passlogix®

white paper

v-go®

The Benefits of an Industry Standard Platform for Enterprise Sign-On

The need for scalable solutions to the growing concerns about enterprise security and regulatory compliance can be addressed more reliably, efficiently and consistently when an enterprise's authentication solutions are built on an industry standard platform for enterprise sign-on.

passlogix

v-go

Executive Summary

In today's post-Enron corporate environment, IT managers must find scalable solutions to the growing concerns about enterprise security and regulatory compliance as they pertain to identity management, sign-on, authentication, and passwords.

These needs can be addressed more reliably, efficiently, and consistently when an enterprise's authentication solutions are built on an industry standard platform for enterprise sign-on.

Until now, authentication and sign-on solutions provided by third parties or built in-house have lacked a platform upon which their functionality could be standardized, raising numerous issues in regards to compatibility and interoperability between disparate systems.

Passlogix's v-GO Sign-On Platform™ is the first and only industry standard enterprise sign-on platform upon which an enterprise can build a full suite of solutions addressing all of their user-related authentication requirements.

Why a Platform?

In what way are an enterprise's complex sign-on requirements best served when all solutions are built on a standard platform? And what exactly do we mean by a "platform" in the first place?

An article in CIO magazine defines a platform as follows:

> A platform is a product, but there is more depth behind solving needs. As opposed to being a "point solution" – meaning that it satisfies one need or

group of needs at a point in time – a platform empowers the user to move beyond the original purchase criteria.

When we speak of an "industry standard platform for enterprise sign-on," we are referring to a set of base functionality upon which a suite of sign-on products can be built. The common functionality provided by the platform enables the products in the suite to automate sign-on to applications -- and to interoperate seamlessly with complementary technologies, such as authentication management and user provisioning.

The result: identity-based solutions can be deployed that solve an evolving set of problems in user authentication, application access, user provisioning and network security.

Without a sign-on platform, it is impossible to solve problems such as:

- Implementing strong authentication to applications enterprise-wide.
- Eliminating user involvement with passwords altogether.
- Universally implementing best practices for user authentication.
- Easily complying with newly promulgated regulations such as HIPAA.

The v-GO Sign-On Platform

The v-GO Sign-On Platform is an open sign-on platform that provides out-of-the-box functionality and open interfaces.

By leveraging the underlying commonality of application logon requests on the client -- regardless of the applications' back-end operating systems, databases, or hardware platforms -- the v-GO Sign-On Platform frees the enterprise from the limitations of the "authentication silos" built into various enterprise applications.

The platform intelligently recognizes and responds to application logon requests as they present themselves to users. By eliminating the need to integrate to applications via scripts, connectors, or wrappers … or the need to modify applications … v-GO can work with an extremely broad array of applications, regardless of hardware platform, operating system, development language, user interface, or the original application developer (vendor or in-house).

An enterprise implementing sign-on solutions built on the v-GO Platform can enjoy several key advantages:

- Extensibility – solution architecture is designed to accommodate the existing network directory, processes, and configuration -- providing the means to more easily integrate with the surrounding infrastructure.

- Flexibility – changes can be made to the IT infrastructure without jeopardizing v-GO sign-on processes.

- Centralization -- sign-on processes are managed, administered, and distributed throughout the infrastructure to all the individual identity silos (network authentication, individual applications, passwords) from a single point of control.

The v-GO Platform enables third-party developers and end-users to implement complete authentication and user provisioning solutions using best of breed components. It also permits seamless integration as if all were developed by one vendor.

Within the enterprise, the v-GO Sign-On Platform performs three core functions:

- Verifying user identities -- via network password or strong authentication.
- Managing application sign-on functions – logon, logon error handling, and password changes.
- Centralizing administration – such as configuration, user activity reporting, and credential provisioning / de-provisioning.

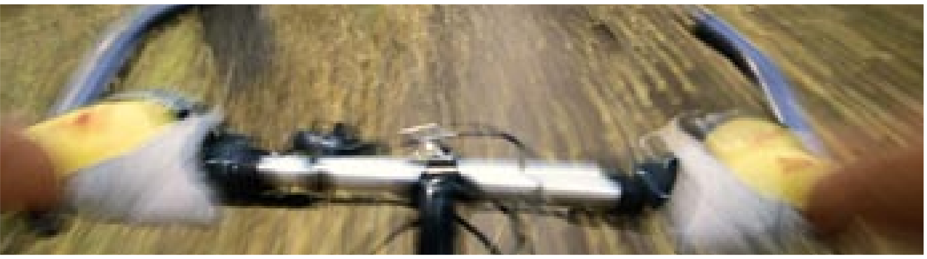
The outcome is a set of reliable sign-on processes that support existing methods -- types of authentication, applications, credentials, password logic -- and are flexible enough to accommodate both infrastructure changes as well as future sign-on requirements.

Elements of the v-GO Platform

The v-GO Sign-On Platform is composed of five key sign-on components:

- v-GO SSO … v-GO Single Sign-On provides interfaces to network and computer logons as well as sign-on to applications, enabling users to log in one time with a single password. Once users are logged in, whatever application they open is served the correct ID and password from v-GO SSO transparently and automatically. The system eliminates the need for users to remember and manage multiple user names and passwords for their applications, while allowing administrators to centrally change and manage passwords.

- v-GO SSPR … v-GO Self-Service Password Reset provides a recovery mechanism for users who forget their network logon. If users forget their Windows password, they can regain access to their computer and the corporate network. The software allows users to reset their password directly



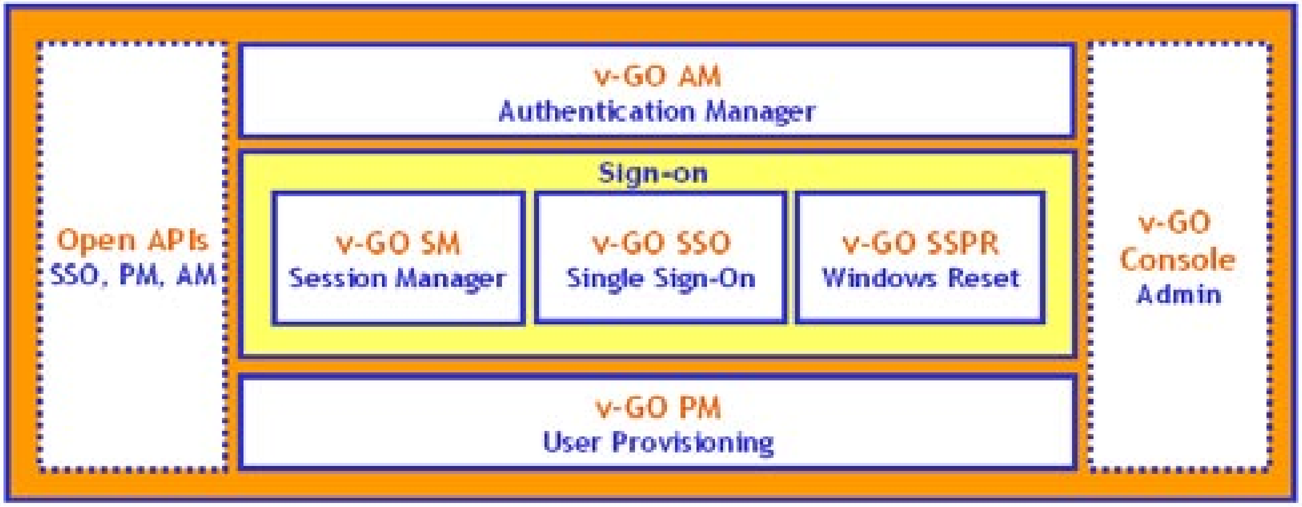
from the Windows logon prompt on their locked-out workstation, so that they can get to their applications within seconds -- without having to call the help desk or go to another workstation.

- v-GO SM … v-GO Session Manager provides initial user authentication and automated user sign-off to those environments (e.g. kiosks) where there is no authentication today, enabling secure kiosk computing at any location within the enterprise. The system monitors and protects unattended kiosk sessions from unauthorized access. Inactive sessions are protected by a secure screen saver, permitting the next user to sign on to a new session while safely terminating the prior session.

- v-GO AM … v-GO Authentication Manager allows organizations to use any combination of tokens, smart cards, biometrics, and passwords to control access to their applications, making it easier to implement advanced authentication strategies … without locking themselves into specific vendors or technologies. The software integrates seamlessly, providing granular control over the level of authentication required to access specific applications.

- v-GO PM … v-GO Provisioning Manager allows system administrators to directly distribute user credentials, usernames, and passwords, to v-GO SSO. The administrator can add credentials for new applications and new users as well as modify or delete old credentials to v-GO SSO. When provisioning a new user on a network, the administrator can place the user's credentials directly into their v-GO SSO account, so the user never knows or touches them.

The v-GO Sign-On Platform integrates with existing infrastructure.



A Platform for Authentication

Many companies today want to move from simple authentication, which uses only a password, to advanced or "strong" authentication.

Advanced authentication typically requires two forms of authentication. Typically, one authentication is "something the user knows," e.g. a password or PIN. The second form is usually "something a user has," such as a token or smart card, or "something the user is," such as a fingerprint or retinal scan recognized by a biometric reader.

For the enterprise planning a transition from simple to advanced authentication, there are many uncertainties regarding type of workstation (dedicated workstation vs. kiosk), type of authenticators desired, and how the use of advanced authentication methods affects permitted access to applications.

By implementing a platform-based approach to authentication rather than native integration of the authenticator, companies can minimize the time, cost, and complexity when changing authentication methods and components.

This gives them two benefits. First, they can more easily accommodate future choices. Second, they can insulate themselves from technology decisions that lock them in to a single vendor.

For example, let's examine a company planning to implement advanced authentication through smart cards. Without v-GO Authentication Manager (v-GO AM), IT must evaluate each authenticator vendor based upon their abilities to support the enterprise's specific applications and operating systems.

These applications may need to be recoded to be smart card aware. If the company is no longer happy with that particular smart card and wants to switch to a new smart card vendor, it must completely throw out any integration done with the prior vendor and re-implement a solution with the new one.

Or, if a company wishes to use different authenticators for different groups of users – for example, SecurID tokens for home-based employees and GemPlus smart cards for corporate campus-based employees – IT must integrate each authenticator to the target applications.

Similarly, a hospital may want a physician to use a finger print at a nurse's workstation, an iris scanner in the operating room – since he is wearing surgical gloves at that time, and a password when logging on from his office.

That means dealing with three vendors and three integration projects to access the same applications. When implemented without a sign-on platform, each authenticator a company wants to use generates its own requirements for integration with network resources and applications.

With v-GO AM, you can mix and match authenticators without worrying about how the authenticators connect to each application; the platform takes care of that automatically.

There are numerous benefits of using v-GO AM for advanced authentication:

- Ensures compatibility with popular authenticator vendors including, but not limited to, RSA SecurID, Ensure Xyloc, Gemplus smart cards, and biometrics.
- Reduces the integration effort, cost, and risk associated with implementing advanced authentication.
- Eliminates the redundant cost of integrating each authenticator to target resources and applications.
- Provides latitude in choice of authenticator technologies and methods.
- Ensures a seamless upgrade path from one authenticator to another over time or as a temporary workaround.
- Allows the grading of application access based upon authenticator usage, which can be

easily modified over time.

- Enables the administrator to easily implement, audit, and enforce delegated authority on an application and authentication method-specific basis.
- Handles context-free logon with a password to Active Directory, LDAP directories, and SQL databases.
- Supports strong authentication via PKI, smart card, token, biometric or other authenticator.
- Permits the flexibility to easily switch between logon methods based upon the capabilities of the workstation used.

You can grade access to applications based upon the type of authentication used (e.g. access to financial systems only with a smart card). And you can make that grading available for other processes. Access can be restricted by individual, role, or group to applications or categories of applications, each with its own level of required authentication.

The administrator can easily delegate access and authority, on a temporary or permanent basis, based upon the application and type of authentication used. He or she can also revoke such delegation at a later time.

A Platform for User Provisioning

With v-GO Provisioning Manager (PM), an administrator can transmit account IDs/passwords to a user's v-GO SSO credential store. The user automatically gains access to the account without having to manually track down the ID/password from e-mail or voice mail and type it into v-GO SSO. We refer to this process as "zero touch™ credential provisioning."

The v-GO PM provides production-ready interfaces to leading provisioning systems, a software development kit that enables quick and easy implementation with other provisioning systems, and an administrative console to permit manual credential provisioning.

Automated credential provisioning "completes the loop" between an administrator granting a user access to applications -- perhaps simply by the act of joining the company or changing roles -- and a user receiving the associated IDs and passwords in a usable form.

Furthermore, a company may not know which provisioning system they will use, may have

several in use, or may use an automated system for some applications and manual provisioning for others. Without a platform, a company will typically have to choose a vendor with a provisioning solution that includes some single sign-on (SSO) functionality -- or pick separate provisioning and SSO solutions that do not function together and often do not work with all of their applications.
Since none of the provisioning vendors have viable enterprise SSO solutions, a separate SSO solution is called for. However, separate provisioning and SSO solutions mean that users still have to be manually supplied their IDs and passwords – weakening security because users know their passwords, and increasing the probability that the IDs and passwords never actually get entered into the SSO solution.

An industry standard enterprise sign-on platform ensures that the provisioning system can communicate with the SSO solution. The platform allows a company to mix and match different automated provisioning systems, in different geographies or subsidiaries with automated populations of authentication data, into the SSO solution.

The choice of provisioning systems becomes seamless and invisible to the end users. Technology risk with regard to choosing one provisioning system over another is removed as pertains to its ability to interface to an SSO system. The uncertainty and expense of integrating a provisioning system to an SSO system are eliminated.

A Platform for Session Management

With v-GO Session Manager (SM), the administrator can secure application access at kiosks located throughout the enterprise.

Kiosks are typically not secure. They are logged in with a generic user ID, which is then shared by everyone using the kiosk. They do not track user identity, manage passwords, safeguard application data from unauthorized users, or log off automatically. Applications can be left open indefinitely, thereby potentially compromising the confidentiality of sensitive or private data.

The ability to quickly start and terminate user-specific sessions on top of the generic kiosk session is required in order to effectively bring user authentication to fast-paced environments, such as hospitals, manufacturing shop floors, and warehouse distribution centers. The ability to automatically terminate open applications when a user steps away from the kiosk is required to bring security to these same environments.

Built on the v-GO platform, v-GO SM allows session management at kiosks to be integrated into an enterprise's total identity management solution.

The v-GO SM software enables administrators to track user identity by user login and logout. It also automates password management.

Inactive sessions are automatically suspended and terminated. Open applications are also closed automatically. A screen saver is displayed until the next user approaches the kiosk to log on for a session.

A Platform for Password Reset

Enterprises that deploy v-GO SSO either:

1. Rely on the Windows password as the primary form of authentication, which can present an access problem when users forget their passwords.

2. Or, they keep the Windows password as a backup when some form of primary authentication fails, e.g. the user loses his smartcard or leaves it home.

Built on the v-GO platform to be fully compatible with v-GO SSO, v-GO Self-Service Password Reset (SSPR) provides a mechanism for users to reset their passwords without a call to the IT help desk.

The user can become authorized to reset his own password by answering a set of questions. When he answers enough question to reach a verification threshold, he is permitted to reset his password.

Answering questions correctly adds to his score, but wrong answers do not disqualify him. This way, lapses in memory and small errors do not drive the user to the IT help desk.

Conclusions

1. Use of a platform enables an organization to solve various related problems over time with one technology investment.

2. An industry standard sign-on platform provides a set of common sign-on functionalities that can be used to solve a large set of provisioning and authentication problems.

3. Use of a standard sign-on platform also ensures compatibility of authentication and provisioning systems with the enterprise’s current and future infrastructure, applications, and authentication devices.

Take the next step

For more information on the v-GO Sign-On Platform for authentication and provisioning, contact Passlogix today:

United States:
1 (866) 727-7564 Toll free
1 (212) 825-9100

United Kingdom:
+44 (0) 7775 692381

v-go®

passlogix®

white paper

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

FSSSO-070805