

**XYLOC®**

# XyLoc SSO Single Sign-On Software



## Still Typing User Name and Password?

## Leverage XyLoc SSO to improve user productivity and data security



### Lower the Administrative Burden of Strong Passwords

Strong passwords are the most secure type of passwords, containing eight or more characters with upper and lower case letters, numbers, punctuation marks and symbols. While these passwords are hard to crack, they are also hard for users to remember and cumbersome to type in. For users who log in and out of a PC multiple times per day, this can result in frustration and lost productivity.

Frequently, users will write down their strong password(s) on a piece of paper, perhaps with other important data. This password “cheat sheet” can easily be inadvertently left at a PC and then viewed by others – compromising workstation security and potentially resulting in a data privacy violation.

When users forget their passwords, they call the Help Desk to reset the forgotten password. The user is locked out of the workstation and prevented from working until someone at the Help Desk can be reached to reset the password. This creates a further loss in user productivity and a burden on limited IT resources.

### XyLoc SSO Solves the Complex Password Problem

Combined with XyLoc Security Server (XSS), the XyLoc SSO (Single Sign-On) scripting tool forms a strong Identity and Authorization Management (*idM*) system. Users can sign on to a PC with a simple password or PIN number, and upon successful authentication can access all desktop and network applications that they are authorized to use with automatic population of user names and strong

password fields, thereby eliminating the need for the user to remember multiple strong passwords for their applications. Given the convenience of a simplified log-on and authentication process, users will maintain a more productive workflow and many unnecessary calls to the IT Help Desk for password resets will be eliminated.

XyLoc SSO is an extremely cost effective tool that removes the complexity of password management while maintaining application software security. Regardless of the application, whether Windows desktop based, web based, virtualized (e.g., Citrix or Symantec), Java-based or legacy, XyLoc SSO can support them all.

### Benefits of XyLoc SSO

- Cost-effective Single Sign-On solution
- Software-based; no appliance required
- Reduces user frustration and enhances productivity
- Self-Service Password Reset capability eliminates calls to the IT Help Desk (sold separately)
- Creation of audit log to view user access activity of disparate applications
- Seamlessly integrates with XyLoc Security Server to form a strong 2-factor Identity and Authorization Management (*idM*) system for Active RF and Passive Proximity cards
- Compatible with all Citrix XenApp and Terminal Services-hosted applications
- Works in “off-line” mode
- LDAP-compatible storage of encrypted credentials (AES 256-bit)

# XyLoc SSO – Flexible, Robust, and Cost Effective

## Support for Strong 2-Factor Authentication

XyLoc SSO and XSS support strong 2-Factor authentication using either Active RF proximity (XyLoc) cards or Passive Proximity cards. Sign-on passwords can be tied to the user's Active Directory password or a PIN number. Fingerprint biometrics can be used instead of a password or PIN number.

## Shared Workstation and Fast User Switching

XyLoc SSO and XSS support both Windows Unique Accounts and shared workstations ("Kiosk") where a common Windows password is used. Each user must still authenticate onto the workstation using their password or PIN number, but since there is a generic Windows log-on, fast user switching is enabled. An audit log of user activity is maintained for auditing purposes, e.g., for HIPAA compliance. With the XyLoc Active RF proximity devices, walk-away security is provided. For passive proximity-based uses, a configurable "hot key" screen lock and configurable inactivity lock/log-off timer are supported, along with a screen lock by a "tap-out" of the passive proximity card.

## User Provisioning

XyLoc XSS provides a web-based graphical interface to quickly and easily provision and de-provision users and their application credentials.

## Self-Service Password Reset

Using the native XyLoc client, users are able to securely and conveniently reset their primary domain passwords, without making a call to the Help Desk.

## Password Policy Enforcement

XyLoc SSO can be configured to enforce strong password requirements during an application password change or expiration, as well as handle periodically required password changes due to group policy settings.

## Citrix/XenApp & Terminal Services Support

XyLoc SSO supports application software virtualization using products such as Citrix XenApp, Symantec, or Terminal Services-hosted applications. Based on the configuration, the desktop can be configured to automatically roam the user's remote session when the user logs into a workstation, and automatically lock the desktop of the user's previous workstation when the user roams to a new workstation.

## Compliance Reporting

XyLoc SSO, in combination with XyLoc Security Server (XSS), records all computer and application access events into a SQL Server database for easy retrieval and reporting.

## Technical Specifications

### Desktop Operating Systems

- Windows 7
- Windows Vista
- Windows XP, XP Embedded

### Server Operating Systems

- Server 2008
- Server 2003

### Directories

- Microsoft Active Directory
- LDAP-compliant

### Administrative Console Requirements

- Microsoft Internet Explorer 7 or later running on a Windows operating system

### 2-Factor Authentication Methods

- XyLoc Active Proximity Cards
- Passive Proximity Cards
- Fingerprint Biometrics

### Application Environments

- All Web-based applications running in Internet Explorer 6.0 or later on supported Windows platforms
- All mainframe applications accessed by terminal emulators
- All virtualized applications (e.g., compatible with Citrix XenApp/XenServer/XenDesktop/ XenPresentation, Symantec)
- Windows Applications, including Java applications
- Desktop Applications (custom/legacy) running on a supported Windows platform
- All clinical applications for Healthcare including:
  - Epic
  - Cerner
  - GE Medical
  - Siemens Medical
  - Meditech
  - Healthland