FUSION MIDDLEWARE
ACCESS MANAGEMENT

An Oracle White Paper
January 2014

Oracle Enterprise Single Sign-on Suite Plus 11gR2 PS2

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

Oracle Enterprise Single Sign-On Suite Plus (ESSO suite) offers a highly adaptable and scalable enterprise identity management infrastructure, providing features such as single sign-on to virtually any application with no modification to the target, client-side Windows password reset, centralized credential provisioning and de-provisioning, support for kiosk environments, strong authentication, and comprehensive auditing.

Supports the Majority of Today's Enterprise Applications

The ESSO suite is designed to provide single sign-on and password reset functionality for most Windows, Web, Java, and mainframe/terminal-based applications running on any operating system and accessed from Windows-based end-user machines. No modification is required to extend single sign-on to target systems. It also provides a cross-platform single sign-on solution for web-based applications, including SaaS, business partner and Oracle Access Management protected applications.

Support for SaaS Applications

The ESSO suite provides single sign-on to web-based applications, including SaaS applications. ESSO Suite also includes a cross-platform portal service that provides single sign-on to web-based applications across various operating systems and devices.

Fast and Efficient Deployment on Existing Infrastructure

The ESSO suite reduces total cost of ownership by leveraging existing infrastructure, such as directory servers and databases, and requiring no modifications to target systems. A fully customized MSI installation package can be easily generated and mass-deployed to end-user machines, eliminating the need for individual configuration.

Minimized Server-Side Footprint

Most functions of the ESSO Suite Plus are managed by the client-side components, including recognizing and responding to application request for credentials, enforcing policies and managing authentication. Some ESSO Suite applications utilize server-side components exclusively for administration and data storage.

Centralized Data Storage with Redundancy

ESSO Suite applications store data centrally in a data repository such as Microsoft Active Directory, Oracle Directory Services, and most other third-party LDAP-based directories, as well as Oracle 11g Database and most other SQL database solutions.

Leverages Existing Data Protection Mechanisms

Leveraging existing infrastructure supports existing failover and backup policies to automatically protect the centrally stored ESSO application data such as user credentials, application templates, and security policies.

Centralized Administration with Secure Policy Enforcement

Client configuration data, such as password policies, administrative overrides, and authentication policies, as well as application credentials, are managed from the administrative consoles included with each ESSO Suite application and synchronized with the repository, providing an efficient way for administrators to enforce specific end-user experiences and security policies enterprise-wide. Administrators can also remotely distribute application credentials to ESSO Suite users using provisioning systems such as Oracle Identity Manager without the need for end-user intervention.

Oracle Access Management Access Manager Integration

Oracle Access Manager (OAM) 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. After a successful authentication to ESSO, the ESSO agent obtains an OAM cookie and automatically injects it into the user's web browser to grant the user seamless access to OAM protected applications. Upon expiration of the ESSO session, the cookie is removed from the browser thus ending the OAM session as well.

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.

Built On Industry Standards

Oracle ESSO Suite applications use industry-standard technologies to implement many area of their functionality, such as:

- User data encryption using MS-CAPI (standard AES)
- Data repository access via Active Directory/AD-LDS, LDAP and SQL
- Interfacing with SmartCards via MS-CAPI and PKCS #11 interfaces
- Interfacing with external and embedded fingerprint scanners via BioAPI/BSP
- Integration with identity management systems utilizing SPML
- Storing configuration data using XML

ESSO Suite Functions

The ESSO Suite handles all tasks related to granting users access to applications, including automatic sign-on, application password change, Windows password reset, kiosk session management, application credential provisioning, as well as strong authentication inside and outside of the session. ESSO Suite's functionality is described in more detail below.

Enterprise Single Sign-On

- Provides automatic single sign-on functionality for most Windows, Web, Java, and mainframe/terminal-based applications running or being accessed from Windows-based workstations. The ESSO Logon Manager agent monitors the session, automatically detecting logon requests from applications and completing the logon automatically whenever possible.
- End-users enjoy hassle-free single sign-on to applications, whether connected to the corporate network, traveling away from the office, roaming between computers or working at a shared workstation.
- ESSO-LM can accept primary authentication inside the user's session directly from the Windows logon mechanism, as well as with most industry-leading SmartCard, proximity card, token, and, with the addition of ESSO-UAM, biometric solutions. ESSO-UAM can also replace the standard Windows logon mechanism with the above strong authentication solutions entirely (including two-factor authentication) for added security outside the session.
- Access Portal Service provides form-based single sign-on to web-based applications across different platforms (PC, Tablet & Smartphone) and operating systems. The service includes a set of RESTful interfaces that enables secure access to ESSO application configurations and credential store. An Access Proxy component provides ESSO capabilities (form-fill single sign-on and header-based authentication) to web-based applications without requiring any form of client component to be hosted on the device.

Application Password Change

- Provides automatic password change functionality for most Windows, Web, Java, and mainframe/terminal-based applications running or being accessed from Windows-based end-user machines. The ESSO Logon Manager agent application monitors the session, automatically detecting password change requests from applications and completing the password change either automatically or by prompting the user for a new application password.
- Automatically generated passwords conform to administrator-configurable password generation policies.
- The new password is automatically added to the user's credential store in the repository.

Self-Service Windows Password Reset

- Provides a fully integrated self-service Windows password reset solution for end-users, eliminating help desk calls and speeding the reset process. The user is challenged with a series of challenge questions which must be answered correctly in order for password reset to succeed.
- Challenge questions and acceptable answers, including the “weight” of each question, are administrator-configurable.
- Self-service password reset functionality is accessed directly from the Windows logon dialog (integrated via GINA or credential provider link, depending on the operating system version), and remotely via Web browser.

Session and Application Management

- In “kiosk” environments, where a single workstation is shared by multiple users, such as hospitals, manufacturing floors or shipping facilities, and other “stand-up” environments in which a session is established with a non-user specific account, the ESSO Suite adds user-level granularity for session and application sign-on within the generic “parent” session.
- By providing a secure screen-saver layer within the “parent” session, the ESSO Suite allows a user to maintain their workstation session state until another user logs on or a time-out period expires, at which point data can be automatically saved and application sessions logged off and the applications themselves terminated, as enforced by the administrator-configurable policy.

Local and Remote Application Credential Provisioning

- Allows administrators to use an Oracle or third-party identity management systems to add, modify, and remove credentials from users’ ESSO profiles, eliminating the need for manual client-side provisioning by the end-user and thus calls to help desk.
- Accepts provisioning instructions via SPML from most major identity management systems, as well as custom applications or scripts.
- If no identity system management is in place, application credentials can be provided by the end-user on their local machine.

Strong Authentication Inside and Outside of the Session

- In addition to standard Windows password and LDAP directory-based authentication, ESSO-LM accepts user authentication from strong authentication devices such as smart cards, proximity cards, and fingerprint scanners.
- With the addition of ESSO-UAM, the above strong authentication methods can also completely replace the standard Windows password method, further tightening the security of your network.

Event Reporting

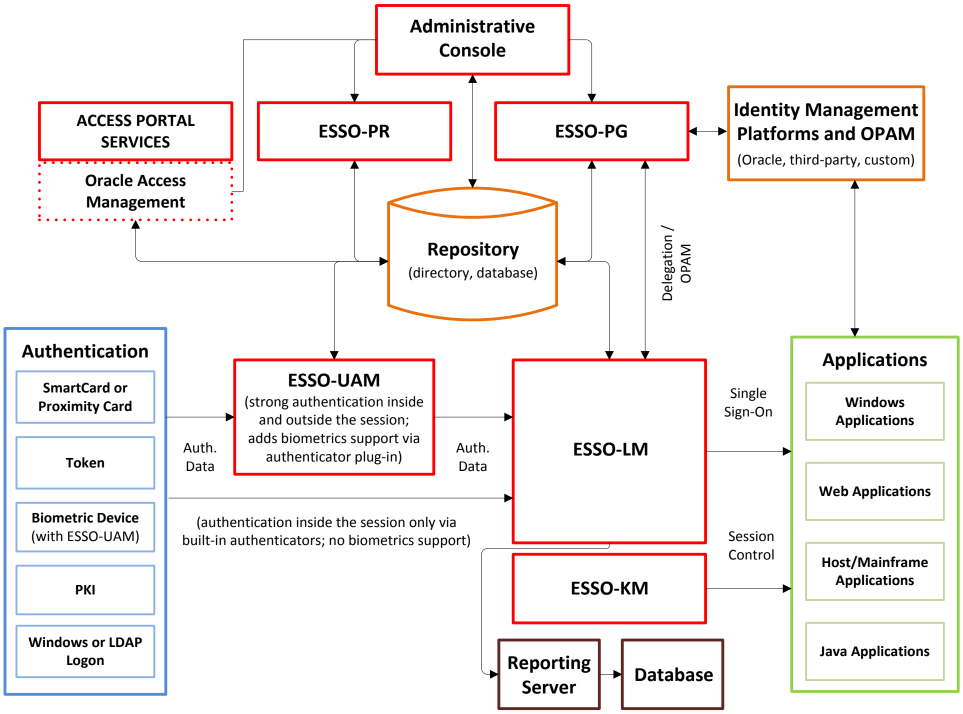
- The ESSO Suite Reporting component of the ESSO Suite provides the ability to generate customized reports on events that routinely take place in the day-to-day usage of ESSO Suite applications such as application logon, credential capture, password change, and so on. Data is stored in a central database; reports can be generated remotely via a Web interface.

ESSO Suite Components

The 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 the self-service password reset ability.
- **ESSO Provisioning Gateway (ESSO-PG)** – automatically distributes credentials systems to the ESSO-LM client
- **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** – captures event data and stores them to a remote database.

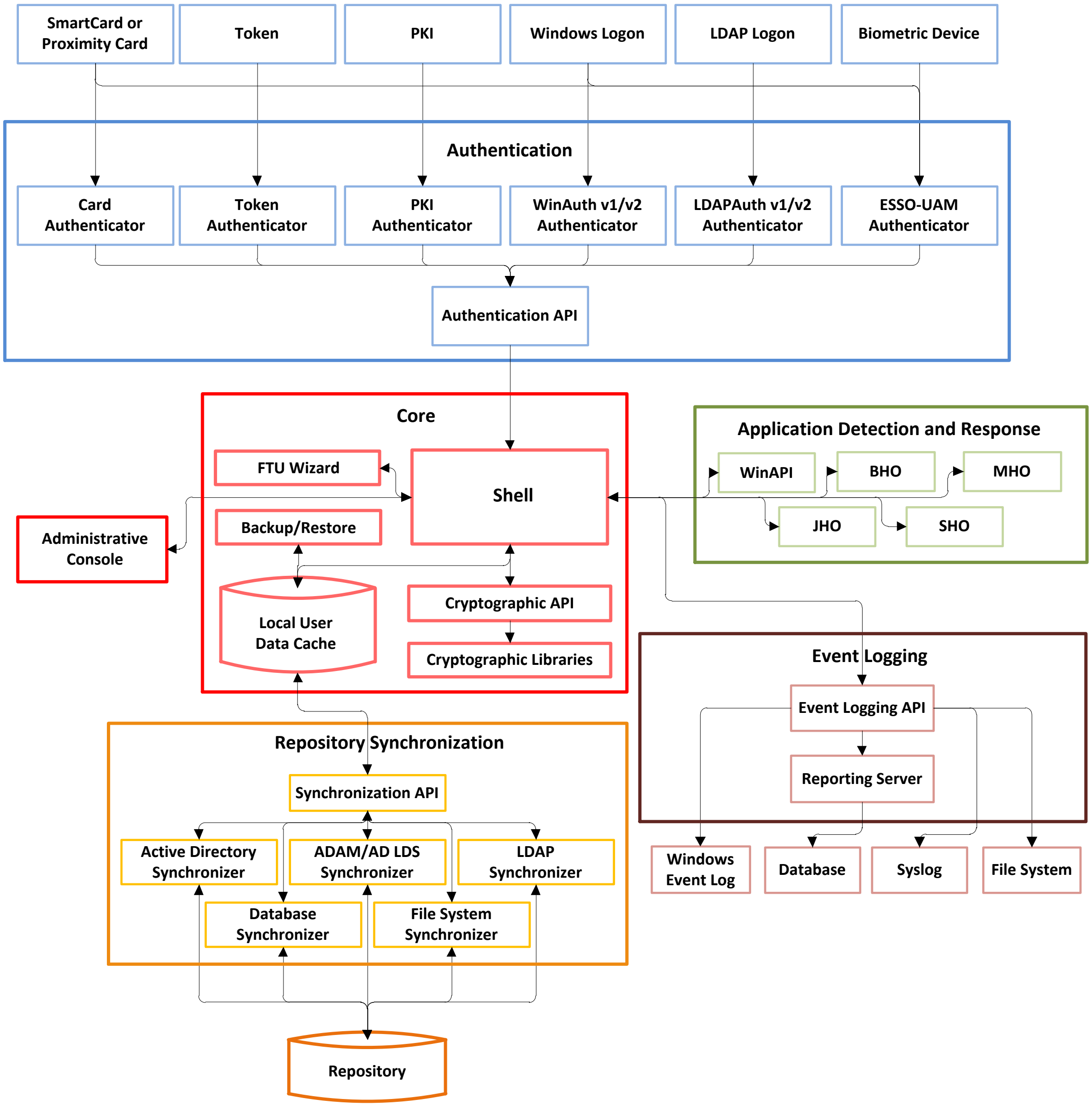
The interaction of the above components is shown below:


Administrative Console
ACCESS PORTAL SERVICES
Oracle Access Management
ESSO-PR
ESSO-PG
Identity Management Platforms and OPAM
(Oracle, third-party, custom)
Repository
(directory, database)
Delegation / OPAM
Authentication
SmartCard or Proximity Card
Token
Biometric Device (with ESSO-UAM)
PKI
Windows or LDAP Logon
Auth. Data
ESSO-UAM
(strong authentication inside and outside the session; adds biometrics support via authenticator plug-in)
Auth. Data
(authentication inside the session only via built-in authenticators; no biometrics support)
ESSO-LM
ESSO-KM
Single Sign-On
Session Control
Applications
Windows Applications
Web Applications
Host/Mainframe Applications
Java Applications
Reporting Server
Database

ESSO Logon Manager (ESSO-LM)

ESSO-LM provides the single-sign on capability of the ESSO Suite. This section describes the following aspects of ESSO-LM's architecture (illustrated in the diagram below):

- Authentication
- Intelligent Application Response
- Local User Data Cache
- Cryptography
- OIM and ID Context Integration
- Synchronization with a Repository
- Event Logging and Reporting



Authentication

ESSO-LM's user authentication mechanism validates the user's privilege to access to the individual credential store and other ESSO-LM functions. It consists of the layers listed below.

Authenticator

An authenticator accepts and collects proof of user's identity using a supported mechanism or protocol, such as Windows password, an LDAP identity, a proximity card or SmartCard, or a biometric solution. It then passes this data to the authentication service for validation.

ESSO-LM supports the following authentication methods out of the box:

- Microsoft Active Directory (Windows domain) account (including two-factor authentication)
- LDAP Directory Account
- SmartCard/proximity card

ESSO-LM, via its built-in authenticators, can consume authentication events and validation data from external authentication infrastructures such as SmartCards, proximity cards, and tokens, provided the appropriate middleware has been installed and configured on the target machine, and with the addition of ESSO-UAM, ESSO-LM gains the ability to use biometric solutions such as fingerprint scanners via the ESSO-UAM authenticator plug-in.

Authenticators can be assigned a grade so that different authentication methods carry a different weight when accessing ESSO-LM and applications that have been provisioned for single sign-on. Once grades are assigned, the administrator can restrict ESSO-LM's response to each application by authenticator grade - for example, ESSO-LM will only respond to an application if the user has signed on to the Windows session with an authentication method carrying a minimum weight of 2. If this requirement is not met, ESSO-LM will prompt the user to authenticate with another method whose grade satisfies the restriction present in the application's template; if the user is unable to authenticate with a sufficient grade, the sign-on request is aborted.

Authentication Service

The authentication service validates the user's identity received from the authenticator against its own credential store or external authentication mechanisms such as a Windows domain, strong authentication solution middleware, or a PKI. If the proof of identity is successfully validated, the authentication service notifies ESSO-LM via the authentication API that the user has been cleared for access.

Note: An authentication service that normally validates against a networked resource such as a Windows domain or a directory can support "disconnected" mode (if fully conformant to the ESSO-LM authentication API) allowing users to access ESSO-LM credentials and features even when not on the corporate network.

Authentication API

The authentication API provides the programmatic interface for the authentication service to interact with ESSO-LM. Thanks to this layered structure, custom authenticators and authentication services can integrate with ESSO-LM via the authentication API. For more information, contact Oracle Support.

> **Note:** Custom authentication code must be digitally signed by Oracle in order to be recognized by ESSO-LM; such digital signature does not constitute support of the custom code by Oracle.

Intelligent Application Response

When an application presents the user with a logon or password change screen, ESSO-detects this event and responds with the appropriate action. ESSO-LM follows the configuration stored in the application template to determine how to interact with the fields and controls in the form. Typically, ESSO-LM does the following:

At a high level, ESSO-LM does the following during a typical sign-on event:

1. Detects the application and loads the first template that matches the application's attributes.
2. (Optional) Performs the actions, such as setting field focus, which might be required by the application to invoke or activate the logon or password change form.
3. Does one of the following:
   - For a logon, retrieves the associated credentials from the user's store (if they exist) and populates the appropriate fields. (If the credentials don't exist, the Agent prompts the user to store them.)
   - For a password change, retrieves the old password from the user's store, generates a new password adherent to the administrator-configured password generation policy, and populates the appropriate fields. (If the administrator configured ESSO-LM not to generate a password for the application, ESSO-LM prompts the user to provide a new password.)
4. Performs the actions necessary to submit the credentials to the application for processing, such as pressing the **Submit** button.
5. (Optional) Detects any follow-up forms or dialogs, such as new password confirmation, and performs the required action.

ESSO-LM can be configured to detect and respond to a wide range of sign-on events, such as logon, password change, and variations of thereof; support is provided for a diverse range of forms, fields, controls, and event flows. A separate internal component is dedicated to each supported application type:

- **ESSO-LM core** – provides support for Windows applications
- **Browser Helper Objects (BHOs)** - provides support for Web applications accessed via the Microsoft Internet Explorer, the Mozilla Firefox, and the Google Chrome web browsers.
- **Mainframe Helper Object (MHO)** – provides support for host/mainframe applications running within a supported terminal emulator.

- **SAP Helper Object (SHO)** – provides support for SAP applications.
- **Java Helper Object (JHO)** – provides support for Java applications running within a supported Java Runtime Environment (JRE).

ESSO-LM identifies each application requesting logon or password change by a set of attributes that uniquely identify the application window and its fields and controls with which ESSO-LM interacts. These attributes are stored locally in the user's ESSO-LM data store as well as centrally in the repository and synchronized whenever an application template is updated by the administrator.

When ESSO-LM successfully identifies an application window and the target fields and controls, it retrieves the appropriate encrypted credentials from the user's data store, decrypts and injects them into the target fields and submits them to the application for processing. The decrypted credentials are never stored on disk and are wiped from memory immediately after the application response even is complete.

ESSO-LM uses the Windows API and helper objects tailor-made for each supported application type to programmatically interact with most applications, eliminating the possibility of credentials being captured by a keylogger or injected into the wrong application when the user inadvertently switches application focus.

The detection and response process for each of the supported application type (Windows, Web, and host/mainframe) is described below.

Windows Applications

ESSO-LM provides single-sign on functionality to virtually all Windows applications. Standalone Java applications running on Java are also supported in this mode.

ESSO-LM uses WinAPI calls to identify each Windows application requesting logon or password calls by a set of attributes which include window title and class, process name, and control IDs of the target fields and controls. ESSO-LM also supports matching for specific text displayed in the target window or dialog that uniquely identifies it to ESSO-LM. The Java helper object (JHO) is used to interface with standalone Java applications via their host JRE.

For detailed information on Windows application detection and response, see the guide *ESSO-LM Best Practices: Template Configuration and Diagnostics for Windows Applications* available from the ESSO Suite documentation Web page.

Web Applications

ESSO-LM provides single sign-on functionality to most Web applications accessed via Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome Web browsers. Java applications running inside those browsers are also supported.

ESSO-LM uses the browser-appropriate helper object to interface with the Web browser and identify each Web application requesting logon or password change by a set of attributes which include the page's URL, DOM (Data Object Model), and HTML element IDs for the target fields and controls. ESSO-LM also supports matching for specific text or HTML code that uniquely identifies the page.

For detailed information on Web application detection and response, see the guide *ESSO-LM Best Practices: Template Configuration and Diagnostics for Web Applications* available from the ESSO Suite documentation Web page.

Host/Mainframe Applications

ESSO-LM provides single sign-on capability for mainframe/host applications accessed via a terminal emulator. A terminal emulator is an application that establishes a terminal session from the user's Windows workstation to a multi-user mainframe system over a variety of protocols, including IBM 5270/5050, Telnet, SSH, and so on. ESSO-LM uses the mainframe helper object (MHO) to interface with the supported terminal emulators via HLLAPI and interact with the target application within the emulator session. Applications running inside a Windows command-line sessions are supported; the PuTTY terminal emulator is also supported.

ESSO-LM identifies each terminal-based application requesting logon or password change by a set of attributes which include the emulator's window title and class, process name, and session short name. Once an active session is detected, ESSO-LM scans the terminal screen with each HLLAPI event (such as screen redraw or keystroke) looking for specific text at specific coordinates, both configured in the application template by the administrator. Both fixed-screen and scrolling-screen applications are supported; ESSO-LM also supports variable column (horizontal) field positioning.

For detailed information on mainframe/host application detection and response, see the guide *ESSO-LM Best Practices: Template Configuration and Diagnostics for Web Applications* available from the ESSO Suite documentation Web page.

Local User Data Cache

When the user completes the First-Time Use wizard, ESSO-LM generates a primary key which is used to encrypt the user's credential store both locally and in the repository. Thereafter, whenever an application requests logon or password change and credentials for that application exist in the user's credential store, ESSO-LM decrypts them to memory, injects them into the application, and wipes them from memory when the sign-on event completes. While the credential store is cached locally in the user's Windows profile, credentials are never stored in unencrypted form on disk.

The local copy of the credential store, sometimes referred to as the user's "local cache," is a permissions-protected folder in the user's Windows profile storing encrypted files containing the user's credentials. The files are encrypted with the user's unique primary key and cannot be decrypted by others. In addition to credentials, the user's local cache also stores copies of the most recent administrative overrides, password generation policies, authentication policies, and other configuration items synchronized from the repository (if applicable).

The main benefit of the local cache is the ability for ESSO-LM to operate in "disconnected" mode, providing single-sign on ability for users who temporarily cannot connect to the corporate network. The local cache also relieves the repository from continuous requests for user data; instead, the data is synchronized periodically between the user's machine and the repository, minimizing server load.

Cryptography

ESSO-LM supports all major symmetric encryption algorithms for securing the user's credential store both locally and in the repository, allowing organizations to meet enterprise-wide security/audit requirements and/or comply with government regulations.

By default, ESSO-LM uses MSCAPI-compliant AES encryption that is fully conformant with FIPS 104-2. Support for legacy algorithms such as, 3DES, has been deprecated in this version yet is provided in case backwards compatibility is needed. Additionally, ESSO-LM's encryption API enables the substitution of practically any other symmetric encryption algorithm.

To secure both the user authentication data and the user's credential store, during initial enrollment, ESSO-LM generates a primary authentication key that is both cryptographically unique and authenticator-independent. The availability of this key is contingent upon the user's successful completion of the ESSO-LM's First-Time Use (FTU) wizard, at which point it can be used to secure user data.

The data remains encrypted at all times, including in the agent's local cache, the directory, and while in transit over the network. ESSO-LM only decrypts credentials (to memory, never to disk) when a configured application requests logon, and wipes the target memory location as soon as the logon request completes.

To generate all random authentication data such as encryption keys or new passwords (adherent to administrator-configurable password generation policies), ESSO-LM uses Microsoft CAPI RNG and RSA CSPs.

OAM and ID Context Integration

As part of the integration between OAM and Oracle Enterprise Single Sign-On ESSO can publish and propagate client-based Identity Context attributes. Once the normal integration has been configured, client-specific claims payload will be sent by ESSO to OAM in the session initiation request together with the user credentials (as if submitted by the user using a browser to access a web resource protected by OAM).

During the request, ESSO makes a call to SSL-protected OAM REST API that was previously configured by the ESSO administrator and made part of the ESSO client distribution.

ESSO provides OAM credentials (acceptable to the OAM Embedded Credential Collector) as well as client-based Identity Context information in the payload. OAM provides ESSO with a valid OAM_ID cookie that is propagated to the client browsers (IE, Firefox, Google Chrome). This OAM_ID cookie enables SSO resources protected by the OAM Embedded Credential Collector. Note that this OAM_ID does not enable SSO with resources protected by the OAM Distributed Credential Collector at this time. When the ESSO Session times out, the ESSO LM client removes the OAM_ID cookie from the browsers to end the OAM session.

Synchronization with a Repository

One of ESSO-LM's key strengths is its ability to store and synchronize application credentials, administrative overrides, and configuration and security (such as password generation or authentication) policies centrally in a repository, allowing users to enjoy the benefits of single sign-on from any workstation on the enterprise network.

ESSO-LM supports Oracle Directory Servers (OID, ODSEE, OUD), Microsoft Active Directory, Microsoft ADAM/AD-LDS, and most other LDAP-compliant directories (such as products from IBM and Novell) , as well as SQL databases and local or networked file systems. Additionally, ESSO-LM exposes a record-level synchronization API allowing integration with custom systems and devices. For users who cannot synchronize with a repository at all, ESSO-LM offers a secure local credential backup and restore mechanism.

Whenever synchronization is triggered (as decided by the administrator - usually when ESSO-LM starts, or when a credential is added, modified, or deleted), ESSO-LM compares the data stored in the local cache to that stored in the repository and replaces older credential records with updated copies in both directions. Note that while synchronization of credentials is bidirectional, configuration and security policies in the repository always take precedence over those cached locally by ESSO-LM and constitute the "domain" policy for ESSO-LM. Since the local cache is tamper-proof thanks to encryption and thus immune to user alterations, synchronization allows for secure enterprise-wide enforcement of ESSO-LM configuration and security policies, both on a per-user and/or a per-group basis.

The administrator can choose whether only the changes or the entire user data store is synchronized each time to manage network load in high user count scenarios. For more information on repository synchronization, see the ESSO-LM deployment best practices guide (available from the ESSO-LM documentation Web page) applicable to your target platform.

Event Logging and Reporting

ESSO-LM offers extensive event logging, auditing, and reporting features, logging virtually all ESSO-LM and other ESSO Suite application events either in the Windows Event Log, Syslog, a local file, or remotely in a database for BI Reporting (via the ESSO Reporting component) or a networked file system. Additionally, events can be captured and delivered through a custom mechanism to external destinations via the ESSO-LM event logging API – for example, an SNMP service, a Windows Event Log, a database, or custom logging system.

Access Portal

The Access Portal Service is an Oracle Access Management Service that provides a web-based logon manager that enables cross-platform single sign-on to web-based applications, without requiring any client components. The Access Portal utilizes secure REST interfaces to access ESSO application and configuration stores and proxy technology to replace the traditional ESSO-LM client.

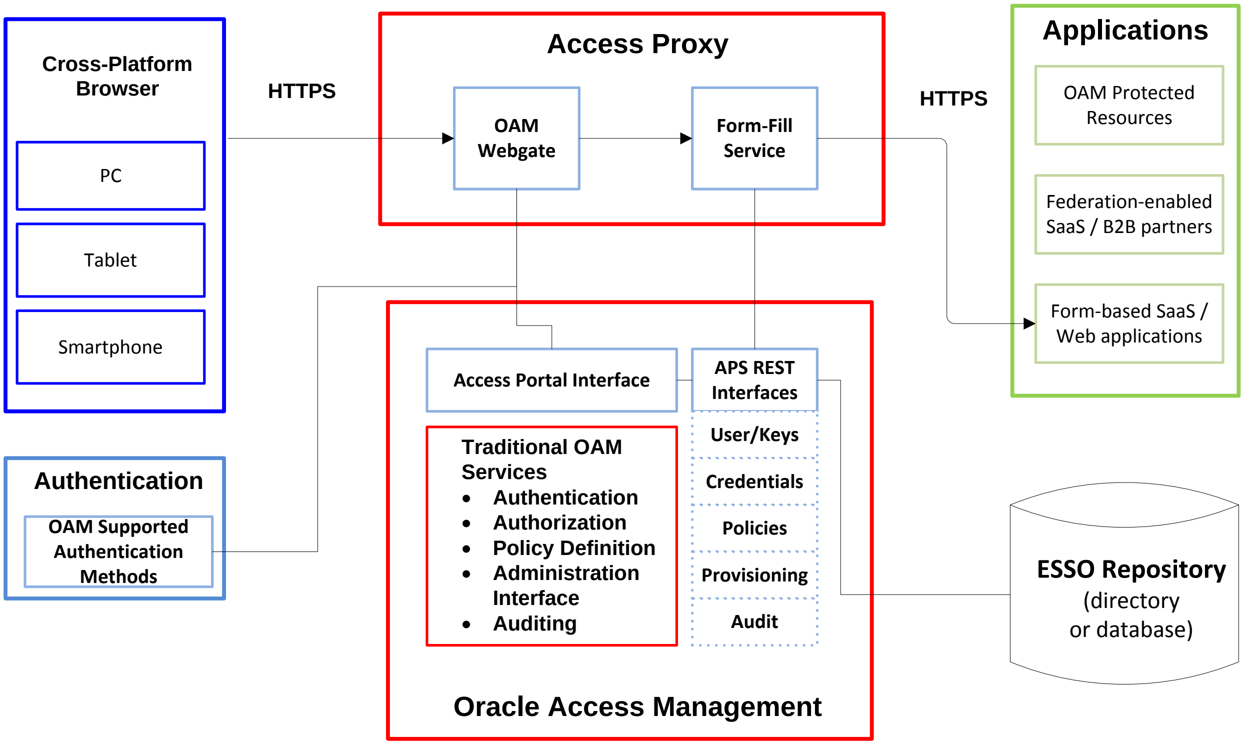
Oracle Access Management is responsible for authentication and authorizing access to the Access Portal service.

A customizable user interface interacts with the REST interfaces and acts as cross-platform presentation layer to ESSO application configurations and credential store.   These same interfaces can also be accessed by 3rd-party developed user interfaces.

A number of different application types are supported, including:

- **Oracle Access Management protected resources.** Provides links to Oracle Access Management (OAM) protected resources. With this type of application the Access Portal simply represents OAM protected URLs. Authentication is handled by standard OAM authentication and session management.
- **Federated Applications.** Provides a link to federated partners and resources. The administrative wizard for federated applications allows an administrator to select existing Oracle Identity Federation trusted B2B partners and SaaS applications. The wizard requests additional information such as the target application to automatically generate an IDP-initiated link as a configured application.
- **Form-Fill Applications.** Provides form-based single sign-on via the Access Portal proxy service. Administrator use standard ESSO template generation wizards to create form-fill templates for required web-based applications and non-federation enabled SaaS applications.

The following diagram represents the high-level architecture for the Access Portal Service (APS):



ESSO Password Reset (ESSO-PR)

ESSO-PR delivers a secure and easy to use self-service Windows password-reset and Windows account unlock solution, reducing helpdesk costs and improving user experience by enabling strong password management for Microsoft Windows through a secure, flexible, self-service interface.

The interface is accessed using a link that appears in the standard Windows logon screen after the ESSO-PR client software is installed on the end-user machine. Depending on the end workstation technology, ESSO-PR either utilizes a GINA stub or a Credential Provider to provide the link. (If the user has not yet enrolled with ESSO-PR, the interface also provides the ability to do so, which can be enforced by the administrator by limiting the number of allowed enrollment cancellations.)

When a user exceeds their allowed number of password reset or account unlock attempts, instead of calling help desk, the user can unlock their account or reset their password by answering a series of administrator-configurable challenge questions. Questions and answers can be either specified by the administrator and stored directly within the ESSO-PR data store or retrieved dynamically via standard APIs from external systems, such as HR databases. Furthermore the ESSO PR Client can direct a user to the OIM KBA authentication engine to facilitate change password via that system.

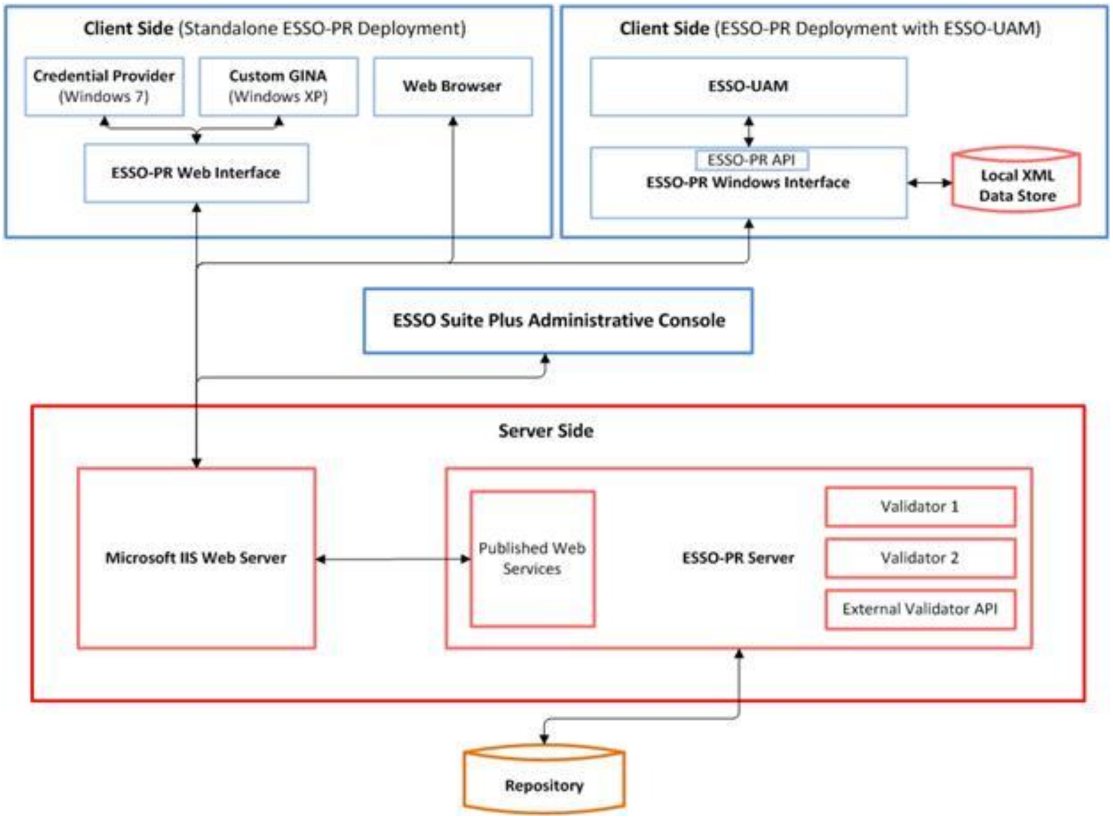
The weight of each question can be individually configured by the administrator using ESSO-PR's confidence-based rating system so that one question can count more towards granting the user access than another. Correct answers add to the user's quiz core, while incorrect answers subtract from it but not necessarily disqualify the user. Once the user correctly answers enough questions to pass the quiz, access to the account unlock and/or password reset functionality is granted.

ESSO-PR groups challenge questions into the following categories:

- **Required questions.** These are questions for which all users should have unique, fact-based answers – for example, a social security number or date of birth. Required questions usually have a high and equal weighting for both correct and incorrect answers, and should be as diversified as possible.
- **Eliminator questions.** These questions are designed to immediately disqualify an unauthorized user because their nature makes it highly unlikely for the unauthorized user to know the answers, which should be personal and unique to the authorized user. Eliminator questions should have low or zero point value for correct answers and high negative point value for incorrect answers.
- **Optional questions.** These questions do not apply to every user and therefore should be used to target specific groups within the enterprise. They are often preference-based questions which could change over time and are not highly weighted for either correct or incorrect answers.

The administrator can assign individual questions to specific users or groups using the ESSO-PR Administrative Console.

The following diagram represents the architecture for ESSO-PR at a high level



ESSO Provisioning Gateway (ESSO-PG)

ESSO Provisioning Gateway (ESSO-PG) allows administrators to remotely provision application credentials for ESSO-LM users via external identity management systems such as Oracle Identity Manager using the Simple Provisioning Markup Language (SPML). This method seamlessly and automatically grants users single sign-on access to the target application without the need for ESSO-LM to capture credentials on the end-user machines. Additionally, ESSO-PG is used for Credential Delegation with ESSO-LM users, and for ESSO-LM to check out and check in credentials managed by Oracle Privileged Account Manager (OPAM).

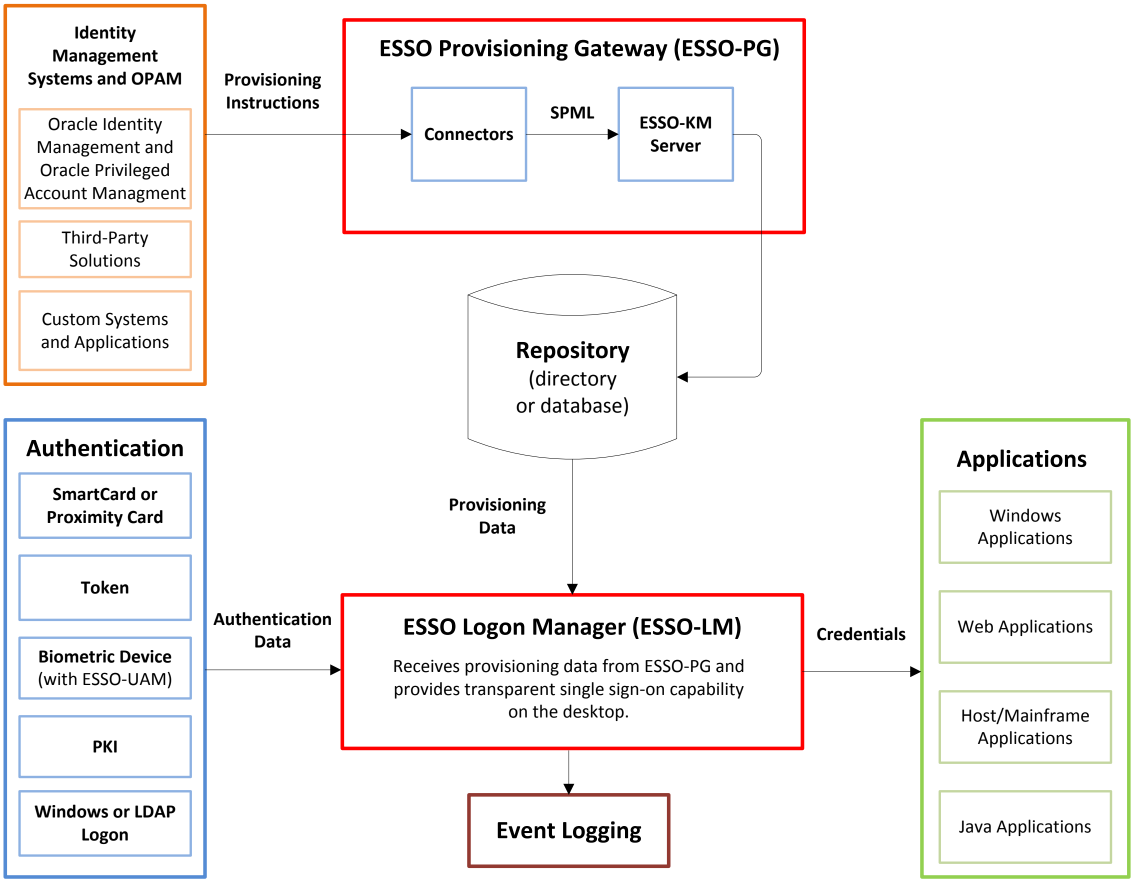
ESSO-PG supports the addition of new user accounts, as well as the addition, modification, and deletion of application credentials within each user account. Once the provisioning instructions are delivered to ESSO-PG from an external system, delegation or privileged account checkouts, ESSO-PG deposits them, encrypted with the user’s unique key, within the individual user containers in the ESSO-LM repository and ESSO-LM makes the necessary modifications to the user's credential store during the next repository synchronization event.

ESSO-PG is also leveraged to securely support user-to-user delegated credentials. An end user can elect to give access to their application accounts to another user. In doing so, they create their own provisioning instruction to the user receiving the credential. The delegating user can control whether or not the receiving user can reveal the password once they have access to it. The account will be removed from the user the received the access through a deletion instruction that is either generate manually by pressing the revoke button or systematically through and account timeout mechanism.

ESSO-PG is also used as a checkout/check-in interface for Oracle Privileged Account Manager (OPAM). An authorized end user can request access to privileged application accounts through ESSO-LM. Upon approval and availability release, a provisioning instruction will be sent from the OPAM server to ESSO-PG. OPAM policies will control whether the user can reveal the privileged credential, or just use it through the ESSO-LM functionality. A user may check-in the credential manually, or the credential can automatically be checked back in after an OPAM policy-defined period of time. Please see the Oracle Privileged Account Manager documentation for more details on OPAM.

ESSO-PG can be administered either via the supplied Web console or command-line interface (if scripting is desired), or via its .NET API, which allows ESSO-PG to interface with custom provisioning solutions and data sources using connector modules. Connectors for major commercial systems such as Oracle Identity Manager, Oracle Privileged Account Manager, IBM Tivoli Identity Server, and several others are supplied with ESSO-PG and are implemented as workflow steps that merge with the respective system's provisioning workflow, intercepting the provisioning event and data from the workflow and supplying a copy to ESSO-PG.

The diagram below describes the functioning of ESSO-PG at a high level:


Identity Management Systems and OPAM
Oracle Identity Management and Oracle Privileged Account Managment
Third-Party Solutions
Custom Systems and Applications
Provisioning Instructions
ESSO Provisioning Gateway (ESSO-PG)
Connectors
SPML
ESSO-KM Server
Repository (directory or database)
Provisioning Data
Authentication
SmartCard or Proximity Card
Token
Biometric Device (with ESSO-UAM)
PKI
Windows or LDAP Logon
Authentication Data
ESSO Logon Manager (ESSO-LM)
Receives provisioning data from ESSO-PG and provides transparent single sign-on capability on the desktop.
Credentials
Applications
Windows Applications
Web Applications
Host/Mainframe Applications
Java Applications
Event Logging

ESSO Kiosk Manager (ESSO-KM)

ESSO Kiosk Manager (ESSO-KM) adds user-level granularity for session and application sign-on and state in "kiosk" environments - hospitals, manufacturing or shipping facilities, and other “stand-up” environments in which a single workstation is shared by multiple users - in which a session is established with a non-user specific account. By running as a secure screen-saver inside the generic "parent" session, ESSO-KM allows the user to maintain their workstation session state until another user logs on or a time-out period expires, at which point data can be automatically saved and application sessions logged off and the applications themselves terminated, as enforced by the administrator-configurable policy.

ESSO-KM consists of three major components:

- **ESSO-KM GINA stub**, which chains to the Microsoft GINA to enable user logon and prevents end-users from circumventing the logon requirement by shutting down ESSO-KM. (ESSO-KM does not replace the Microsoft GINA.)
- **ESSO-KM Session Agent**, which monitors session activity, grants access to the kiosk, displays a screen-saver that informs other users about the session state, and executes actions whenever a session event occurs as configured by the administrator.
- **ESSO-KM Desktop Manager**, which starts and stops the ESSO-KM secure screen-saver which obscures the Windows desktop until a user successfully authenticates to ESSO-KM.

ESSO-KM supports the following session states:

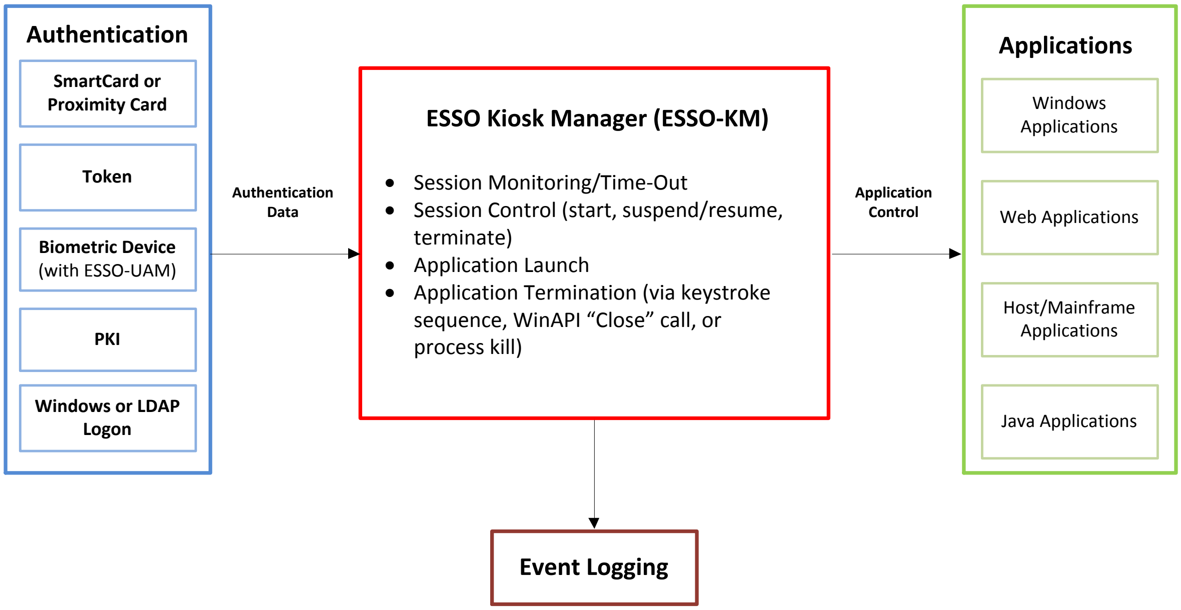
- **Active,** where the user is actively working on the kiosk.
- **Suspended,** where the user is logged on but the SM secure screensaver is running to prevent anyone else from accessing the user’s information.
- **Null,** where there is no user logged onto the kiosk, usually directly after the machine has finished starting up, or when a suspended session is terminated after an inactivity timer has elapsed.

ESSO-KM recognizes the following session events:

- Session start, end, suspend, and resume
- Authenticator removal and timeout
- Application run and terminate
- External application call

The administrator specifies the action ESSO-KM should take on each session event - for example, terminate any applications left open by the previous user in a manner specified in the application template (e.g., using the Windows "Close" function, by killing the application process, or a series of keystrokes and mouse-clicks to save open data), and then run one or more applications required by the current user.

The following diagram illustrates the functioning of ESSO-KM at a high level:


Authentication
SmartCard or Proximity Card
Token
Biometric Device (with ESSO-UAM)
PKI
Windows or LDAP Logon
Authentication Data
ESSO Kiosk Manager (ESSO-KM)
Session Monitoring/Time-Out
Session Control (start, suspend/resume, terminate)
Application Launch
Application Termination (via keystroke sequence, WinAPI "Close" call, or process kill)
Application Control
Applications
Windows Applications
Web Applications
Host/Mainframe Applications
Java Applications
Event Logging

ESSO Universal Authentication Manager (ESSO-UAM)

ESSO-UAM is a strong-authentication solution that replaces the standard Windows logon mechanism with a SmartCard, proximity card, token, or a biometric logon method (Windows password remains available as a logon option once ESSO-UAM is installed). Once configured, any of these methods can be used to authenticate to ESSO-LM through the ESSO-UAM authenticator which is installed by the ESSO-UAM installer when ESSO-LM is detected on the target system.

Users can easily enroll strong authentication devices with ESSO-UAM and use them to log on to and unlock their Windows workstations while administrators can deploy security policies on a per-user or per-group level to ensure that enterprise-wide security requirements are strictly enforced.

ESSO-UAM supports the following logon methods:

- **Fingerprint** – enables the enrollment and use of third-party fingerprint scanners, such as external USB scanners and scanners built into laptop computers. Requires a supported biometric reader device and the BIO-key BioAPI Biometric Service Provider (BSP) to be installed and configured on the end-user workstation. Administrators can configure up to ten fingerprint samples for enrollment.

- **External BSP (via BioAPI)** – enables the enrollment and use of a third-party BioAPI-compliant Biometric Service Provider (BSP) modules, including fingerprint, palm, retina/iris scanners and facial feature analyzers. Requires a supported biometric device and BioAPI-compliant BSP middleware to be installed and configured on the end-user workstation.

- **Smart Card (with or without PIN)** – enables the enrollment and use of SmartCards. ESSO-UAM does not modify the card's contents in any way – existing card data is associated with the user's account during enrollment and subsequently used for authentication once enrollment is complete. Additionally, the PIN present on the card can be enforced if two-factor authentication is desired.

- **Proximity Card (with or without PIN)** – allows the enrollment and use of RFID and other proximity cards. Additionally, a PIN can be defined and enforced if two-factor authentication is desired.
- **Knowledge Based Authentication** – allows the user to enroll and gain access to a system through a question and answer solution. This gives users a fall back authentication in the event of a lost or broken strong authentication device.

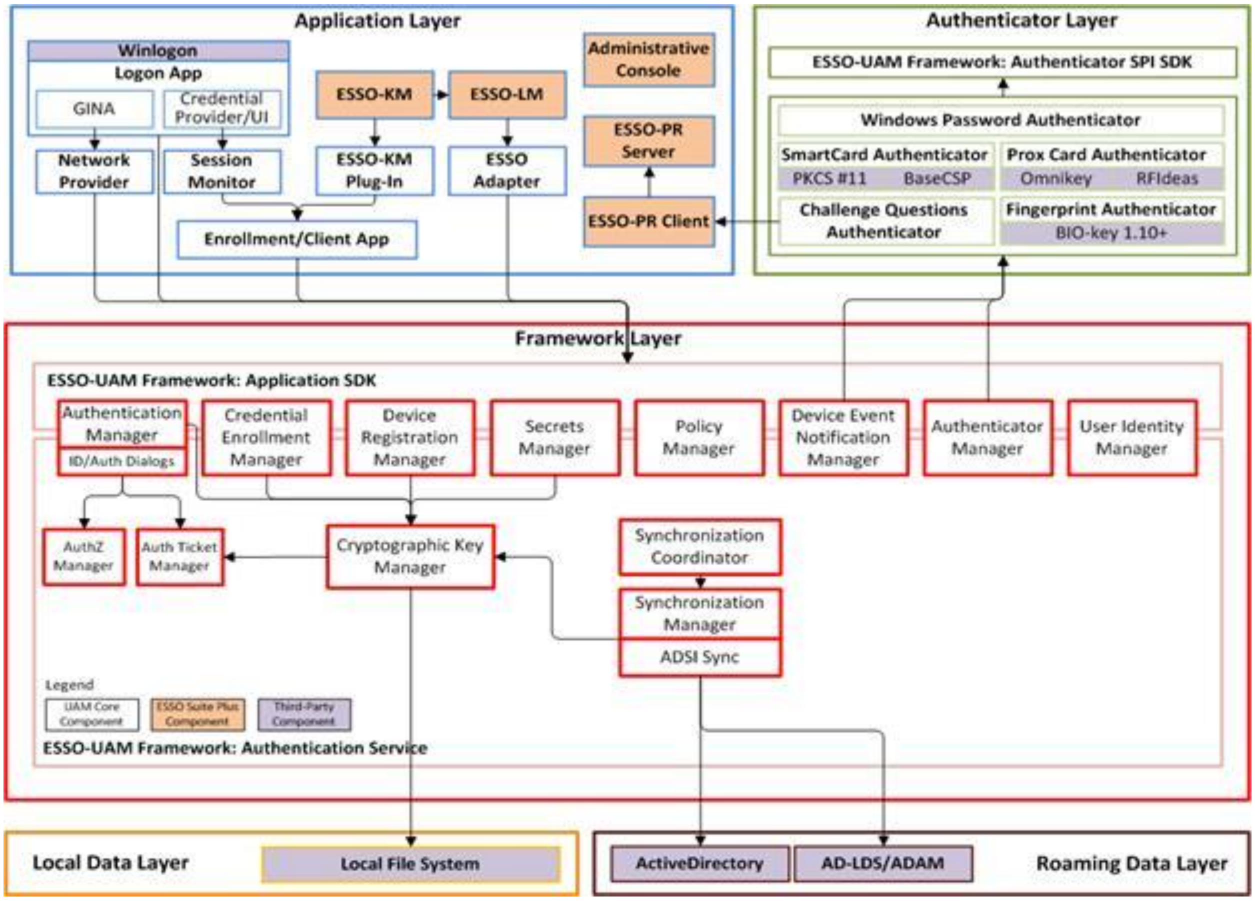
ESSO-UAM can be deployed in either local mode or enterprise mode. In local mode, ESSO-UAM configuration is configured and stored in the user's secure local cache on the user's workstation, while in enterprise mode ESSO-UAM configuration is synchronized with the ESSO-UAM repository and configured remotely by the administrator.

While in enterprise mode, the administrator can configure ESSO-UAM security policies on a per-user or per-group basis and deploy them enterprise-wide to override any ESSO-UAM settings configured locally by the end-user, allowing for automatic and robust enforcement of enterprise security guidelines. Once synchronized, enterprise security policies remain in effect even if the end-user workstation disconnects from the repository.

The following options are available for enforcement in each policy:

- Target user or group
- Enable/disable each logon method
- Prompt for enrollment on session start if not enrolled
- Enrollment grace period
- Number of fingers (built-in fingerprint authentication only)
- PIN required (SmartCards/proximity cards only)
- PIN minimum length and allowed characters (proximity cards only)
- Removal action (what happens when logon method is activated inside a session)

The following diagram provides a high level overview of ESSO-UAM:



ESSO Anywhere

ESSO-Anywhere provides a way to deploy Oracle Enterprise Single Sign-on Logon Manager (ESSO-LM) and Oracle Enterprise Single Sign-on Provisioning Gateway (ESSO-PG) to end users without administrator intervention, facilitating faster and more cost-effective deployment, and automating version control of deployment packages. The administrator configures ESSO-LM (and optionally ESSO-PG) locally, creates a deployment package, and then distributes it via a networked solution such as a Web server or a file share. Users can then download ESSO-Anywhere and perform the installation with certainty that the configuration is exactly as it should be.

ESSO Reporting

The Reporting component of the 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 ESSO Suite applications.

The reporting sub-system consists of the following components:

- **Centralized database** – stores all event data from which reports can be generated.

- **BI Publisher reporting console** – accesses the SQL and Oracle database and generates reports from the stored event data.
- **Reporting service** – collects audit/reporting events into the database.
- **ESSO Suite applications** - capture event information and send the data to the reporting service.

Terms and Abbreviations

The following table describes the terms and abbreviations used throughout this guide:

Term or Abbreviation	Description
ESSO-LM	Enterprise Single Sign-on Logon Manager
ESSO-PR	Enterprise Single Sign-on Password Reset
ESSO-PG	Enterprise Single Sign-on Provisioning Gateway
ESSO-KM	Enterprise Single Sign-on Kiosk Manager
ESSO-UAM	Enterprise Single Sign-on Universal Authentication Manager
ESSO Reporting	Enterprise Single Sign-on Reporting
ESSO-Anywhere	Enterprise Single Sign-on Anywhere
ESSO Suite	Enterprise Single Sign-on Suite Plus

Accessing Oracle ESSO Suite Documentation

We continually strive to keep our documentation accurate and up to date. For the latest version of this and other Oracle ESSO Suite documents, visit http://docs.oracle.com