



First Universal Single Sign-on Solution • Very Easy to Deploy
Quick Payback and High ROI • Robust, Faster and More Secure

v-GO SSO is the first Universal Single Sign-On solution, which works with all your applications, without a lengthy and complex implementation and deployment process. 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 flexible architecture supports your environment, user requirements and financial constraints. v-GO SSO's patented client-side intelligence, combined with superior directory integration and a simple, yet powerful, administrative console, delivers the benefits of faster, more secure sign-on in days– not months.

Enterprise users can enjoy 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. v-GO SSO supports any type of user authentication from smart cards to biometrics, and integrates with any LDAP directory or Microsoft® Active Directory®, ADAM and SQL Server. This allows your organization to apply the security it needs as you require it, while relying on the infrastructure you already trust. Your users can log-on to your network and easily and securely access all their applications from desktops, laptops and kiosks.

Universal Single Sign-On

The biggest user complaint with IT is “passwords” and the biggest security weakness in IT networks is poor end user password selection and management. A uniform authentication and application sign-on solution has been seen as the holy grail of both user convenience and computer security. Properly implemented, such a solution can enforce strict password policies and eliminate the tendency of employees to write their passwords down on sticky notes or store them in their PDA. v-GO SSO delivers Universal Single Sign-On for all your Windows®, Web, JAVA™, Unix Telnet, in-house developed, and host-based applications, providing your users with secure and reliable access without having to remember numerous passwords. 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. Weak and stale passwords can be a thing of the past with v-GO SSO managing the strongest possible passwords for each application, ensuring secure and convenient access every time.

Very Easy Deployment

Implementing and managing v-GO SSO is made simple with its client side intelligence, GUI administrative console and superior directory integration. Point and click wizards walk an administrator through all the tasks of configuration, deployment, and administration. Even directory support is simple since v-GO SSO extends the directory without touching your base schema. Your network administrator can deploy v-GO SSO without any scripts or integration, enabling faster rollout with minimal resources. v-GO SSO ships with the ability to recognize most popular applications right out of the box. Customers can implement and deploy v-GO SSO in less than a week, assuring faster, more secure authentication for all your users and a quick payback for your CFO.

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 frequently as every 30 days. Managing these passwords is a time-intensive task. Productivity losses due to password proliferation are not limited to just your users. Companies with multiple password-secured systems often attribute 20% or more of help desk calls to password-related issues. For a 10,000-person organization, that's millions of dollars annually and tens or hundreds of thousands of dollars each month. By simplifying and automating password management of all applications, v-GO SSO significantly reduces help desk costs and enables you to recover productivity lost to chasing down forgotten passwords and wrestling with complex, inefficient security protocols. 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%.

Robust, Faster and More Secure

v-GO SSO delivers uncompromising security, speed and the lowest resource requirements in the industry. With its small memory footprint, event specific resource use, and record level processing, v-GO SSO's impact on both the client and the network is minimal, enabling great performance without security limitations. v-GO SSO keeps resources and credentials protected when stored in your directory, in transit, in local cache and in memory. Financial institutions, government agencies, healthcare and other organizations that need to meet stringent privacy and security regulations, can trust and benefit from v-GO SSO's FIPS 140-2 compliance and sub-second logon to any application, including industry specific applications.

Out-Of-The-Box Universal 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, 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 application
- Full support for Windows console applications
- Full support for JAVA AWT or 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.

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 95, 98, NT, 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™ and RSA Keon™ 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
- Smart card support for multiple vendors/devices

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 settings including password policies, system rules,

- UI functionality, re-authentication parameters, etc.
- Available as a .Net 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 synchronization upon any network status change, return from hibernation/sleep, timed intervals, network changes and other events
 - Full support for Microsoft AD, ADAM, and LDAP v2/v3 directories including Sun Java System Directory Server, Novell eDirectory, etc.
 - Full support for Microsoft SQL Server
 - File-share synchronization provides directory-like functionality
 - Synchronizer API supports virtually any other repository or storage device

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 programmatically initiates 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, applications and RACF or ACF2

User Session Controls

- Set session controls for Windows, v-GO and application sessions
- Set v-GO session timer for session re-authentication for every logon, once per session, or as frequently as desired
- Force re-authentication for specific applications
- Optional integration with desktop lock/unlock and screensaver events

Credential Management

- 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 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® 95, 98, NT® 4.0 (SP 6a), 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® 98, 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

passlogix®

Entrust® Ready

160 Pearl Street, 4th floor, New York, NY 10005

Tel: 212.825.9100 x 2 or 866.727.7564 x 2

Fax: 212.825.0326

Web: www.passlogix.com

Email: sales@passlogix.com