TECHNICAL LEAFLET

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

ENTERPRISE SINGLE SIGN-ON MANAGER (E-SSOM)

ENTERPRISE SINGLE SIGN-ON MANAGER (E-SSOM), A KEY PART OF THE TOOLS4EVER IDENTITY & ACCESS MANAGEMENT (IAM) SUITE, PROVIDES A MODULAR APPROACH TO SINGLE SIGN-ON AUTOMATION AND AUTHENTICATION.
E-SSOM IS A FLEXIBLE SOLUTION THAT GIVES AN ORGANIZATION OPTIONS FOR STRIKING THE PERFECT BALANCE BETWEEN ACCESSIBILITY AND SECURITY.

OVERVIEW

System administrators can choose to implement the complete E-SSOM suite or start with the most critical modules and build-out a system as their needs dictate over time. Simply start with the Central Server and add any combination of the following E-SSOM modules:

AUTOMATED LOGIN (AL)

The Automated Login module ensures that a user only needs to log in once with their Active Directory user name and password then they are automatically authenticated for every system and application they are allowed to use with a single login. The AL module saves a tremendous amount of time enabling users to move seamlessly between systems and applications without having to stop repeatedly to log into separate systems. Automated Login handles all the log-in screens for an end-user automatically.

Features:

- Support for all types of applications, Telnet, mainframe, Java, Flash, Client-Server, HTML, VBScript, etc.
- Enables System Administrators to manage application definitions
- AD group membership regulation for establishing which end-users are granted access to Automated Login and to which applications
- Can automatically handle password reset requests for specified applications
- Selective delegation of application access by end users to other colleagues if enabled by System Administrators. All actions by the end-user are stored centrally in a SQL database for tracking and audits.

AUTHENTICATION MANAGEMENT (AM)

Enable end users to access required applications with just the swipe of a smart card via the E-SSOM Authentication Management (AM) module. Additionally, in environments where added security is required, System Administrators can implement two-factor authentication replacing the normal Windows login with a smart card and a PIN code. The AM module supports a number of physical recognition types: cryptographic passes, active RFID smart cards and biometrics.

Features:

- Compliance with requirements for HIPPA, SOX and other government regulations
- Adjustable complexity of the PIN code
- Adjustable memory period for the entered PIN code
- End-user self-service for linking smart cards to their account
- Connections to existing access systems
- Delegation options so that managers can reset PIN codes or withdraw and issue smart cards

VIRTUAL DESKTOP AUTOMATION (VDA)

The Virtual Desktop Automation (VDA) module provides the ultimate in flexibility for fast user switching from one workstation to another – especially beneficial for healthcare applications where users may be moving rapidly from one workstation to another between patients. The VDA module is fully integrated with all VDI types and produces a user-friendly form of Follow Me. The user only has to introduce the smart card to the reader and within 8 seconds, the VDA module automatically enables a reconnect with the open session for a seamless, secure user experience.

Features:

- One-Touch-Access: The end user simply logs in by placing or tapping a card on the reader
- Citrix Ready certification - works in conjunction with virtualized desktops (Microsoft RDS, VMware View, and Citrix XenApp / XenDesktop) or Terminal Services
- Multiple smart cards per end-user
- Enforcement of security policies that require only smart cards that are already registered in another system to be used

WEBSSO

The WebSSO module offers external SSO so that those working at home with their PC or laptop only have to log in once, after which access is automatically granted to all cloud applications from any device. The end-user logs in to WebSSO with the username and password registered in Active Directory and they're granted access to all of their normal systems and applications.

Features:

- Seamless integration with Active Directory
- No extra investment needed for firewall products or similar
- Continuous communication with the central E-SSOM server so that changes are always available everywhere

CENTRAL SERVER

For each module to operate, the Central Server is a minimum requirement. The Central Server is not a hardware appliance, rather a software service that can be installed on any Windows server. The Central Server manages the definition of the application profiles, the log-in details of end-users per application and the audit details. The server is managed via the E-SSOM console.

Features:

- Redundant data via SQL Server cluster or replication
- High availability 99.999% via automatic failover and offline caching on clients
- Reporting engine for automated HTML, email and CSV reports
- Intuitive interface for defining applications to enable SSO
- Delegated interface so that the help desk can carry out administrative tasks

EAST – CALL: 866-482-4414 OR EMAIL US AT: NASALES@TOOLS4EVER.COM
WEST – CALL: 888-770-4242 OR EMAIL US AT: NWSALES@TOOLS4EVER.COM