V-GO® SSO

Proven Single Sign-On Solution • High Performance
Very Easy to Deploy • Quick Payback and High ROI

v-GO SSO is a proven Enterprise Single Sign-On solution that works with all of your applications, without a lengthy and complex implementation effort. Whether you are deploying strong authentication, implementing an enterprise-wide identity management initiative or simply focusing on the sign-on challenges of a specific group of users, v-GO SSO's architecture supports your technical requirements and computing environment.

v-GO SSO's patented client-side software enables it to recognize and respond to password requests from almost any system or application. v-GO SSO supports any type of user authentication from password to smart cards to biometrics, and can store user credentials and its own system settings and policies in any LDAP directory or one of several SQL databases. The administrative console simplifies administration by automatically recognizing and configuring applications for sign-on with minimal effort by the administrator. Enterprise users gain sub-second single sign-on while connected or disconnected to the corporate network, while roaming between computers, or while sharing a kiosk with multiple users.

Proven Single Sign-On

The biggest user complaint with computers is "passwords" and one of the biggest security weaknesses in computer networks is poor password selection and management by end-users. A solution for unified authentication and application sign-on has been seen as the holy grail of both user convenience and computer security. With v-GO SSO, users authenticate once, and v-GO SSO does the rest. It detects and responds to all password-related events to automate every password management task for the end-user, including logon, password selection, password change and password reset. v-GO SSO delivers single sign-on for all your Windows®, Web, JAVA™, Unix Telnet, in-house developed, and host-based mainframe applications.

Secure Password Management

Because it automatically manages passwords, v-GO SSO can eliminate the tendency of employees to write their passwords down on sticky notes or store them in their PDA. Weak and stale passwords can be a thing of the past when v-GO SSO is configured to enforce strict password policies, even for applications that do not enforce it themselves. v-GO SSO keeps passwords and related data protected wherever they are located, in your directory, in transit from the directory to the client, in client local disk cache and in client memory. v-GO SSO uses the strongest cryptography available, including TripleDES and AES. v-GO SSO's FIPS 140-2 compliance helps financial institutions, government agencies, healthcare and other organizations comply with the stringent privacy and security regulations that govern their operations.

High Performance

In both client/server and terminal services environments, v-GO SSO delivers uncompromising speed while consuming minimal resources. It can logon to any application, including industry-specific applications, in less than one second. With its very small memory footprint – typically less than 1MB and event-specific resource use, v-GO SSO's impact on both the client and the network is minimal; additional hardware or software is not required.

Very Easy Deployment

Implementing and managing v-GO SSO is made simple with its graphical administrative console, superior directory integration and easily deployable client-side software. Point and click wizards walk an administrator through all the tasks of configuration, deployment, and administration. v-GO SSO ships pre-configured for most popular applications right out of the box. The administrative console has built-in intelligence to automatically configure v-GO SSO for applications it has never seen before with almost no involvement by the administrator – no scripting, no programming, no integration. Configuring the central repository or directory is simple because v-GO SSO utilizes the one already installed. Your network administrator can deploy v-GO SSO from a central location using any software distribution system, without having to add any hardware or software to the network and without having to involve end-users in the installation process.

Quick Payback and High ROI

In most organizations, employees must remember from 5 to 30 passwords and are required to change some of them as often as every 30 days. It may be difficult to see the time wasted entering, changing, writing down, forgetting and resetting passwords because it is lost in small, but frequent, increments, but it all adds up to a significant consumption of employee time. Productivity losses are not limited to just your users. Companies with multiple password-secured systems often attribute 20% or more of their help desk calls to employees' difficulties with passwords. For a 10,000-person organization, that's millions of dollars annually and tens or hundreds of thousands of dollars each month. By automating sign-on and eliminating users' need to manage passwords, v-GO SSO significantly reduces help desk costs and enables you to recover the lost productivity. The ability to quickly implement v-GO SSO and cut help desk costs makes it possible for organizations to recover the cost of the software in months, not years, while generating a Return on Investment well in excess of 100%.

Out-Of-The-Box Proven Single Sign-On For The Following Applications

v-GO SSO is preconfigured for the following applications and platforms. v-GO SSO can be configured for virtually **any other** application, even highly customized or in-house developed applications, **in less than 15 minutes!**

Host/Mainframe Systems & Applications

- Full support for AS/400 (via 5250), OS/390 (via 3270), and Unix-compatible (via Telnet) systems and applications
- Preconfigured for most commercial emulators including: Windows Telnet, Attachmate Extra!, G&R Glink, Hummingbird HostExplorer, IBM Pcom, IBM Host On-Demand, NetManage (WallData) Rumba, ScanPak (Eicon) Aviva, WRQ Reflection, Zephyr Passport, Bluezone, Attachmate Extreme, Hostlink and many more
- Full support for multi-screen logon/password change scenarios
- Full simultaneous support of multiple emulators and sessions

Windows and Client Applications

- Preconfigured for Microsoft Office, Adobe Acrobat Reader, FrontRange Goldmine, Interact!, PKZip, and many more
- Preconfigured for client-server applications such as Citrix ICA Client/Program Neighborhood, Microsoft SQL, Novell GroupWise, Oracle, Siebel Sales, and many more
- Full support for any 32-bit Windows, Windows console, JAVA AWT and Swing applications

Web and Browser-Based Applications

- Preconfigured for Microsoft Internet Explorer
- Support for Web pages including form-based and pop-up sign-ons
- Web Access/SSO support for: Netegrity SiteMinder, Oblix NetPoint, Tivoli AccessManager, OpenNetwork DirectorySmart, Entrust GetAccess, RSA ClearTrust, Citrix NFuse, and many other enterprise access management solutions.
- Specific web-sites can be excluded from SSO

E-mail, Groupware and Chat

Preconfigured for Microsoft Outlook, Lotus Notes, Lotus Organizer, Novell Groupwise, Qualcomm Eudora, Meeting Maker, Corporate Time, ICQ, AOL IM, MSN Messenger, Yahoo! Messenger and Netscape Mail.

Dial-up Networking & VPNs

- Preconfigured for Microsoft Dial-up Networking, Internet Explorer Dialer, AOL, Compuserve, EarthLink, Mindspring, MSN and WorldNet.
- Support leading VPN solutions from AT&T, Nortel, Cisco, and many more

Authentication Options

v-GO SSO integrates with most authentication methods and provides support for both primary login and re-authentication requests (i.e. forced re-authentication, session time-out or application specific authentication request) for both connected and disconnected use.

Windows Authentication

- Microsoft Windows 2000, XP & 2003 support
- Full support for Windows roaming profiles for user mobility
- Full support for MS Windows authenticator for certificate, smart card, biometric, or token without additional software
- Optional password change pass phrase to protect against administrative breach
- Optional integrated GINA for enhanced security

LDAP Authentication

- Authentication from any LDAP directory such as Sun Java System Directory Server, Novell eDirectory, etc.
- Optional password change pass phrase to protect against administrative breach

PKI Authentication

- Entrust-Ready, uses PKI cryptographic services for key encryption

Strong Authentication

- Full support for any MS CAPI CSP based smart card
- Biometric support for multiple vendors/devices, including SAFLINK

Security

- v-GO SSO authentication engine relies on two independent factors that are only present at run-time and randomly encrypted during the session in memory
- Credentials secured at all times in the directory, in transit, on the client and in memory. Individual credentials decrypted on-the-fly as needed.
- Full FIPS 140-2 compliant MS CAPI support for 3DES, AES and RC4 as well as for key generation and hashing services
- Defenses protect against breach or inspection by other processes
- All components digitally signed and run-time validated

Central Administration

Console

GUI based Administrative Console provides wizard- based configuration and control over all settings and users, including:

- Directory configuration and administration
- Management of individual users or users by role and group
- User and application configuration and policy control
- Control of v-GO SSO settings including password policies, system rules, UI functionality, re-authentication parameters, etc.
- Available as a .Net console or as an MMC snap-in.
- Control of v-GO settings including password policies, system rules, UI functionality, re-authentication parameters, etc.
- Available as either a .Net based v-GO Administrative Console or as an MMC snap-in.

Deployment

- Deploys using most deployment tools - Windows Installer (MSI), SMS, Tivoli, Zenworks, Novadigm, etc.
- Configurable First-Time-Use to set-up users and specific applications

Credential Management

Credentials securely stored in a directory, file share or database for distributed access

- Full support for Microsoft AD, ADAM, and LDAP v2/v3 directories including Sun Java System Directory Server, Novell eDirectory, IBM Directory, Oracle Directory and basic support for OpenLDAP and Critical Path
- Full support for Microsoft SQL Server and Oracle 9i and 10g databases
- File-share synchronization provides directory-like functionality
- Synchronizer API supports virtually any other repository or storage device
- Full support for synchronization upon any network status change, return from hibernation/sleep, timed intervals, network changes and other events

Other Features

Mobility & Backup/Redundancy

- Full mobility support, allowing users to log-on from any network workstation and any number of machines simultaneously
- Multiple users can easily and securely share one machine such as a Kiosk

Automated Password Change

- Detects or triggers password change for application, web site, host/mainframe, and/or network passwords
- Fully automated password generation and change, including a silent mode that does not allow any user involvement
- Password-generation policies include minimum and maximum length, allowing or restricting alpha, numeric, and special or repeated characters; uppercase and lowercase; begin/end character criteria, and more
- Full support for synchronized/shared passwords, such as Outlook and Windows domain, or applications and RACF or ACF2

User Session Controls

- Set session controls for Windows, v-GO SSO and application sessions
- Set v-GO SSO session timer for session re-authentication for every logon, once per session, or as frequently as desired
- Force re-authentication for specific applications
- User can temporarily pause v-GO SSO

Application Configuration

- Optional auto-prompt automatically recognizes password-protected applications and Web sites and prompts for configuration
- Configuration wizard makes setup of new logons very simple
- Configurable application interaction, detection and response methods for seamless SSO support

Server Based Computing (Terminal Services & MetaFrame)

- Full support for Windows Terminal Server and Citrix MetaFrame in all modes including Published Application
- Share credentials between local and virtual sessions

Event Logging & Reporting

- Administrator controlled logging of user v-GO SSO events and activities including logon, password change, authentication, policy setting, etc.
- Log events to the Windows Event viewer, an XML file, or support virtually any other method via Event API
- Generate usage reports based on user object detail

Customization

Modular architecture with exposed APIs enables easy integration, alternative authentication methods, credential repositories, and event logging mechanisms

Minimum System Requirements

SSO Client Agent

- Microsoft® Windows® 2000, XP, 2003 Server
- 100 MHz Pentium processor and 64 MB RAM
- Disk Space: ~2.5 MB for the installed program and data; a complete installation requires ~7 MB; ~25 MB available on hard disk for installer
- Internet Explorer 5.5 SP2 or higher with 128-bit encryption
- Citrix MetaFrame support requires MetaFrame 1.8 or higher
- Installation via MSI package requires Windows Installer 2.0

SSO Administrative Console & Server

- Microsoft® Windows® 2000, XP, 2003 Server
- 100 MHz Pentium-compatible processor and 64 MB RAM
- .NET Framework 1.0
- Windows Installer 2.0 or higher
- Disk Space: ~4 MB for MSI installer; ~31 MB for EXE installer, overall ~15 MB for the installed program and data
- Directory requirements Active Directory, Sun Java System Directory 5.1 or higher, Novell eDirectory 8.5 or higher, or other LDAP v2/v3 compliant directory

Zvetco Biometrics; 6820 Hanging Moss Rd. Orlando FL, 32807
www.zvetco.com; 407-681-0111