



## Enterprise SSO Manager (E-SSO-M)

Many resources, such as internet applications, internal network applications and Operating Systems, require the end user to log in several times before they are empowered to carry out their work activities

**E-SSO-M** is a software solution that allows the end user to log into the network only once and automatically gain access to all applications and resources.

### How does it work??

E-SSO-M operates as an extra layer of software, which processes all the login dialogues for the end user. It generates an automatic entry of the username and password. The end user only needs to remember one username and password eliminating subsequent login requirements.

### Benefits of E-SSO-M

Using E-SSO-M in an organization produces multiple benefits:

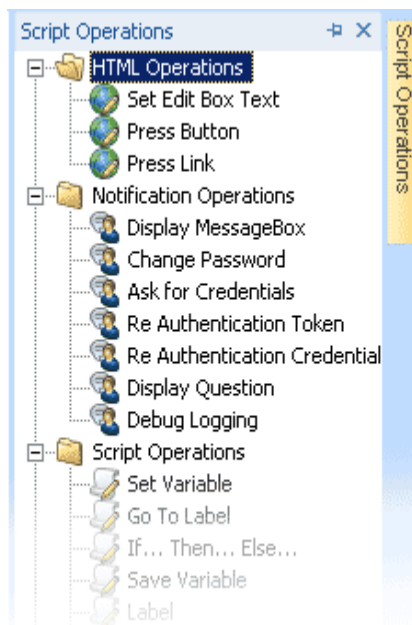
- **Convenience:** Some departments require employees to log into 15 applications or more. From normal LAN based applications to external internet applications, having E-SSO-M at your organization means that the end user no longer needs to log into several applications at the start of the work day.
- **Security:** E-SSO-M eliminates the need for users to remember multiple passwords. Instead, they can log in using one strong password. Most of us are familiar with the common end user workarounds associated with managing login information for several applications – sticky notes on a computer monitor, a piece of paper hidden under a keyboard, etc. These workarounds negate the very security policies that were meant to protect critical information. By eliminating these vulnerabilities and enhancing the security of the one password that does need to be remembered, E-SSO-M provides organizations with much more than a convenient means of access.
- **Compliance:** E-SSO-M works on several levels to guarantee compliance.
  - *Central access registration.* E-SSO-M operates as a central gateway to all applications. This allows multiple compliance options such as the ability to deny network access to a certain employee in one single SSO action rather than having to deny access throughout every application in the network.
  - *Integral reporting.* E-SSO-M can report both user account access and time of access into individual applications.
  - *Access restriction.* Before E-SSO-M logs into an application, it can perform several checks: can the application be accessed from this work station by the specific employee; has the Access Card been inserted into the reader; is the entered PIN code valid? The same system link that allows access to buildings also ensures that certain employees can only start up certain applications in certain rooms.

## Concept

The E-SSO-M concept is based on a successful and proven building block structure created by Tools4ever. The advantage of this concept is that new applications can be added to the list of existing E-SSO-M applications with increased speed and flexibility. The building block structure also allows system administrators to extend and adjust current templates.

## Templates

The E-SSO-M trial download contains a limited set of application templates. The Tools4ever department of professional services, however, creates a large library of templates to support many applications in an out-of-the-box way. Within a few days, an average E-SSO-M implementation of 1,500 end users and 20 applications is delivered by a Tools4ever consultant. After that, the system operator is free to make any desired template adjustments via the block building system.



### E-SSO-M Block building concept

Enterprise SSO Manager is revolutionary Single Sign-On solution, based on a building block concept that no other comparable product can match. This concept allows 100% guaranteed support of the application landscape and allows easy manipulation of both users and their applications.

Adding building blocks to a template is done via the user-friendly GUI drag-and-drop interface. After adding a building block to a template, several parameters of that building block can be redefined.

Future E-SSO-M options will include new actions to make templates more intelligent. Script actions provide for several types of functions: saving information in a database, applying extra access security (Smart Card), sending e-mail, etc. Since the building blocks have a modular structure, Tools4ever can easily add extra functionality to E-SSO-M. Development of building blocks can also be requested. If you are interested, please contact your nearest Tools4ever office.

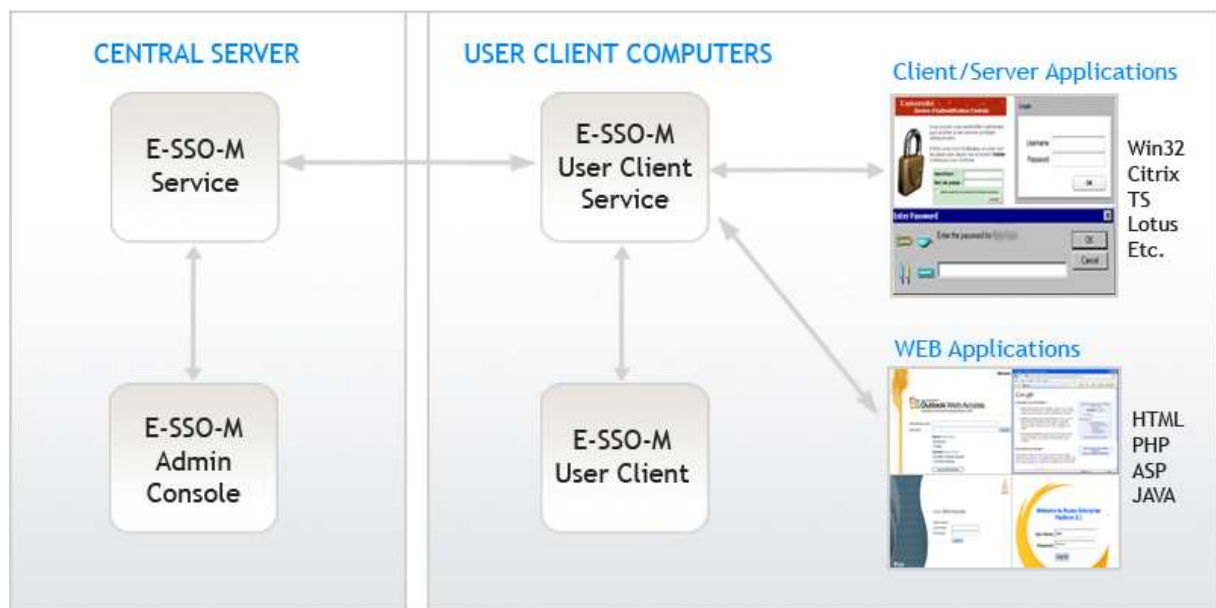
## E-SSO-M - Architecture

E-SSO-M is designed as a high-level enterprise solution to support very large networks that necessitate a reliable SSO solution. The diagram below shows an overview of the relationship between the various E-SSO-M modules.

SSO architecture supports a service that works as a central information point for all local SSO services available on each work station. At the E-SSO-M level, the system administrator can make central adjustments via the E-SSO-M Admin Console. This console defines and allocates application templates to employees or a group of employees. Specific settings, such as load balancing, high availability, delegation of control, etc., can be defined.

SSO user-client software is available for any work station and allows the end user to adjust E-SSO-M settings to his or her personal demands. For example, E-SSO-M can be switched off temporarily. User credentials can be erased for specific applications, delegated to a different user for predefined period of time etc.

A link to Windows and Browser applications is formed via a Windows Hook and a Browser Helper Object. This mechanism allows the SSO User Client Service to know exactly which dialogues are shown to which end users. This type of link is based on the published Microsoft standard, which guarantees correct functioning on any platform in any situation. Therefore a network consists of a hybrid environment with a terminal server, Citrix, XP, Vista, IE6 or Firefox, etc. All platforms are supported by E-SSO-M.



## E-SSO-M Scalability

Peak usage of an SSO application occurs in the morning, when most employees start working and must log into the network. Specifically, research has indicated that 96.5% of the utilization of an E-SSO-M application takes place during the first thirty minutes of the work day. During this time, the central E-SSO-M engine needs to supply data for all end users and their respective applications. In order to process these requests, E-SSO-M has a feature that allows for the login requests to be distributed amongst several Microsoft Windows Services. The license model allows an unlimited number of instances of the E-SSO-M service in the network. Networks of up to 250,000 work stations can be supported through this service model.

## E-SSOM-M High availability

Users will increasingly depend on the SSO solution. Therefore, E-SSO-M availability is crucial. E-SOM-M guarantees that, via various mechanisms, end users will always be able to utilize this software. A high level of availability is also crucial. The following mechanisms illustrate how this is possible:

- **Replication**  
User account credentials have been stored in a relational database. In order to guarantee safe storage of this data, standard means are available. Placing the database on a cluster server and/or database replication are strongly supported features with E-SSO-M.
- **Multiple services**  
The central engine of E-SSO-M is the Microsoft Windows Service. E-SSO-M contains a feature that allows multiple services to run. Information, with respect to end user credentials and configuration data (settings in E-SSO-M), are exchanged via a replicated database. E-SSO-M on an end user work station will automatically select the most available service. The license model allows an unlimited number of E-SSO-M services to operate.
- **Local caching**  
Local caching is supported if a work station cannot connect to the central E-SSO-M service. E-SOM-M has a feature that utilizes local work station caching a so-called offline mode. This feature fully supports laptop users who do not always connect to the company network yet still require E-SSO-M. The offline mode is also available in the unlikely event that the central E-SSO-M services are not available.

## E-SSO-M Security

In an SSO application, all employee usernames and passwords need to be stored. It is crucial that this data is well secured. E-SSO-M has been specifically designed to ensure the integrity of user account data.

- **Communication.**  
All information exchanged between the E-SSO-M componentry is encrypted. No readable text is communicated between the work stations and the central service.  
\* Caching. When a laptop is used, usernames and passwords are stored locally on the hard disk. This data is encrypted.
- **Database.**  
The central database stores a copy of every username and password. This too, is encrypted
- **Logging.** All end user activity is stored in the central E-SSO-M database, except for the username and password of the application in question. E-SSO-M has been designed by Tools4ever security experts so that sensitive information is exchanged and stored only when required.

The encrypted algorithm in E-SSO-M is based on DPAPI Security. Other encrypted algorithms can be applied in order to meet the required company security standard.

## DPAPI Security

DPAPI provides an essential data protection capability that ensures confidentiality of information while allowing for the recovery of underlying data in the event of lost or changed passwords. The password based protection provided by DPAPI is excellent for a number of reasons:

- It uses proven cryptographic routines such as strong Triple-DES algorithm in CBC mode robust SHA-1 algorithm, and PBKDF2 password-based key derivation routine.
- It uses proven cryptographic constructs to protect data. All critical data is integrity protected cryptographically, and secret data is wrapped using standard methods.
- It uses large secret sizes to greatly reduce the possibility of brute-force attacks to compromise the secrets.
- It uses PBKDF2 with 4000 iterations to increase the work factor of an adversary trying to compromise the password.
- It sanity checks MasterKey expiration dates.
- It protects all required network communication with Domain Controllers by using mutually authenticated and privacy protected RPC channels.
- It minimizes the risk of exposing any secrets by never writing them to disk and minimizing their exposure in swappable RAM.
- It requires Administrator privileges to make any modification to the DPAPI parameters in the registry.
- It uses Windows File Protection to help protect all critical DLLs from online changes even by processes with Administrator privileges.

## E-SSO-M Integration with other solutions

The central E-SSO-M engine supports integration with external systems and applications. E-SSO-M offers a COM object as an interface, but also has an open standard SPML (Service Provisioning Markup Language). SPML is based on SOAP/XML messages and E-SSO-M supports web services. E-SSO-M allows integration with:

1. Password reset applications such as password synchronization or helpdesk applications. If a password is reset for a certain user in a certain application, integration allows processing of this reset by E-SSO-M. As a result, password changes are transparent to the end user.
2. User Provisioning. In the event that a new employee joins the organization, user accounts and passwords must be created in various systems and applications. E-SSO-M has the ability to connect too many of the popular automated User Provisioning Applications such as UMRA, IDM3, ILM, Sun Identity Manager, etc. This integration allows end users to be recognized immediately in E-SSO-M, creating several benefits: 1) the end user does not need to create or remember various passwords 2) the end user does not need to make himself or herself known within E-SSO-M 3) the end user has direct access to the application landscape of the organization.
3. Reporting. All data related to end users' access of applications is stored in a SQL database. The data model of E-SSO-M is published and can be accessed with reporting tools.

## E-SSO-M Several user accounts per employee

An employee sometimes needs access to an application via more than one username. For example, system administrators may have a "normal" account and an admin account. Perhaps this system administrator needs to access applications in various environments which have been created for development, testing or production. In these cases, E-SSO-M shows an extra dialogue that allows the administrator to select a specific username and/or environment when an application starts up. After this initial selection, E-SSO-M ensures that the application starts up in the right environment using the correct username/password.

## E-SSO-M Delegation of application

During a vacation or sick leave, it may be necessary to provide another user with temporary access to a different application so that critical business processes can continue. This requires changes to the network security settings in order for the temporary user to obtain the correct access rights, or the usernames/passwords may simply be exchanged. Both approaches have a negative effect on security policy: access rights are often not returned to their original settings, or passwords are not changed at the end of the period.



E-SSO-M has a unique feature that allows user credentials of an absent employee to be delegated to a different employee (the delegate) for a specific application during a defined period of time. When the delegate starts the designated application, he or she receives a popup that allows them to select

The absent employee can define to whom and for which period the user credentials can be delegated. Once the period has finished, the rights of the delegate to use the user credentials automatically ends.

## E-SSO-M Offline portable mode

E-SSO-M has a feature that allows local workstation caching, a so-called offline mode, in case a workstation fails to connect to a central E-SSO-M service. This feature is primarily meant for laptop users who do not always connect to the company network, yet want to make use of E-SSO-M.

## More information :

