager (ESSO-AM)** allows organizations to use any combination of tokens, smart cards, biometrics and passwords to control user access to their applications; making it easier to implement advanced authentication strategies. The software integrates seamlessly, providing granular control over the level of authentication required to access specific applications.
- **Oracle ESSO Provisioning Gateway (ESSO-PG)** allows system administrators to directly distribute user credentials, usernames and passwords to Oracle ESSO. The administrator can add credentials for new applications and new users as well as modify or delete old credentials to Oracle ESSO. The Provisioning Gateway is also the interface that is used to integrate OIM, which enables provisioning of users to all enterprise applications and enables Oracle ESSO.

ARCHITECTURE:

The figure below represents the various components of Oracle ESSO. The ESSO-LM agent and the ESSO-LM admin console form the base components and all the other components are offered as add-on modules. The ESSO-LM is the primary component for detecting requests for credentials, analyzing the response necessary, responding reliably, logging events and administering settings.


ORACLE Password Reset
ORACLE Management Console
ORACLE Provisioning Gateway
Oracle Identity Manager (OIM)
Password
PKI
Biometrics
Token/Smart card
User Auth
Directory (OID), Database (10g) Windows Domain
Oracle Access Manager (OAM)
ORACLE Logon Manager
ORACLE Authentication Manager
ORACLE Kiosk Manager
User's Desktop
SSO Web Sites
Windows
Mainframes (OS390, AS400)
Java
Extranet & Portal
Application Sign-On

The Oracle ESSO Management Console enables administration of the ESSO environment and creation of application templates. Templates tell the desktop client which screens/fields of an application are used for username, password, etc. Templates are stored in a central repository (AD, SQL, TDS, etc). The desktop client automatically "synchronizes" with the repository to get new templates or updates for existing templates. The desktop client is responsible for performing SSO to desktop applications (Windows, Web, Java, Mainframe applications). It then populates the appropriate forms and fields based on the information contained in the template. Field information such as username and password can be filled in manually by the end-user during first time use or Oracle Identity Manager (OIM) can provision the user's account information automatically.

STORING AND SYNCHRONIZATION OF USER CREDENTIALS

1. Storing of User Credentials:

Oracle ESSO stores user credentials locally in the encrypted Local Credential Storage. No unencrypted credentials are stored on disk or in memory. Oracle ESSO stores the local, secure credential file in a specific directory within the application data directory of the user profile. This file can be secured from other users by properly configuring Windows security on NTFS partitions. This also means that if Windows "Roaming Profiles" are enabled, users can log on to Windows from any computer within a domain and their credential file will be available to them.

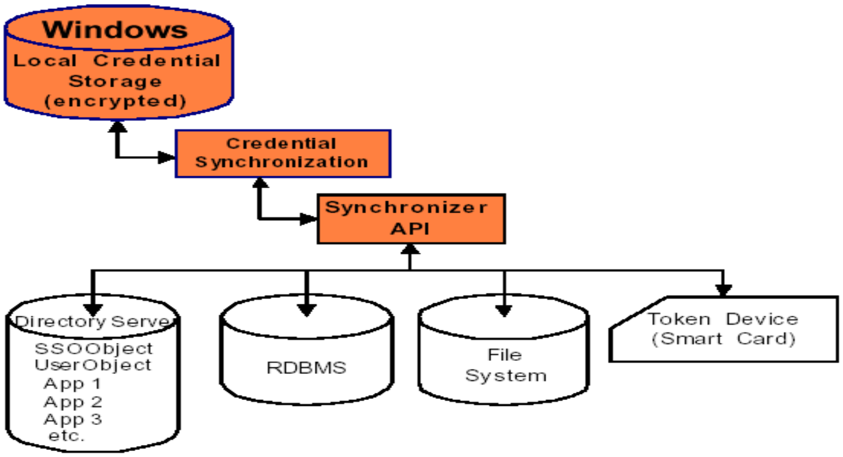
The benefits of local user credential storage are:

- Encrypted storage for security.
- Credentials are secured because they are never exposed in memory.
- Local storage delivers faster access than server-based systems.
- Users can log on from any computer within a domain if Windows "Roaming Profiles" are enabled.

2. Synchronization of Credentials:

While Oracle ESSO stores user credentials locally, it can synchronize the credentials and settings with remote network shares, directories, devices and so on. Synchronizing user credentials to a directory service or network drive enables mobility, eases deployment, simplifies administration and increases security (for example, on public workstations)

Oracle ESSO supports multiple directory services including Oracle Internet Directory, Sun Directory Server, Novell NDS, and Microsoft Active Directory Server out-of-the-box to store users' ESSO credentials

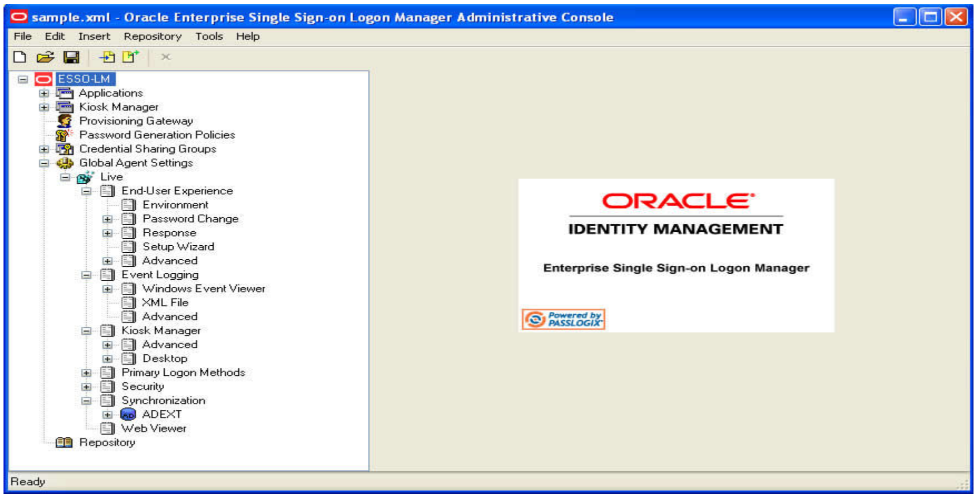


- The Benefits of synchronization for user credentials are:
  • Ensures that the latest set of user credentials for each application is available from all locations at all times.
  • Automatic backup of user credentials.
  • Availability of user credentials from multiple computers without requiring a new infrastructure.

ADMINISTRATION AND MANAGEMENT

Oracle ESSO has a GUI based Administrative Console which provides a wizard based configuration and control for:

- Directory configuration and administration
- Management of individual users or users by role and group
- Application configuration and policy control
- User configuration and policy control
- All of Oracle ESSO settings including password policies, system rules, UI functionality, re-authentication parameters, etc.



Oracle ESSO provides an out-of-the box connector for Oracle Identity Manager (OIM) whereby enterprises can provision their users with ESSO credentials such that they will never have to know their passwords.

HEALTHCARE USECASE FOR ESSO

Healthcare Challenges:

- Doctors often work at multiple hospitals – resulting in multiple passwords per location
- Doctors often have limited time to access information to respond in an emergency to provide the best care possible
- Doctors require access from anytime and anywhere, including Kiosks/Nurses Station, Private Office or another hospital
- Doctors demand fast, convenient and simple access to information
- Doctors may refer patients to another hospital that's more efficient
- HIPAA - Poor password/security practices and high Help Desk calls and costs

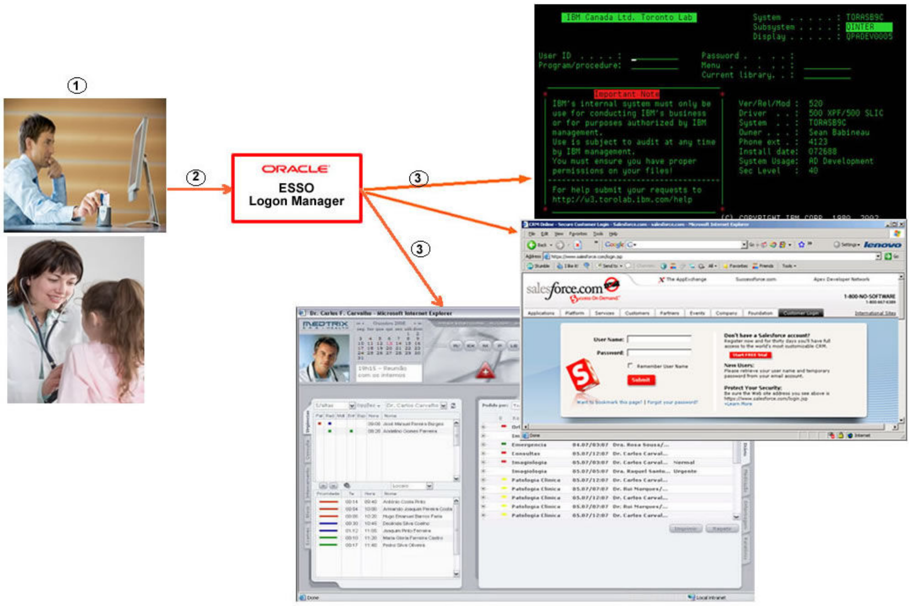
How Oracle ESSO can help Healthcare Organizations

Oracle ESSO would be installed on the hospital desktop and the doctor or health worker issued with a smartcard that can securely authenticate them to their computer or kiosk of choice.

Here are the steps that a typical doctor or health worker would undertake on an Oracle ESSO enabled desktop:

1. Insert smartcard through the associated reader and insert PIN to logon
2. The access policy can be set to require stronger authentication (such as a password) for users after which a user-specific Oracle ESSO session is enabled

3. Oracle ESSO then provides single sign-on to the healthcare applications depending on the associated user access policy



```
   IBM Canada Ltd. Toronto Lab                    System . . . . . : TORASB9C
                                                  Subsystem . . . . : QINTER
                                                  Display . . . . . : QPADEV0005

User ID . . . . :  _______      Password . . . . :
Program/procedure: _______      Menu . . . . . . : _______
                                Current library. . : _______

 -------------------------------------------
          Important Note
  IBM's internal system must only be       Ver/Rel/Mod :  520
  use for conducting IBM's business        Driver  . . :  500 XPF/500 SLIC
  or for purposes authorized by IBM        System  . . :  TORASB9C
  management.                              Owner . . . :  Sean Babineau
  Use is subject to audit at any time      Phone ext . :  4123
  by IBM management.                       Install date:  072688
  You must ensure you have proper          System Usage:  AD Development
  permissions on your files!               Sec Level   :  40
 -------------------------------------------
  For help submit your requests to
  http://w3.torolab.ibm.com/help
 -------------------------------------------
                                   (C) COPYRIGHT IBM CORP. 1980, 2002.
```

ESSO Benefits for Healthcare

Deploying Oracle ESSO in healthcare helps doctors and healthcare providers to overcome sign-on challenges and provides the following benefits

- Provides converged access. Doctors can use a single card for both physical and logical access
- Provides Physicians fast, easy and convenient access to desktops, healthcare resources and applications
- Offers user identification, authentication and session management by leveraging authentication card and PIN with no passwords to remember
- Provides a secure way to access applications from shared workstations minimizing infrastructure cost
- Facilitates access from anywhere. For example, home office, private office, or other hospitals
- Increases productivity
- Reduces Help Desk calls and user frustration
- Helps address HIPAA concerns

CONCLUSION

The Oracle ESSO Suite benefits enterprises in the following ways:

1. ESSO accelerates cost savings by virtually eliminating password-related Help Desk calls
    - An average enterprise spends about $25 on a help desk call, and 40% to 60% of calls to Help Desk are password-related.
    - ESSO also eliminates the need for enterprise users to remember multiple passwords.
2. ESSO helps address audit problems within an enterprise by facilitating these auditing capabilities.
    - Application access review by user
    - User account reconciliation
    - Cross-application access removal
    - Ability to enforce stronger password policy
    - Robust, repeatable process enforcement
3. ESSO improves user productivity and satisfaction through intuitive self-service password reset.

Deployment of Oracle ESSO can enable almost every enterprise to realize significant cost-savings in addition to enhanced user productivity and accelerated compliance with audit requirements. The Oracle ESSO Suite is easy to deploy and provides a fast time to value and compelling ROI.

Oracle Enterprise Single Sign -On Technical Guide
June 2009
Author: Kavya Muthanna

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