

Bioscrypt® VeriSoft™ Single Sign On

Multi-factor authentication with a single sign on

ENTERPRISE SINGLE SIGN ON

Bioscrypt VeriSoft Single Sign On stores usernames and passwords for multiple applications and automatically enters logon credentials when a registered application is accessed. Users no longer have to memorize the growing number of passwords for web based and Microsoft® Windows™ applications.

MULTI-FACTOR AUTHENTICATION

Bioscrypt VeriSoft Single Sign On supports multifactor user authentication, including fingerprint biometrics, user passwords, smart cards, proximity cards and virtual tokens. This robust feature allows for multiple authentication methods to be used in any combination when assigning access privileges to applications and services.

FINGERPRINT VERIFICATION

Password protection is no longer considered to be effective protection for an organization's sensitive and private information. Bioscrypt's award-winning fingerprint-matching algorithm, which placed first at the Fingerprint Verification Competition (FVC) in 2002 and 2004, has been independently validated as the most accurate and inter-operable fingerprint verification technology on the market.

AUTOMATED PASSWORD MANAGEMENT

Password generation is completed behind the scenes and is transparent to end users. The result is a highly secure and easy-to-use identity and access management solution that is designed to authenticate users quickly and efficiently while securing sensitive organizational data.

PHYSICAL/LOGICAL ACCESS CONVERGENCE

Bioscrypt VeriSoft Single Sign On enables Door-To-Desktop® convergence by sharing identity credentials with the enterprise's existing physical access controls.

Reduce password management costs

Automate user logons

Replace or augment passwords with strong authentication

Unify user identities across the enterprise

Enforce corporate security policies

Use existing identity infrastructures

Reuse physical access credentials



Bioscrypt® VeriSoft™ Single Sign On

FEATURES

PASSWORD MANAGEMENT

- Supports most Microsoft® Windows™-based applications
- Supports most Web interfaces
- Supports many VPN clients (including Cisco® VPN)
- Supports Terminal Server & Citrix® Presentation Manager

SINGLE-SIGN-ON AUTOMATION

- Corporate and personal scripts
- Drag-and-drop learning

DIRECTORY INTEGRATION

- Microsoft Active Directory™
- LDAP v3 compliant directory server

MULTI-FACTOR AUTHENTICATION

- Passwords
- Fingerprint sensors
- Smart, contactless, and proximity cards
- Virtual tokens

SELF-SERVICE PASSWORD RESET

- Users can securely store personal questions for identity verification
- Eliminates help desk calls for user password resets

CENTRALIZED IDENTITY and POLICY MANAGEMENT

- Dynamic Policy Engine
- Centralized user enrollment
- Role-based access control
- Delegated administration
- Event viewer

MULTI-LINGUAL INTERFACE

- English, French, Spanish, Portuguese, and German

SUPPORTED HARDWARE

LAPTOPS WITH EMBEDDED FINGERPRINT SENSORS

- Authentec® and UPEK® sensors

FINGERPRINT READERS

- Authentec, UPEK, Secugen® readers

KEYBOARDS

- Authentec and UPEK fingerprint sensor
- PCSC-compatible smart card
- Proximity/contactless card

PROXIMITY / CONTACTLESS CARD READERS

- Omnikey

SMART CARD READERS

- PCSC compatible



INTEGRATED APPLICATIONS

SINGLE SIGN ON

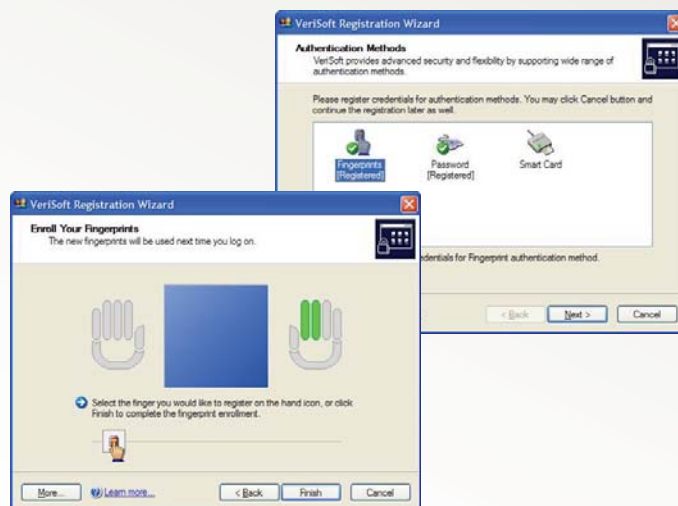
SSO allows automatic logins by retrieving and entering user names and passwords for applications and web sites. SSO can easily manage user names and passwords for hundreds of different applications and Internet addresses with its adaptive learning process.

SECURE DESKTOP LOGON

Log on to Windows by using multi-factor authentication, including any combination of fingerprint biometrics, smart cards (contactless or proximity), and passwords. A centralized policy determines the user's required credentials.

BACKUP and RESTORE

A complete and convenient method to protect and migrate password, account, and identity information between machines for recovery purposes. Backups can be done into other secured cryptographic devices such as smart cards, USB tokens, or secure encrypted files.



SYSTEM REQUIREMENTS

SERVER

- Windows 2000™ with SP 4, Windows 2003™ or newer
- Microsoft Active Directory (or LDAP v3 compliant directory server)
- Internet Information Server™ v5.0 or newer
- Internet Explorer™ v6.0 SP1 or newer
- 60 MB hard disk space

DESKTOP CLIENT

- Windows 2000 with SP 4 or newer (incl. Windows XP™)
- Internet Explorer v6.0 SP1 or newer
- 53 MB hard disk space

BIOCRYPT INC.
505 Cochrane Drive
Markham, ON, Canada
L3R 8E3

P: 905.940.7490
F: 905.940.7492
sales@bioscrypt.com

www.bioscrypt.com