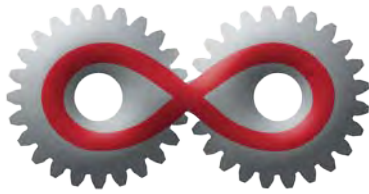


tools4ever



Tools4ever's Single Sign On Now Features Access Card Integration

Two-factor authentication supported for all card readers

Lynbrook, NY (PRWEB) December 06, 2011 - Tools4ever, the market leader in Identity & Access Management (IdM) solutions, has introduced a new version of its Single Sign-On solution, E-SSOM. The primary new feature in this version is Two-factor authentication (2FA), or integration with access card systems. This new feature provides the primary login for Single Sign-On with additional security through the use of an access card/smart card with a PIN code. Rather than entering a single combination of user name and password, users can now login by holding their access card against a card reader and entering a PIN code. By combining Single Sign-On with this authentication method, users can benefit from a convenient single login, while unauthorized users are banned from access to the network.

With two-factor authentication (TFA or 2FA), two independent tokens are used to confirm a user's identity. Two-factor authentication is regarded as a highly secure means of authentication because it is based on something the user owns (the access card) and something the user knows (the PIN code). E-SSOM offers end-to-end integration with all common readers for two-factor authentication, including HID, UziPas, Mifare, Biometrie, Gridtoken, Proximity Based Devices and RFID.

E-SSOM offers native integration with the card reader's driver software and links the access card ID to the user's credentials (user name/password) in Active Directory. No additional software is required to create this link.

E-SSOM offers various additional two-factor authentication options, including:

- Auto Application Start: When end users have verified their identity using their smart card and PIN code, the system will automatically launch a set of applications and log them in, so that they can start working immediately.
- Auto Application close: When a workstation has been locked by a user, other users will typically only be able to log in after restarting the workstation. E-SSOM offers the ability to unlock workstations without the need of a restart. It will properly stop the applications of the locked user and perform a fast user switch or follow me to the new user.
- Self Service registration: When a user holds an unknown card against the reader, E-SSOM will ask which username/password has to be linked. It is not required to centrally link and issue cards in advance. The end user himself will be able to perform the registration process. which results in a considerable reduction of the workload on the central smart cards issuing point.

- Pin code memory: After users have entered a PIN code, E-SSOM will remember it for a predefined period. This means users do not have to enter the PIN code each time they use their smart card to log in.

- Behavioral authentication: E-SSOM enables users to exactly define how smart cards must be handled. For instance, they can indicate that the card should remain in the reader (contactless reader) during the period the employee is logged in. Another option is only to require this during login. Yet another possibility is to require the card is presented to the reader for a couple of seconds. As long as the reader supports these options, they can be set in E-SSOM.

A full list of card readers supported by E-SSOM is available at:

<http://www.tools4ever.com/products/enterprise-single-sign-on-manager/two-factor-authentication/readers/>