Global Information Assurance Certification Paper

Fredy Santoso
GSEC Practical
Version 1.4
July 8, 2002

v-GO™ SSO: Single Sign On or Single Password Solution?

Abstract:
This paper discusses a popular Single Sign-On product available in the market today, which is named v-GO™ SSO. Developed and patented by Passlogix, Inc., this software is mainly targeted at corporate users.

The main objective of this paper is to provide information and a clear understanding of the v-GO™ SSO product which will help the reader to see what the product actually is so that users can decide if this product meets their organization's needs. Furthermore, this paper also covers the details on how the product works and what customization can be made to achieve the maximum benefits. Some possible integrations of this product with other solutions to provide stronger security solutions are also discussed.

Background:
Look around your desk! Can you find that yellow sticky paper with an important note written on it? It has been a common situation everywhere that people use sticky paper to remind and inform them of something they always need to remember. One type of the notes that you can find easily attached to monitor screens is password lists.

When you have only one or a couple of passwords to remember, you are still doing okay. When you need to remember more than 10 different usernames and passwords, then the problems start. With the addition of the strong password rules required by many organization's security policies, it is not an easy job anymore to remember a bunch of completed strings, especially when those strings are even not logical for human memory. "Given the choice, users will usually choose a password that is easy to remember and type, and will choose the same password or series of passwords for different applications." [5]

Many organizations also require users to change their passwords every certain period; for example every 30 days, and users are faced with stress and headache because in addition to that, they cannot reuse the same password they had before. As the result of that, many users are tempted to write down those passwords and stick them on the monitor screen or keyboard.

Many users also forget their passwords easily and then they need to call the helpdesk to reset their passwords. The main objective of applying strong password policies is to protect the organization's information and resources, but

with this kind of situation, the organization may suffer great security risks due to user unawareness (like sticky paper notes) and a big amount of money for the password management, recovery, etc.

Many organizations are trying to solve this problem. There are many solutions available in the market today: password management tools, handy password storage like smart cards, stronger and easier authentication methods to replace passwords (e.g. biometrics, tokens), or the reduction of the number of the passwords required by integrating the organization's standard applications and services. Usually those solutions involve product integration into the organization's system and involve a lot of backend support.

Single Sign-On (SSO)

> "Single sign-on (SSO) is mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where he has access permission, without the need to enter multiple passwords." [7]

Single Sign-On (SSO) has attracted many organizations. With the main concept to use only a single password to access all applications and services throughout the organization, you can see how users can benefit from it. Since there is only one password to remember, users will not need to write it down and stick it somewhere. Easier to remember, and no more helpdesk calls to reset passwords. Fewer security risks, since there is now only one password for each person to access all applications.

> "Meta Group has found that SSO provides significant management savings and improvement in accuracy and consistency of user data. SSO also would decrease helpdesk calls by 33% and increase overall information security by 32%." [1]

Passlogix, Inc. has been developing a Single Sign-On product named v-GO™ and recently Passlogix, Inc. was awarded two US patents for SSO [3].

With a different approach, rather than having the product work on the server side, v-GO™ is client-based software. It is installed and runs on the client machines. As a client based software, v-GO™ does not need any server or backend infrastructure to enable its operation [6].

Users are managing their own password lists inside their client machines. Those credentials are stored in encrypted format in the hard drive and once a user is authenticated to the system, v-GO™ will work in the background and respond to every single application logon screen which requires user credentials and provide the credentials appropriately [2].

v-GO™ works with all Windows applications, web sites, and host-based applications. Since v-GO™ can recognize all of the Windows applications login boxes and respond to them, there is no need for difficult software integration.

Out of the box, v-GO™ is ready to use with most popular software like Lotus Notes, Eudora, Outlook, etc., which have been integrated into it. In addition to that, v-GO™ is configurable to accept customization and software addition. Users basically will need to configure their v-GO™ to meet their own personal needs, by adding their applications and web sites accounts into it. v-GO™ also recognizes if there is a login dialog box which is not configured yet in v-GO™ and will prompt the user to configure it.

v-GO™ Offering [9]:

Authenticator:

There are many options available as the authenticator for v-GO™. The authenticator is the key to get into v-GO™ and allows v-GO™ to operate by giving out user names and passwords to other applications. From the simplest one, i.e. your Windows login name and password, to the PKI certificate-based authentication, v-GO™ works virtually with all of these methods of authentication.

There is also another type of authenticator that comes together v-GO™, Graphical Password. Basically it is a replacement of password in the form of text with a kind of mouse movement and clicking. In the authentication window, the user will be presented with a visual task and he needs to do the task correctly per his own definition. Upon successfully doing this authentication task, user will be logged in to the system and v-GO™ will be enabled.

PKI Support:

Entrust PKI and RSA PKI, are both supported and v-GO™ is ready to be used with the existing PKI infrastructure owned by the organization. By using PKI certificates for authentication, organizations can benefit since all of the passwords stored in the local disk are encrypted using the user's PKI profile.

Automatic Strong Passwords Generation:

v-GO™ also can meet the organization's security policy for the strong password requirement and the regular password change. To help those users having difficulty defining a new strong password to replace the old one, v-GO™ can be configured to generate the strong password to satisfy the organization's password rule. v-GO™ recognizes the password expiration notice and will walk the user through the password change process. It generates a strong password to replace the old one and keeps this new one. The user never needs to remember this strong password because v-GO™ remembers it for the user.

LDAP Support [4]:

The latest release of v-GO™ also supports any LDAP directory servers which allows the users to use LDAP credentials as the authenticator as well. Linking v-

GO™ with the LDAP server will benefit the users of recovery in the future since the credentials will be synchronized with the LDAP server in addition to being store in the local hard drive. Administrators will benefit with an easy method of pushing out application updates for v-GO™ (for example, when some new standard organization applications need to be added). Certain organizations, which apply LDAP as the single credential for the organization services will benefit since when a user leaves the organization, by removing the LDAP credential, the user loses access to all applications and services.

Portability
v-GO™ stores user credentials in an encrypted format in the local hard drive. This information is tied together with the user's NT profile. For organizations which enable the NT roaming profile for their users to allow them to login from any connected PC within the organization, there is no problem implementing v-GO™ since the user credentials will also follow the users in the roaming profiles, which means the users can always login from any PC and always can access the credentials.

v-GO™ in Action [9]
Installation
v-GO™ installation is pretty simple, just like a normal software installation automated with a wizard. There are three types of installation available:

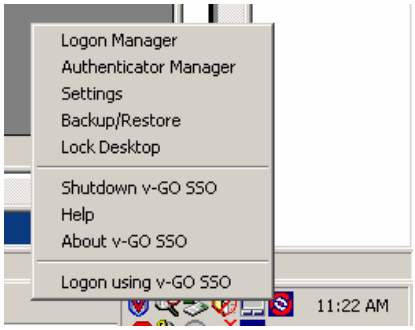
- *Typical* - This will install v-GO™ SSO with the Windows authenticator
- *Custom* - User can select which authenticators to be installed and other components such as the LDAP synchronizer
- *Complete* - Install all components: range of authenticators, and other functionalities

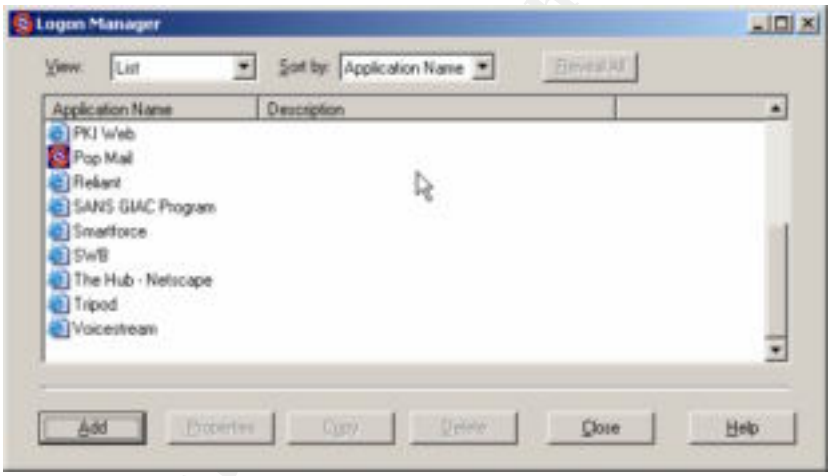
Choosing authenticator
After installation process, the next screen will ask the user to choose which authenticator to use. From the drop-down list users can choose the preferred authenticator. The available authenticators in this drop down list depend on the ones enabled during the installation process.
Usually for an organization deployment, the administrator will enable only one authenticator (which is the organization choice) and users will not be given the choice of another authenticator.

Registering application password
Next step, users will need to register their application passwords. The *Bulk Add* screen (defined by the administrator) will prompt the users to setup all the organization pre-defined applications. This *Bulk Add* helps users to setup all application credentials quickly so that the user can enjoy the benefits immediately.

Managing your passwords

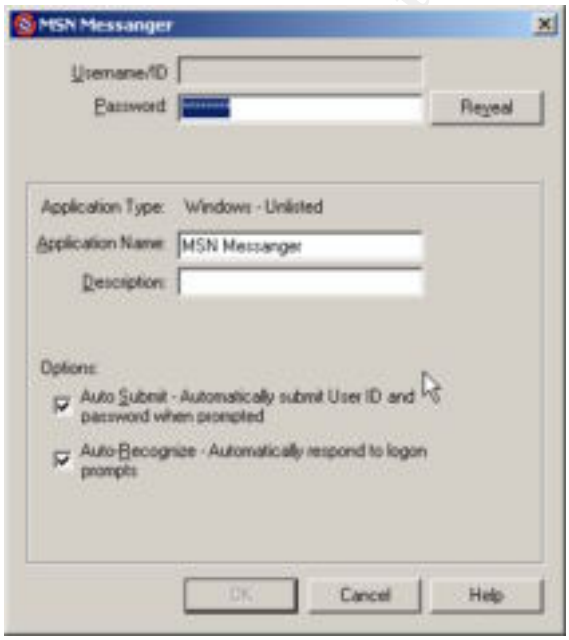
End users can always manage their password list. By right clicking the v-GO™ icon and choosing the *Logon Manager* menu, v-GO™ will show the entire registered application password list. Using this window, a user can add, edit, view, or delete entries.





Users also can customize each entry's specific behavior, like *Auto-Submit* and *Auto-Recognize.*

- *Auto-Submit*: v-GO™ will automatically hit the Enter/Submit button right away after it fills the user credentials to the login dialog box.
- *Auto-Recognize*: v-GO™ will recognize the user login box and automatically respond to it.



Adding web and application logins

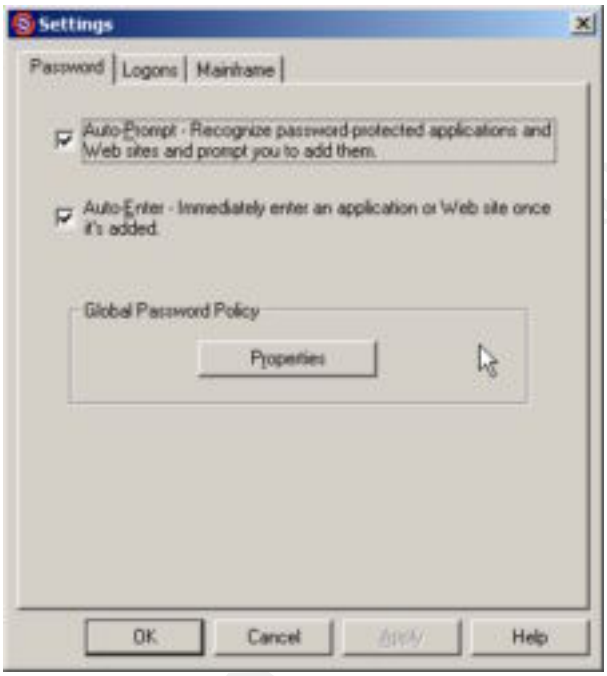
There are two ways for end users to add their additional applications and web sites to v-GO™. The first way is by using the *Logon Manager* from v-GO™ menu. Open the *Logon Manager* and click *Add*, then define the application/web site and enter the user name and password.

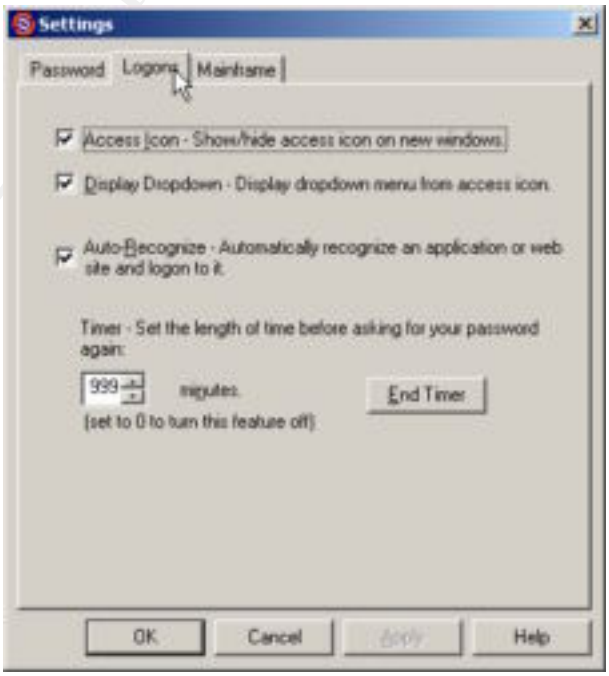
The second way is that you may wait for v-GO™ to prompt you (with *Auto-Prompt* enabled) to add the application credential to v-GO™ when you launch the application and it prompts the login box.

Advance Settings

There are some more settings users can customize in order to set v-GO™ meets the user's specific needs.

All the settings here are global settings. For special setting for certain entries only, users can specify by opening the *Logon Manager* and clicking on a certain entry and choosing *Properties*.





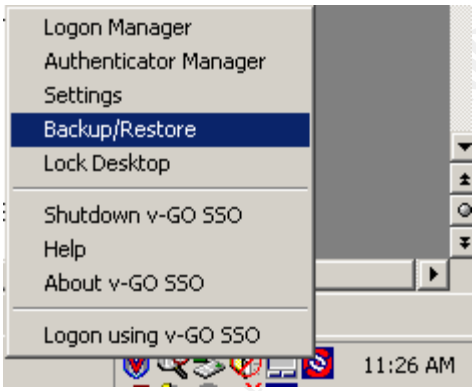
- *Auto-Prompt* – this enables v-GO™ to recognize the password-protected applications and web sites and prompt the user to set up the user name and password for this specific application or web site.
- *Auto-Enter* – this enables v-GO™ to enter an application/web site once it is added to v-GO™.
- *Access Icon* – to show/hide the v-GO™ access icon. By default it always appears on the top right side of every new window (beside the window minimize icon).
- *Auto-Recognize* – automatically recognizes the registered applications and web sites login dialog box and automatically fill the information without the user's interaction.

- *Timer* – This is to specify how often v-GO™ needs to ask the user to be re-authenticated. If it is set to 0, then the user needs to supply his single-password every time there is a need to login to an application or a web site.
- *Password Policy* – this is the setting to adjust v-GO™ to meet the organization password policy. Letting v-GO™ take care of your password roll-over does not mean it will do all the jobs correctly; for example if v-GO™ password policy is not set properly to meet the organization's password policy, then v-GO™ will not be able to generate and supply a strong password to meet the organization's password policy.
- *Enable Mainframe* – This will enable mainframe support which allows v-GO™ to recognize and respond back to login dialog in a mainframe session.

Backup and restore

A user may create a back up of his password bank and store it properly in a safe place. With this backup, the user then can always restore the password bank in case there is a failure on the machine or for migrating purposes.

To backup and restore a profile, right click the v-GO™ icon in the system tray and choose Backup and Restore menu. There will be a wizard to assist users to go through the process.



Some tips:

Hide the Access Icon

By default, v-GO™ puts its icon in the system tray and user can access the menu by clicking this icon. In addition to that, v-GO™ also puts an additional icon in the right upper corner of the current active window. This icon (beside the minimize window icon) is intended as an easy way to add new applications and provide login for those applications that the user has not set to login automatically. In

certain cases, this icon can block or disturb other icons that may be present beside the minimize icon as well (like if you have dual monitor, you will have an additional icon here). To take out this icon, you may go to the *Settings* menu and in the *Logons* tab, uncheck the menu "*Show/Hide access icon on new windows".*

Fill in complete URL

When you visit a web site, which requires user name and password, and you have not setup v-GO™ with the information yet, it will prompt you to set it up. After you enter your user name and password, then v-GO™ will always recognize this web site and respond to the login box with the user name and password you have provided.

After registering many web sites, you may recognize that sometimes, v-GO™ responds incorrectly to the web sites! If you look deeper, you would recognize that those web sites have the same domain name. That is the problem since v-GO™ only records the domain name of the websites by default.

So that if you registered a user name and password for www.abc.domain.com, then you have another login for www.bdg.hij.djk.domain.com, v-GO™ will be confused which one to present since it has two records recorded only with domain.com information.

To prevent this wrong login, you may edit the individual items and supply the correct and complete URL. Go to *Logon Manager* and right click the corresponding item and choose *Properties*. In the URL box, make sure you enter the correct and complete URL. By doing so to each item, v-GO™ will respond correctly to each web site you have configured.

Take out Auto-recognize

Auto-recognize and *Auto-submit* feature provides the user with easy and convenient way of login because right after v-GO™ enters the user name and password to the application login box, it will also hit the *Enter/Submit* button so that basically the user will not need to do anything, just within a snap, the login process is done.

However, in certain applications and web sites, this kind of feature can cause a looping problem. Certain application/web sites will direct the user back to the login screen after the user successfully logs out. With that *Auto-recognize* feature enabled, every time you log-out, you will be redirected to the login screen, then you will be logged in again since v-GO™ recognizes the login screen and responds to it.

To solve this looping problem, you may consider taking out the *Auto-recognize* for certain applications and web sites. Go to the *Login Manager*, right click the item you want to configure, and uncheck the option "*Auto-recognize.*"

Now for that application or web site, v-GO™ will respond to the login box after you click *Login Using v-GO™ SSO* from either the v-GO™ icon in the system tray or the one beside the window minimize icon.

Take out *Auto-submit*
Certain login dialog boxes, in addition to user name and password fields, have other items such as radio buttons or options to check. If there is such a need to check/choose before hitting the "*Enter/Submit*" button, then you may need to take out the Auto-Submit in that particular entry of your password list. Go to the *Login Manager*, right click the item you want to configure, and uncheck the option "*Auto-submit."* Now for that application or web site, v-GO™ will recognize the login box and fill the credentials there, but it will not hit the *Enter/Submit* button and will let you do it instead.

v-GO™ customization [8]
Even though v-GO™ is a client based software, it has a unique feature that makes it possible to be customized to meet certain organization's requirement.
Out of the box, v-GO™ has a bunch of well-known software already registered so that it is ready to be used by end users. In case the end users have some other applications which are not registered in v-GO™, they can always easily add that application to be recognized by v-GO™. End users for sure will customize v-GO™ to meet their own specific needs based on what applications being used. Besides applications, end users also need to add web sites they visit regularly to v-GO™ to enjoy the Single Sign On feature fully.

For a specific organizations' needs, v-GO™ also can be customized first and then pushed out to the community using that "*tailor-made*" version. An administrator can easily add some more organization specific applications which are not "*built-in*" to the application list so that all users will get those applications ready to use with v-GO™ as well. There are two files that can be edited in v-GO ™ which allow this customization to be made.

- *ftulist.ini*: this file defines the first time setup for end users after the installation is complete and it also defines the "*Bulk Add*". By defining all the organizations' applications here, end users will be able to setup all the application credentials in one shot right after the first login. In that one window "Bulk Add" form, users will be able to key in all the user name and password combinations for each application defined by the administrator and v-GO ™ will work right away after that.
- *entlist.ini*: this file defines the rest of the organization standard applications which are not defined by the standard v-GO™ package.

By editing these two files, an administrator can define some additional applications to be included for the end users.

How about future updates?
For example, now the organization is deploying "*customized*" v-GO™ with all the organization standard applications listed in v-GO™ so that basically it is ready to use for all the users without any further customization.

After three months, there are some more new applications added to the organization standard applications. It will be a pain if the IT support people need to help each user to add these new applications to v-GO™ as well.

This can be done easily since v-GO™ has the LDAP synchronization feature which allows the administrator to put the updated *ftulist.ini* and *entlist.ini* to the LDAP server and when the end user logs in to his machine and enables v-GO™, the *ftulist.ini* list in the client machine will be updated with the new one from the LDAP server.

With this approach, every time there is a new application that needs to be added, an administrator only needs to update the *ftulist.ini* and upload the file to the LDAP server. End users will get this update the next time their v-GO™ synchronizes with the LDAP.

Still regarding LDAP, in addition to the ftulist.ini update through LDAP, users' credentials (which are stored in encrypted format on the hard drive) also can be synchronized with the LDAP. This will enable a user to roam to another machine and pull his applications credentials and use them there. It also serves as a backup so that a user can always obtain his credentials back in case his machine fails for any reason.

Security concerns:
Utilizing an SSO product like v-GO™ is extremely convenient and it reduces a lot of the burden from the end users. However, there are many things to be considered, especially if v-GO™ is deployed in the entire organization. Security needs to be maintained and ensured. Picture this, with one password to enable the rest of the applications, it means now once the one password is cracked, all security is breached for that user.

Choose a strong authenticator
A strong authenticator is needed to ensure that only the designated user has access and nobody else can do so. v-GO™ alone with Windows login credential or a graphical password is not enough of a secure lock to protect the organization's information.

Integration with a token-based authenticator (like a smart card) and PKI certificate will add more layers of security to the existing system. Biometric devices can also be integrated with the v-GO™ client. With those added layers of authentication, it will ensure that the end users are authenticated properly before they are granted access to the password bank.

The authenticator chosen to be used with v-GO™ is supposed to be the one presented in the system login screen, i.e. the *GINA* (Graphical Identification and Authentication). Windows login is the default GINA for Windows operating system, however, other GINAs can be installed to replace the existing Windows login.

Why do we need to use v-GO™ with the GINA as the authenticator? Because this ensures that when the user locks the screen, it closes the access to the v-GO™ as well. When combined with hardware token and the token is not there, nobody else can access the system and v-GO™ client.

However, there is a possibility to use v-GO™ with an authenticator which is not the GINA. This can create a problem and security risk if the user logs-off from the authenticator and leaves the PC running without locking the screen. Some passwords decrypted previously in the session still remain and can be viewed in the Logon Manager window. v-GO™ has a time-out setting, and before this time-out ends, those decrypted password will remain readable.

Setting up the timeout
Again, the time out in v-GO™ settings defines how long v-GO™ client remains active until it needs authentication again. Many users like to set it up as long a time as possible, so that it reduces the annoyance of doing the authentication again and again, and actually, this is the “true Single Sign-On”; once you have logged in, that’s it!
Certain organizations may consider disabling this by setting the timeout to zero, which means authentication is needed every time v-GO™ needs to supply a user name and password for an application. This can be a good approach since there will not be any possibility that somebody’s password is stolen just because he is around without locking his screen, but with that put in place, now v-GO™ become a Single Password Solution and not Single Sign-On. User will need to supply this single password again and again in response to every application login.

Password Management Concern
Certain organizations deploying v-GO™ to the entire community also need to consider password management. What it means is that now the password management job becomes each user’s responsibility with the help of v-GO™. Maintaining the primary credential, which is the one used as the authenticator, becomes extremely important since this is the only one managed by the organization. Each user manages the rest. Organizations can provide back up and synchronization through the LDAP, for example, but users become the primary manager of their own credentials. Basically the ordinary way prior to v-GO™ (helpdesk calls to reset passwords) still can be used to retrieve passwords in case v-GO™ fails and there is no backup available.

Back-door dilemma
This is another situation where an organization deploys v-GO™ with the combination of a strong authentication method like smart card or biometrics. In order to get into the machine and enable v-GO™, a user needs to present the smart card/biometric and after the authentication process, access is granted. v-GO™ is actually enabled using the Windows authentication user name and password which will be presented by the primary login (smart card or biometrics) to the system after the user is authenticated. Such a system usually will generate a strong password and never let the user know about it. This is to ensure the strong authentication takes place and the user is truly authenticated before he is granted access to the system.

However, backdoors exist. Many secure biometrics/smart card GINAs always allow the user to setup a back door, i.e. to login using normal user name and password with the consideration that the user will be able to still login to the system in case the authentication device fails (for example: card reader is not working properly, the fingerprint reader is not working). With that in place, even though it provides an alternative during an emergency and maintenance by support teams, it creates security holes.

Others with the knowledge of the user name and password will be able to get into the system, and with the v-GO™ enabled inside there, full-control of the system is achieved.

Security policy to control password-rollover
The password rollover process is truly easy with v-GO™ in place. Users will benefit from the strong password generation and there is no need to remember it. However, some users may tend to write down the password (as back-up, to use with back-door, etc). If the organization wants to enforce the strong security policy, then v-GO™ should be configured to capture the password rollover without the option to let the user to specify their own password.

What is not in place yet, and what to expect to have in the future
Many aspects still can and need to be done to enhance the v-GO™ product. User portability for example, by storing the user credentials on something users can bring with them easily and use anywhere, it means integration of v-GO™ with smart cards. Stronger and truly integrated biometric authentication with v-GO™ will enhance the security by closing the back door.

Conclusion:
v-GO™ is a good and convenient Single Sign-On solution, easy and fast to deploy, but it needs careful planning and consideration of security concerns. By combining this solution with other factors of security, such as strong authentication mechanism and strong security policy and practice, we can achieve great security while maintaining end users' ease.

References

1. Chen, Anne. "*Web Identity Crisis.*" Ziff Davis Media, Inc. June 24, 2002, page 52. URL: http://www.eweek.com/article2/0,3959,268099,00.asp. (July 4, 2002).

2. Dix, John. "*Single sign-on doesn't have to be difficult.*" Network World, Inc. November 12, 2001. URL: http://www.nwfusion.com/columnists/2001/1112edit.html. (July 2, 2002).

3. Favaro, Michele. "*Passlogix is Awarded Two U.S. Patents for SSO.*" Passlogix, Inc. February 19, 2002. URL: http://www.passlogix.com/media/pdfs/pressreleases/Passlogix_Patents.pdf. (July 2, 2002).

4. Favaro, Michele. "*Passlogix Announces v-GO SSO 3.1.*" Passlogix, Inc. February 19, 2002. URL: http://www.passlogix.com/media/pdfs/pressreleases/v-GOSSO_3.1.pdf. (July 2, 2002).

5. Sturdevant, Cameron. "*Self-Serve and Save.*" Ziff Davis Media, Inc. January 21, 2002. URL: http://www.eweek.com/article2/0,3959,35332,00.asp (July 2, 2002).

6. Sturdevant, Cameron. "*Single Sign-On Goes to Work.*" Ziff Davis Media, Inc. March 18, 2002. URL: http://www.eweek.com/article2/0,3959,34689,00.asp. (July 2, 2002).

7. "*Single Sign On*." The Open Group. May 5, 1999. http://www.opengroup.org/security/sso/ (July 2, 2002).

8. "*v-GO™ SSO Administration Guide*", Passlogix, Inc. , February, 2002.

9. "*v-GO™ SSO Users Guide*", Passlogix, Inc., February, 2002.